Shelby County Information Technology Services' Policies and Procedures

Prepared by the

Shelby County Department of Information Technology Services
And
The Information Technology Steering Committee

Version 1.1c

01-15-15

Policy and Procedure Update Listing

The policies listed in this table have been modified since the last publication date.

Policy Name	Modified Date	Modifier	Notes
Adoption or Modifying of a Guideline, Policy, Procedure or Standard	*01-01-2000*	*Jane Doe*	*Misc.*
All Policies	08-01-16	Shawn McClure	Performed review of all policies and updated review dates.

Table of Contents

I. RESPONSIBILITIES OF INFORMATION TECHNOLOGY SERVICES 5
A. MANAGEMENT OF INFORMATION TECHNOLOGY SERVICES FOR THE COUNTY 5
B. TO DEVELOP TECHNOLOGY POLICIES, STANDARDS AND PROCEDURES 6
C. TO REGULATE TECHNOLOGY POLICIES, STANDARDS AND PROCEDURES 6
II. GUIDELINES, POLICIES, PROCEDURES AND STANDARDS 7
A. ADMINISTRATION AND SUPPORT 7
1. Adoption or Modifying of a Guideline, Policy, Procedure or Standard 7
2. General Principles for Everyday Technology Decision Making 10
3. Service Desk Notification 15
4. Service Desk Triage: 18
5. Portable Storage Usage 20
6. Scheduled Downtime 23
7. Software Key Management 29
B. APPLICATIONS, SOFTWARE DEVELOPMENT AND MAINTENANCE 31
1. Software Installation and Usage 31
C. ASSETS AND INVENTORY 36
1. Hardware and Software Installation Standards 36
2. Disposal of Obsolete Computer Equipment 38
3. Disposal of Media 40
4. Removal of Property 42
D. BACKUP, RECOVERY, DATA RETENTION, ARCHIVING 44
1. Data Classification Policy 44
2. Data Retention Policy 48
E. INTERNET AND EMAIL USAGE 53
1. Download Media and Streaming 53
2. Email and Digital Document Searches 57
3. Email Use and Accountability 59
5. Mobile System Use 66
F. PRIVACY 69
1. Employee Privacy Policy 69
2. Web Privacy Policy 71
G. SECURITY 73
1. Establishment of Security Program 73
2. Clear Screen Policy 75
3. Network Security Policy 78
4. Firewall and Router Configuration Standard 104
5. Acceptable Use Policy v1.4.b 108
6. Data Encryption and Key Management Policy 115
7. PKI Certificate Policy Statement 120
8. Information Security Policy 122
9. Shelby County ITS Patch Management Policy 131
10. Physical Security Standards and Personal Asset Management Policy 134
11. Software Development Life Cycle Policy 137
12. Security Incident Management and Response Policy 145
13. Shelby County Breach Notification Policy 153

14. Video Surveillance Policy 167
15. Physical Access Procedures 172

I. Responsibilities of Information Technology Services

A. Management of Information Technology Services for the County

ITS is charged with the overall organization and administration of Information Technology Services as characterized within the County. ITS will strive to apply the latest technologies to increase staff effectiveness, exploit technology opportunities, and gain advantages from technology advances. This responsibility applies to all computing, information, and network systems and services owned or administered by the County.

1. Development of Standards
   ITS will create standards and procedures for the management of information technology consistent with the mission and function of technology within the County's environment. (Please refer to Section II.)

2. Implementation of Best Practices
   ITS will research, identify, and implement those technology best practices which, when adhered to, will ensure an effective and sustainable Information Technology Services program suitable for the scope and goals of internal County services.

3. Management of System Development
   ITS will manage the lifecycle of all software systems and application programs targeted for County operation. ITS will strive to promote economy, efficiency, and effectiveness of departmental programs through timely, useful, and reliable information while preventing fraud, waste, or abuse. (Please refer to Section II.)

4. Communications Management
   ITS will operate and maintain a converged communications network capable of supporting voice, video, and data communications. ITS will, as requested by the Commission, provide additional services to insure the most efficient use of the communications infrastructure.

5. Security Policy Development
   ITS will maintain security policies which will delineate what must be done to keep the County's technology environment safe form malicious attacks, unlawful disclosures, and disruptions of operation. Practices and procedures will be developed for each policy to outline how the policy will be effectively implemented and the possible consequences of failure to abide by approved policies. (Please refer to Section II.)

6. Data Center Operations
   ITS will maintain a centralized data center adequate to support the computing challenges of the County's diverse lines of business. The data center will function according to best practices for operations, security, and continuity of services. (Please refer to Section II.)

7. Technical Services and Products
   ITS will be the focal point for the acquisition of technology services and computing-related products. ITS will work with vendors and suppliers of technical services and products to ensure the County acquires appropriate technology, and that technical requirements are adequately met. ITS will be the County's primary resource for technical expertise and the Commission's sounding board for technical guidance and recommendations.

B. To Develop Technology Policies, Standards and Procedures

ITS will develop policies, standards, and procedures (PSP) to implement an effective and sustainable technology program for the County. These PSPs will represent practical guidelines to define program operations. Areas to be addressed by PSPs are:

1. Application Development
2. Audio Visual Services
3. Document Management
4. Data Center Operations
5. Email Services
6. Help Desk Services
7. IT Project Management
8. Technical Services
9. Website Services
10. Telecommunications

C. To Regulate Technology Policies, Standards and Procedures

Appropriate use of technological resources is framed by the same legal and ethical considerations that apply to other public resources. The County requires that all its staff, elected officials, and approved guests abide by these policies. ITS will monitor for compliance with approved PSPs, and the will assist all County departments and agencies to identify and correct breeches in policy, or take punitive actions where appropriate.

II. Guidelines, Policies, Procedures and Standards

A. Administration and Support

1. Adoption or Modifying of a Guideline, Policy, Procedure or Standard

a) Policy Intent:

This document establishes standardized methods for adopting, modifying, formatting, and reviewing Information Technology Services (ITS) policies, standards and procedures. (Abbreviated as: "POLICY").

b) Scope:

This process applies to Information Technology Services guidelines, policies, procedures and standards.

c) Policy:

The purpose is to define a procedure for the drafting, vetting, and adoption of regulations pertaining to ITS and demonstrates the preferred format to be used.

d) Procedure:

The Approval and Revision Process for ITS Policies, Standards, or Procedures is outlined below.

(1) Conception: The Administrator will accept and review suggestions for a new or to be amended policy. The Administrator may abbreviate the following process in order to expedite the adoption of a "POLICY" as circumstances require. If the Administrator declines to initiate an adoption/revision process, the originator may appeal to the Chief Information Officer (CIO).

(2) Foundation: The Administrator will assign ITS management staff to lead, facilitate or monitor these efforts. The ITS management staff will initially work with the originator to document the need and scope of the "POLICY". If applicable, a broadly advertised formal notice of intent to adopt or amend a "POLICY" in a specific content area may be extended to invite appropriate decision makers, stakeholders, experts, users or others and the IT Steering Committee (ITSC) to participate. This notice will invite comments regarding the content area of the "POLICY" and seek volunteers to join a working team. The CIO may waive this comment period.

(3) Team Formed: Based upon feedback, the ITS management staff will form a working team. The Administrator and CIO may assign members to a working team. The working team will determine the required comment period and procedure abbreviations (if any) and ensure a sponsor has been designated.

(4) Drafting: The Team will research and prepare a draft "POLICY" which will include an impact assessment and a sunset or re-evaluation date. "POLICY" will include language designating which divisions/positions are responsible for developing implementation procedures and enforcing the policy. Procedures and standards will incorporate similar language regarding enforcement.

(5) Communication: The Administrator and the CIO will communicate regularly to the ITSC on "POLICY" development. It will be the responsibility of the leadership to communicate this information and provide feedback on behalf of the groups and functions they represent within the timeliness required by the working team. Final draft Policy will be presented to the CIO for review and comment. The CIO will present the "POLICY" to the ITSC at her/his discretion.

(6) The CIO (or designated working team representative) will present the final draft and the impact of the proposed Policy to the ITSC. The ITSC will discuss and notify the County Commission that this change in policy will be made.

(7) At the CIO's discretion, a policy and/or a "POLICY" may be returned to any of the above groups for further comment and/or revision.

(8) The format for "POLICY" will conform to the format in this document.

e) Applicability of Other Policies

This document is part of the County's cohesive set of security policies. Other policies may apply to the topics covered in this document and as such the applicable policies should be reviewed as needed.

f) Enforcement:

(1) Compliance - All staff engaged in operations, analysis or actions subject to a "POLICY" are responsible for becoming familiar, and complying, with the contents of the "POLICY"(s). Supervisors are responsible for incorporating standard operating procedures to ensure their staffs are familiar with, and adhere to, the "POLICY" affecting their program functions.

(2) Review - At his/her discretion, the CIO may initiate an effectiveness review of any existing "POLICY".

g) Policy Owner:

Shelby County Commission

h) Policy Administrator:

Chief Information Officer, Department of Information Technology Services

i) Policy Approval Date:

Current Revision Review Date:		08/01/2016
Current Revision 1.1	Approval Date:	10/10/2014
Original Version 1.0	Approval Date:	10/25/2012

j) Policy Effective Date:

Current Revision 1.1	Effective Date:	10/10/2014
Original Version 1.0	Effective Date:	10/25/2012

k) Compliance:

l) Supporting Form(s):

m) Definitions:

(1) The Administrator - The term the Administrator refers to the Associate to the CIO of the Department of Information Technology Services . See Guidelines and Procedures (A-B) for details of the responsibilities of the Administrator as they relate to the development or review of ITS "POLICY"(s).

(2) Chief Information Officer (CIO) - The term Chief Information Officer refers to the CIO, the chief administrative officer of Shelby County Government.

(3) Standard - A standard is a specific approach, solution, methodology, product, or protocol that must be adhered to for establishing uniformity.

(4) Standard Operating Procedure - The term Standard Operating Procedure (SOP) is the description of a prescribed method that must be used by the Department of Information Technology Services staff to develop or review "POLICY", standards, or procedures. SOPs are not appropriate to describe procedures or requirements that apply to members of the public, other than persons acting as agents of, or under contract with, Shelby County.

n) Appendices:

2. General Principles for Everyday Technology Decision Making

a) Policy Intent:

This document is to establish a general framework of architecture principles to aid in everyday decision making.

b) Scope:

This process applies to Information Technology Services policies, standards, and procedures.

c) Policy:

It is understood that formal Policies, Standards, Procedures, etc. will never exhaustively encompass every single aspect of ITS work within Shelby County. Yet, each ITS worker is faced with critical decisions as an integral part of their everyday work. Such everyday decisions frequently have lasting consequences. It is difficult to anchor such everyday decisions in the absence of a general framework of principles. Therefore, a set of easy, general architecture principles have been developed to aid in such everyday decision-making.

(1) The County is a single, unified enterprise.
(2) Information is a countywide asset.
(3) Security and Privacy are core missions.
(4) Limit the number of product/technology options.
(5) First reuse, then buy, then build.
(6) Optimally exploit existing products/technologies.
(7) Ensure orderly sunset & support of legacy products/technologies.
(8) Follow a set of well-defined criteria for selecting new products/technologies.
(9) Centralize identity authentication. Federate authorization as necessary.

d) Rationale/Procedures:

(1) *The County is a single, unified enterprise.* A single ITS enterprise with shared products and policies lowers costs and improves service. Further, any attempt at optimization is more likely to be fruitful when it targets the County as a whole rather than a single agency or program. Economies of scale, not only extract deeper discounts from vendors, but also facilitate interoperability and cross-training, thereby lowering costs and improving supportability. It is in the best interests of all parties to continue this trend and explore greater opportunities for collaboration and standardization across the County.

(2) *Information is a countywide asset.* Quality information is critical to effective government decision-making and accurate reporting to its citizenry. In some cases, common data elements are dispersed across multiple information

systems platforms, with disparate formats, contexts, and meanings. Authoritative sources of particular data elements are often not well-documented, and stewardship is not always codified. Such a state of affairs impedes countywide information flow, leading to poor governmental decision-making and underserved citizenry. Lacking effective data/information standards, agencies and programs are currently left to creating ad-hoc solutions, leading directly to the fragmentation of the County's information assets, compromised accuracy and integrity of its reports, and increased operational costs.

(3) *Security and Privacy are core missions.* Security and privacy of information are essential to government operations in order to retain the public trust. Citizens expect the government to apply security and privacy consistently and monitor compliance. Security controls must be clearly defined so costs and risks may be balanced appropriately. The County should implement security and privacy practices at all levels of government to ensure the confidentiality, integrity, and availability of its information assets. The County must do everything in its power to protect its information assets from unauthorized or accidental use, disclosure, disruption, modification, or destruction.

(4) *Limit the number of product/technology options.* In the past, individual arms of the County have acquired technologies on their own without much consultation or coordination with one another. The accumulative effect of that is the current reality, viz., a smorgasbord of competing technologies. This has some obvious disadvantages: lack of interoperability, lack of adequate support, lack of depth of coverage, lack of economies of scale, etc. In order to ensure greater success of ITS in the County, it is critical to limit the number of technology options. This will enhance interoperability for there will be fewer moving parts to interface with. This will increase the level and depth of support for there will be a higher headcount per technology option, directly leading to higher in-house expertise. This will increase economy of scale for there will be a higher market share per technology option, directly leading to increased pressure on vendors to provide deeper discounts, dedicated training, etc. Taken together, limiting the buffet of technology options promises to reduce ITS costs and improve service.

(5) *First reuse, then buy, then build.* Clearly, the best value to be extracted from existing investments is to reuse them to the maximum extent possible. If it is determined without a doubt that an existing ITS asset cannot meet current requirements, then the County should explore an off-the-shelf product that comes the closest to satisfying such unmet requirements. It is likely that the County will need to modify its workflows and business processes in order to utilize an off-the-shelf product, but that is still preferable to creating a custom product exclusively for its requirements. Only if it is ascertained that there does not exist any off-the-shelf product that comes even close to meeting its requirements, should the County explore the option of building a custom

product. While all generalizations are subject to caveats, it is extremely likely that the lifetime total cost of ownership for a custom product will far exceed that of an off-the-shelf product.

(6) *Optimally exploit existing products/technologies.*The County should fully utilize what it already owns. Unfortunately, due to the pace of innovation in IT, as well as the aggressive nature of marketing, the technology sector is more susceptible to hype than other sectors. Nevertheless, the County needs to summon the discipline to stick with the products/technologies that it already owns, as long as they continue to deliver an acceptable level of performance to its customers, and as long as vendors continue to support said products/technologies. Specifically, the County should consider exploiting additional capabilities of products it already owns that are still supported by their vendors, even when they may not be the best-of-breed in a particular niche.

(7) *Ensure orderly sunset & support of legacy products/technologies*. Legacy products/technologies invariably support business-critical processesand yet they become increasingly less sustainable over time due to two reasons. One: vendor support declines over time, and ultimately ceases to exist. Two: there arises a bidirectional pincer attack on the resource-pool for legacy technologies. The original resources are subject to retirement and attrition. At the same time, lack of market opportunity discourages younger personnel from acquiring the necessary legacy skills. But the diminution in sustainability does not reduce the business criticality of legacy products/technologies. Therefore, there needs to be proper planning, as well as an orderly sunset and support strategy for legacy products/technologies.

(8) *Follow a set of well-defined criteria for selecting new products/technologies.* The marketplace continues to explode with new products/technologies at a rapid pace. Clearly, no single entity, least of all the County, can afford to sample them all indiscriminately. That said, the County also cannot allow itself to fall too far behind the technology curve, lest it deprives itself of viable superior options. Therefore, it needs to chart a prudent middle course that can both filter out the hype, and yet discern lasting trends that have the potential to deliver higher returns. The selection criterion for a product/technology are as follows, in descending order of importance: *Customer Value (Return on Investment), Installed Base within the County & Supportability, Scalability, Sustainability (Viability), General Excellence & Market Position, and Alignment with Long-term Architecture*. Customer Value (Return on Investment) should command the highest weight. Cost considerations should be holistic, not just the one-time cost of acquisition, but a best estimate of the lifetime total cost of ownership. If a product/technology has a large installed base within the County and the County is already comfortable supporting it, it makes sense to continue with that product/technology and negotiate a deeper volume discount from the vendor. Scalability and Sustainability (Viability) are

important from an enterprise perspective. There exist ITS products that were originally acquired by individual agencies, which may have been adequate for meeting the requirements of those individual agencies, but do not scale, and therefore, cannot be sustained on an enterprise basis. It goes without saying that it is in the best interests of the County to bank on products that command positions of excellence in the marketplace. Finally, it is also in the best interests of the County to select products/technologies that are in alignment with its long-term architecture vision.

(9) *Centralize identity authentication. Federate authorization as necessary.* Authentication of computer and user identities should be centralized to improve service, allow unified credentials and/or single sign-on, and reduce application development and support costs. Centralization of authentication permits appropriate management and security controls to be applied universally. Make applications and appliances consume authentication from external directories. Microsoft Active Directory (A.D.) remains the authoritative directory for all internal ITS resources within the County. All internal applications and appliances should be fully A.D.-aware. The County currently does not have a unified directory for its external users (citizens, vendors, and partners), but it is working toward developing one. Individual applications and appliances are free to maintain their own dedicated authorization (roles) modules. However, wherever two or more applications or appliances require sharing authorizations, they should consider federating such authorizations to a neutral repository, with the system of record granted complete control to manage such authorizations [PCI DSS 7.1.4].

e) Enforcement:

(1) Compliance - All staff engaged in operations, analysis or actions subject to a "POLICY" are responsible for becoming familiar, and complying, with the contents of the "POLICY"(s). Supervisors are responsible for incorporating standard operating procedures to ensure their staffs are familiar with, and adhere to, the "POLICY" affecting their program functions.

(2) Review - At his/her discretion, the CIO may initiate an effectiveness review of any existing "POLICY".

f) Policy Owner:

Shelby County Department of Information Technology Services

g) Policy Administrator:

Chief Information Officer, Department of Information Technology Services

h) Policy Approval Date:

Current Revision Review Date: 08/01/2016

Current Revision	1.0	Approval date:	10/10/2014
Original Version	1.0	Approval date:	10/25/2012

i) Policy Effective Date:

Current Revision	1.0	Effective Date:	10/10/2014
Original Version	1.0	Effective Date:	10/25/2012

j) Definitions:

3. Service Desk Notification

a) Purpose:

Establish good incident reporting practices and expectations of ITS staff in problem resolution.

b) Scope:

This policy applies to all Shelby County organizations, employees, and contractors, and any other individuals or organizations that use Shelby County Technology resources. Shelby County Technology resources include, but are not limited to: networks, servers, data, applications, and information. It applies to all Shelby County facilities.

c) Exceptions

Severe issues or outages are alerted via automated process when they occur. These occurrences during nonworking hours would be the exception. If an employee can provide details to help shed light on an issue or the cause of an issue during their working hours, they should provide that information.

d) Policy:

Incident Awareness

When an employee first becomes aware of an incident during their normal job functions, whether the incident is an e-mail outage that they have noticed or something this individual perceives to be an incident, they should take steps to notify Shelby County's Information Technology staff of the issue.

The incident should be reported by anyone who experiences or notices the issue to make sure that it does not go unreported.

e) Procedures:

How to Report Incidents

When reporting incidents, please use one of the following methods:

1. Telephone/Voicemail – call the Service Desk and alert the ITS staff to the issue, if afterhours leave a voicemail and detailed call-back information so someone can get back to you.
2. E-Mail– send an e-mail to the Service Desk so a ticket can be opened to alert ITS staff to the incident, do not send High emails or emails for emergency after-hours issues.

Basic Troubleshooting should be performed prior to calling Service Desk

Employees must first try to resolve software or hardware problems before creating Service Desk issues. This includes rebooting the PC or restarting a program for software problems, or checking cable connections on hardware concerns.

If the problem cannot be resolved, a Service Desk issue must be created documenting all actions taken in an attempt to resolve the problem. A print screen of any error messages must be attached to the issue in order to assist assigned users in determining a resolution.

Information to Include when Reporting Incidents
An incident report should include as much information about what the user noticed as possible. Screen shots should be included where appropriate to best describe the issue and allow the ITS department to work on the issue more quickly.

Employees should also include what they were doing or attempting to do when they noticed the incident. This will help pinpoint the cause of the issue and allow the ITS department to assist in providing alternate steps to the employee to correct the problem where necessary.

Alerting Others of Incidents
When an employee sends an incident report to the ITS department, they should also let others within their own department know of the incident. This will help reduce the number of calls to the Service Desk for assistance with the same incident.

Escalation of Incidents
Once an incident is submitted to the Service Desk it will be worked on in the priority order it has been received. If the item is critical to the function of Shelby County's business, the item will be escalated in priority.
In the event that the user submitting the incident is not satisfied with the level of service they are receiving, a request can be sent to escalate the priority of the ticket. This will move the item to another technician or group of technicians, allowing the priority to be moved up.

Note: Setting a high priority on all incidents submitted will cause them to be looked at in the order they are received. Also remember that setting a high priority when not needed is like "skipping in line".

Additional Information Required
When an incident is submitted to the Service Desk, a technician will review the incident and request further information as needed. The incident will remain open for three days, waiting for more information. If no information is received, the incident will be closed to prevent items from being left open for longer than necessary.

f) Applicability of Other Policies:

This document is part of the Shelby County Government Information Technology Services cohesive set of security policies. Other policies may apply to the topics covered in this document and as such the applicable policies should be reviewed as needed

g) Enforcement:

The Information Technology Services Manager of Customer Service will enforce this policy. Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities are suspected, the county will report such activities to the applicable authorities.

h) Policy Owner:

Shelby County Government

i) Policy Administrator:

Chief Information Officer, Department of Information Technology Services

j) Policy Approval Date:

Current Revision Review Date:			08/91/2016
Current Revision	1.0	Approval Date:	10/10/2014
Original Version	1.0	Approval Date:	11/04/2013

k) Policy Effective Date:

Current Revision	1.0	Approval Date:	10/10/2014
Original Version	1.0	Approval Date:	11/04/2013

l) Terms and Definitions:

Systems (in this context) - an automated process or function made up of multiple computer applications.

4. Service Desk Triage:

a) Purpose:

The details provided within this policy, in the sections that follow, will outline the priorities for the Service Desk staff when top level problems present themselves.

b) Scope:

This policy is designed to provide a guide line to both Service Desk employees and employees in other departments. This policy applies to all Shelby County organizations, employees, and contractors, and any other individuals or organizations that use Shelby County technology resources. Shelby County technology resources include, but are not limited to: networks, servers, data, applications, and information. It applies to all Shelby County facilities.

c) Exceptions

The Shelby County Information Technology Services reserves the right to allow certain exceptions at their discretion.

d) Policy:

Under normal operations, support will be given on a first-come, first-served basis and problems will be solved as soon as possible. However, the following ranking scheme should be used to categorize all requests for assistance. Additional consideration may be given to remote users. The contact and resolution times given below are the ITS department's general guidelines under normal circumstances. During extraordinary situations, such as a natural disaster, prolonged power outage, or other catastrophic events, contact and resolution times may be longer.

e) Procedures:

Priority	Issue	First Contact
1 Emergency	Business Halted - Critical Component(s) down, multiple users affected no work around, time critical.	Immediate—less than 30 minutes
2 High	Business Impacted - Critical component(s) degraded, significant loss of productivity, and one or more users affected no work around, time critical. (Examples: widespread network outage, payroll system, sales system, telecom system, etc.)	1 hour
3 Medium	Non-Critical component(s) down or degraded, One or more users affected, a work around exists, not time critical.	4 hours
4	Non-Critical problem or requirement. Little or No	8.5 hours

Low	impact to business or users. Daily problems that arise and can be worked in the order they were received.	
6 Scheduled	Non-Essential Scheduled work (Examples: Project - office moves, telephone moves, new workstation installation, new equipment/software order, new hardware/software installation, scheduled events)	Scheduled

f) Applicability of Other Policies:

This document is part of the Shelby County Government Information Technology Services cohesive set of security policies. Other policies may apply to the topics covered in this document and as such the applicable policies should be reviewed as needed

g) Enforcement:

The Information Technology Services Manager of Customer Service will enforce this policy. Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities are suspected, the county will report such activities to the applicable authorities.

h) Policy Owner:

Shelby County Government

i) Policy Administrator:

Chief Information Officer, Department of Information Technology Services

j) Policy Approval Date:

Current Revision Review Date: 08/01/2016
Current Revision 1.0 Approval Date: 10/10/2014
Original Version 1.0 Approval Date: 11/04/2013

k) Policy Effective Date:

Current Revision 1.0 Approval Date: 10/10/2014
Original Version 1.0 Approval Date: 11/04/2013

l) Terms and Definitions:

5. Portable Storage Usage

a) Purpose:

Shelby County Government (SCG) Information Technology Services (ITS) has adopted the following policy to reduce the risk of company information being compromised and to address the usage of data stored on portable storage devices. The purpose of this document is to ensure that Sensitive Information is kept securely and safeguarded from unauthorized disclosure, loss or damage.

b) Scope:

This policy applies to all Shelby County organizations, employees, contractors, and any other individuals or organizations that use Shelby County technology resources. It applies to all locations where Shelby County Technology Resources are accessed.

This policy is one component of the comprehensive ITS security plan and must be used in conjunction with all ITS policies including, but not limited to, the Network Security Policy and the Information Security Policy to assure sufficient protection of the data, the end user, and the SCG ITS network.

c) Policy:

It is the policy of SCG to promote the collaboration and remote use of data and information while also maintaining its security. This policy provides guidance for the use of portable storage with SCG Sensitive Information.

d) Procedures:

a. Portable storage devices will be issued to SCG employees as necessary to complete assigned job duties.

b. USB flash drives and portable hard drives that support strong encryption are the only acceptable devices for use with SCG sensitive data and information. Special circumstances requiring the use of portable storage devices which would normally be disallowed must be approved by the ITS Security Officer prior to use.

c. iPods, MP3 players, portable hard drives and USB devices not owned by Shelby County, and other devices with internal or removable storage such as cameras and phones must not contain sensitive SCG data and information.

d. Employees are not permitted to use their personal portable storage devices to store sensitive SCG data and information (including but not limited to PCI and ePHI).

e. All portable devices containing sensitive information will be encrypted utilizing approved encryption technology as required in the SCG "Data Encryption Policy".

f. All portable storage having contained ePHI must be destroyed, disposed of, rendered blank, or reassigned according to Health Services policy HS-217.

g. All staff who utilize portable storage devices shall exercise due diligence to physically and logically safeguard these devices (including but not limited to PCI and ePHI data) used outside of the office.

h. ITS policy prohibits the copying, moving, or storing of PCI cardholder data onto local hard drives and removable electronic media [PCI DSS 12.3.10.a].

i. All removable media must be scanned for viruses while connected to a device on the SCG network.

j. It is not permissible to copy sensitive SCG data from portable media to non-SCG systems or to unapproved media. This includes 3rd party internet or cloud based storage services and mechanisms.

e) Applicability of Other Policies:

This document is part of the Shelby County Government Information Technology Services cohesive set of security policies. Other policies may apply to the topics covered in this document and as such the applicable policies should be reviewed as needed.

f) Enforcement:

The Security Officer will enforce this policy. Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities are suspected, the county will report such activities to the applicable authorities

g) Policy Owner:

Shelby County Government

h) Policy Administrator:

Chief information Officer, Department of Information Technology Services

i) Policy Approval Date:

Current Revision Review Date:			08/01/2016
Current Revision	1.0	Approval Date:	10/10/2014
Original Version	1.0	Approval Date:	08/11/2013

j) Policy Approval Date:

Current Revision	1.0	Approval Date:	10/10/2014
Original Version	1.0	Approval Date:	08/11/2013

k) Compliance:

l) Supporting Forms:

Data Encryption Policy
Network Security Policy
Information Security Policy

Health Services Policy HS-217

m) Definitions:

Portable Storage Devices – Devices which include but are not limited to the following;

- USB flash drives, memory sticks, MP3 players, Secure Digital (SD) cards
- Cellular Phones
- External Hard Drives, Optical Media (CD/DVD/Blu-Ray Discs), Tapes,
- Floppy Discs
- Laptops, Tablets, Personal Digital Assistant (PDAs)

n) Appendices:

6. Scheduled Downtime

a) Purpose:

This policy will describe the outage notification procedures for scheduled downtime requirements for Information Technology Services.

b) Scope:

This policy applies to all IT Services employees, contractors, and any other individuals or organizations that use or maintain Shelby County technology resources not limited to networks, servers, data, applications and information at all Shelby County facilities.

c) Policy:

a) To reduce the effects of scheduled outages, downtime will occur on a weekend or after normal work hours.
b) Maintenance, equipment upgrades or application enhancements affecting response time or access to any portion of the Shelby County information system will be scheduled. Any action that may make a resource unavailable is scheduled.
c) Schedule downtimes with primary customer contacts in an effort to coordinate with them and to make them aware that a specific resource will be unavailable on a given date or dates at a predetermined time prior to sending a Service Outage Announcement.
d) Outage Notifications are sent, as requested by customer contacts, to help reduce support calls about a service that is unavailable in advance.
e) While regularly scheduled downtimes will be used to accommodate all changes and maintenance, additional downtimes may be required. These downtimes will typically be used to implement new equipment or perform extended maintenance to correct an issue needing immediate attention.
f) Employees at Shelby County will be notified via e-mail of an upcoming downtime at least two weeks prior to the outage. Emails will also be sent to all affected employees one week prior to the downtime, and a third and final email will be sent the evening before the downtime.
g) The ITS Staff will also publish a downtime calendar with the dates and times for all downtimes scheduled throughout the year.

d) Procedures:

a) Send a Service Outage Announcement email following the outline below for each Service Outage Type:
   i) Scheduled Maintenance:
      (1) Send a Service Outage Announcement email.
         (a) Email NOC no later than 12:00pm (noon) on the workday before the planned outage. (You may email NOC as early as 4 weeks before a scheduled outage.)
         (b) Address email announcement to:
            NetworkOperationsCenter@shelbycountytn.gov;
            ITEC_CS_LIST@shelbycountytn.gov;
         (c) Use the following as the Subject:

"Notice of Scheduled Maintenance for {Date of outage}"

(d) Use the Format in Exhibit A (Notice of Interruption).

Fill in the information as requested.
State who is the responsible person for this outage.
State who you want NOC to notify.

ii) Service Interruption:

(1) Inform your customers about the outage in the manner defined by the Business Relationship Manager (BRM).

(2) Send a Service Outage Announcement email.

(a) Email NOC after informing your customer.

(b) Address email announcement To:

NetworkOperationsCenter@shelbycountytn.gov;
ITEC_CS_LIST@shelbycountytn.gov;

(c) Use the following as the Subject:

"Notice of Service Interruption for {Date of outage}"

(d) Use the Format in Exhibit A (Notice of Interruption).

Fill in the information as requested.
State who you informed and the manner used.
State who is the responsible person for this outage.
State who you want NOC to notify.

iii) Informational Alert:

(1) Send a Service Outage Announcement email.

(a) Email NOC when the information has been verified.

(b) Address email announcement To:

NetworkOperationsCenter@shelbycountytn.gov;
ITEC_CS_LIST@shelbycountytn.gov;

(c) Use the following as the Subject:

"Notice of Informational Alert"

(d) Use the Format in Exhibit A (Notice of Interruption).

Fill in the information as requested.
State how you verified the information.
State who is the responsible person for this information.
State who you want NOC to notify.

iv) Rescheduling and Canceling Outages

(1) Rescheduling Outages:

(a) Rescheduled outage requests not received by the NOC with 24 hour notice, require you to notify the customer and BRM.

(b) Email NOC with the updated schedule.

(c) Address email announcement To:

NetworkOperationsCenter@shelbycountytn.gov;
ITEC_CS_LIST@shelbycountytn.gov;

(d) Use the following as the Subject:
"Notice of Scheduled Maintenance for {Date of outage}– Update "

(e) Use the Format in Exhibit A (Notice of Interruption).
List scheduling changes in NOC Special Handling section.
Update the outage information.
Phone NOC supervisor and relay changes

(2) Canceling Outage:

(a) Email NOC with the updated schedule.

(b) Address cancelation email announcement To:
NetworkOperationsCenter@shelbycountytn.gov;
ITEC_CS_LIST@shelbycountytn.gov;

(c) Use the following as the Subject:
"Notice of Scheduled Maintenance for {Date of outage} – Canceled "

(d) Use the Format in Exhibit A (Notice of Interruption).
List details in NOC Special Handling section.
Phone NOC supervisor and advise of the cancelation.

b) Network Operations Center responsibility
Based on your Announcement:

i) NOC Supervisor will reject announcements that do not adhere to this policy.
ii) NOC email account will automatically forward your announcement to ITS management and Support persons as defined in the outlook rule based on the email Subject.
iii) NOC will send an email notice to listed users as requested in the announcement.
iv) NOC will send email reminders to the users listed as often as requested in the announcement.
v) NOC will forward appropriate user replies to the responsible person listed in the announcement.

e) Applicability of Other Policies:

This document is part of the Shelby County Government Information Technology Services cohesive set of security policies. Other policies may apply to the topics covered in this document and as such the applicable policies should be reviewed as needed.

f) Enforcement:

The Security Officer will enforce this policy. Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities are suspected, the county will report such activities to the applicable authorities.

g) Policy Owner:
Shelby County Government

h) Policy Approval Date:
Current Revision Review Date: 08/01/2016
Current Revision 1.0 Approval Date: 10/10/2014
Original Version 1.0 Approval Date: 11/06/2012

i) Policy Effective Date:
Current Revision 1.0 Approval Date: 10/10/2014
Original Version 1.0 Approval Date: 11/06/2012

j) Policy Owner:
Information Technology Services Network Operations Center

k) Policy Administrator:
Information Technology Services Administrator

l) Compliance:

m) Supporting Forms:
Notice of Interruption (see Appendix)

n) Definitions:
For the purposes of this policy, unless otherwise stated, the following definitions shall apply:

c) Network Operations Center (NOC): Technical Support group which monitors, reports and tracks service outages and interruptions.
d) Service: An Information Technology Services supported business solution, function or process.
e) Service Outage Types:
   i) Scheduled Maintenance – A planned task or outage of an SLA covered service, scheduled in a manner that provides 24- hour notice, of any maintenance to a service or component that may or may not affect users.
   ii) Service Interruption – An unplanned loss of SLA covered services wherein ITS customers are not afforded 24 hour notice by ITS prior to the interruption regardless of cause.
   iii) Informational Alerts – An alert or warning providing information regarding Phishing, Scams, or General Notice.

o) Appendices:

Exhibit A (Notice of Interruption)

Note: You must notify your users if you are unable to send an Outage Announcement before 12:00pm (noon) on the **workday before** the outage.

Copy the following into a new email and fill in the details.
Each **word in bold type** must remain. Keep the Font Arial, Size 10

Notes to NOC –
Please send on [{date} (and {date})...] [When do you want the notice sent? When do you want a reminder sent?] [any other necessary information] [Customers you contacted]

Send email notice to the following:

Primary Customer Contact email addresses:
List Primary Customer Contact's email address as found in the County's Exchange Global Address-Book. If no individual names are needed, Fill Primary Customer Contacts: with a single Blank Line
(No Commas between first and last name; use Semi-Colons between names)

ITS Support Contact(s) and/or ITS BRM email addresses:
List the ITS Support Contact's email address(s) of those who may want to be notified of this event.
List the email address as found in the County's Exchange Global Address-Book
(No Commas between first and last name; use Semi-Colons between names)

Department Contact email addresses:
If you are not sending this notice to individual Customer Contacts, then list the departments who you want notified as they are listed in the County's Exchange global Address-Book
(No Commas between names; use Semi-Colons between names)
(example HLTHHealthDepartment ; CMSACommunityServicesAgency)

Responsibility:
List the primary and secondary contacts that are responsible for answering all user questions and assuring the outage is successful. Include phone numbers for all provided contacts.

~~~~~~The NOC will Email the following to the customers~~~~~~
~~~~~~

Start Time:
End Time:

User Requirement: Any user-friendly instructions that will assist our users during this outage

7. Software Key Management

a) Policy Intent:

This policy will outline how software installation keys should be kept and managed if they are included with an application purchased by the Shelby County.

b) Scope:

All Shelby County Information Technology Services employees

c) Policy:

The sheer amount of applications used in any organization can be overwhelming. There are applications for everything from infrastructure management to e-mail and financial. All these items will likely have manufacturer-imposed measures to ensure they are legally owned by Shelby County.

The Information Technology Department needs to keep track of all licenses owned of a particular software application that can be handled by an inventory asset policy. Software keys are a bit of a different animal. They should be noted with the application and asset inventory, but access to these keys should be managed separately. This policy will define which employees have access to the software keys and where they should be stored.

d) Procedures:

Storage of Software keys

Software keys should be safely stored. If they are misplaced or leave the organization, they can be very difficult, if not impossible, to recover.

The following requirements for storing keys will be observed:

- Store installation keys separate from installation media
- Keep installation keys in a location that can be locked
- Restrict access to the storage location of the installation keys
- Type the installation keys with the application name to allow for legibility

Access to Installation Keys

The following positions within Shelby County have access to the installation keys and media:

- Information Technology Services managers
- Desktop configuration employees

Misuse of Installation Keys

Installation keys belonging to Shelby County are not to leave the organization. Employees should not use these keys for personal application installations.

e) Applicability of Other Policies:

This document is part of the Shelby County Government Information Technology Services cohesive set of security policies. Other policies may apply to the topics covered in this document and as such the applicable policies should be reviewed as needed.

f) Enforcement:

The Security Officer will enforce this policy. Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities are suspected, the county will report such activities to the applicable authorities.

.

g) Policy Owner:

Shelby County Government

h) Policy Administrator:

Chief Information Officer, Department of Information Technology Services

i) Policy Approval Date:

Current Revision Review Date:			08/01/2016
Current Revision	1.0	Approval Date:	10/10/2014
Original Version	1.0	Approval Date:	11/04/2013

j) Policy Effective Date:

Current Revision	1.0	Approval Date:	10/10/2014
Original Version	1.0	Approval Date:	11/04/2013

k) Compliance:

l) Supporting Forms:

m) Definitions:

n) Appendices:

B. Applications, Software Development and Maintenance

1. Software Installation and Usage

a) Policy Intent:

The purpose of this policy is to address all issues relevant to software installation, deployment and usage on Shelby County's computer systems. This policy is a living document and may be modified at any time.

b) Scope:

This policy is effective for all Shelby County employees and computer systems.

c) Policy:

This policy will set protocol as to how software is to be delivered to better enable Information Technology Services (ITS) to achieve its objective of delivering stable, well-performing technology solutions and insure licensing compliance.

Shelby County will allow the use of specific software applications on equipment that it owns. Only applications needed for County duties and tasks will be installed on its computers.

Shelby County's ITS Division relies on installation and support to provide software and hardware in good operating condition to Shelby County employees so that they can best accomplish their tasks.

d) Procedures:

(1) ***Acceptable use***

This section defines the boundaries for the "acceptable use" of the County's electronic resources, including software, hardware devices, and network systems. Hardware devices, software programs, and network systems purchased and provided by the County are to be used only for creating, researching, and processing County-related materials. By using the County's hardware, software, and network systems, the user assumes personal responsibility for their appropriate use and agrees to comply with this policy and other applicable County policies, as well as city, state, and federal laws and regulations.

All software acquired for or on behalf of the County or developed by County employees or contract personnel on behalf of the County is and shall be deemed County property. All such software must be used in compliance with applicable licenses, notices, contracts, and agreements.

(2) Purchasing

All purchasing of County software shall be centralized with the ITS Division to ensure that all applications conform to corporate software standards and are purchased at the best possible price. The request must be sent to the Information Technology Services Division, which will determine the standard software that best accommodates the desired request. It is then reviewed by ITS before the software is purchased. After sign off form ITS, the request must then be sent to Purchasing for financial approval.

(3) Licensing

Each employee is individually responsible for reading, understanding, and following all applicable licenses, notices, contracts, and agreements for software that he or she uses or seeks to use on County computers. Unless otherwise provided in the applicable license, notice, contract, or agreement, any duplication of copyrighted software, except for backup and archival purposes, may be a violation of federal and state law. In addition to violating such laws, unauthorized duplication of software is a violation of the County's Software/Hardware Policy.

(4) Current Software

(a) The following software standards will apply:**Desktop Operating System (32bit)**

- Microsoft Windows XP
- Microsoft Windows 7 Professional

(b) Productivity tools package

- Microsoft Office 2003, 2007 and 2010 Standard and Professional.
- Word
- Excel
- PowerPoint
- Access (Professional Edition users only)
- Outlook

(c) Financial software

- GEMS

(d) Internet software

- Microsoft Internet Explorer 8.0

(e) Accessories

- WinZip 8.0

- Adobe Acrobat Reader (current approved version)
- Remote Tools for ITS to access desktops
- Trend Micro Antivirus Software

(f) Employees needing software, including these programs listed above must request such software from the Information Technology Services Division. Each request will be considered on a case-by-case basis in conjunction with the software-purchasing section of this policy.

(1) Acceptable Usage

- An ITS-created "image" or OEM installation on the hardware
- An ITS Division installation procedure that provides for the following:
  - Installation options
  - Upgrade considerations (if applicable)
  - Data conversion (if applicable)
- A shortcut to a network application (not truly an installation)
- An automated installation through an ITS-developed solution that may be used in a rapid-deployment scenario or silent-install situation
- A terminal application, Citrix application, or other application

(2) Unacceptable Usage

- An installation not by a procedure
- A piece of software purchased for one's home computer
- A downloaded title from the Internet
- A pirated copy of any title
- A different title from the current software list of this policy
- Any means not covered by the ways that software can exist on County computers
- Any software that is free for personal use

(g) Software licensing

Most of the software titles on Shelby County's current software list are not freeware; therefore, the cost of software is a consideration for most titles and their deployment.
It is the goal of the ITS Division to keep licensing accurate and up to date. To address this, the ITS Division is responsible for purchasing software licenses for the following software categories:

- Desktop operating system software
- Productivity tools package
- Internet software
- Accessories

The other software categories (workgroup-specific titles) are the purchasing responsibility of the workgroup in which they serve. However, the application(s) are still installed and supported by the ITS Division.

To control costs, licensing costs are a factor in the decision-making processes that go into client software planning and request approval.

(h) Software Requests

If a user is to request software for a computer, the proper procedure is to complete the Shelby County support request follow the procedures in the Purchasing Section of this document.

(i) Exceptions:

Any contracted employees that use personal or external County equipment while working with the County. The County reserves the right to allow certain exceptions to the applications outlined herein. These exceptions will be made for business purposes at the discretion of the Shelby County Division of Information Technology Services (ITS).

e) Applicability of Other Policies:

This document is part of the County's cohesive set of security policies. Other policies may apply to the topics covered in this document and as such the applicable policies should be reviewed as needed.

f) Enforcement:

The Security Officer will enforce this policy. Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities are suspected, the county will report such activities to the applicable authorities.

g) Policy Owner:

Shelby County Government

h) Policy Administrator:

Chief Information Officer, Department of Information Technology Services

i) Policy Approval Date:

Current Revision Review Date:			08/01/2016
Current Revision	1.0	Approval date:	10/10/2014
Original Version	1.0	Approval date:	11/04/2014

j) Policy Effective Date:

Current Revision	1.0	Approval date:	10/10/2014
Original Version	1.0	Approval date:	11/04/2014

k) Compliance:

l) Supporting Form(s):

m) Definitions:

n) Appendices:

C. Assets and Inventory

1. Hardware and Software Installation Standards

a) Purpose:

The intent of this policy section is to establish guidelines for the installation, configuration, maintenance, and management of the software and hardware on the Shelby County network.

b) Scope:

This policy applies to all Shelby County organizations, employees, and contractors, and any other individuals or organizations that use Shelby County technology resources. Shelby County technology resources include, but are not limited to: networks, servers, data, applications, and information. It applies to all Shelby County facilities.

c) Policy:

Users and department managers, with the help of the Division of Information Technology Services (ITS), will ensure their software and hardware are in compliance with all license agreements.

All servers and workstations will be configured to ensure the installation of effective security measures via ITS approved images.

Only software authorized by the Division of ITS will be installed on Shelby County computers and communications equipment via ITS approved methods.

All software acquisitions and upgrades will be reviewed by the Division of ITS for verification of available technical support and appropriate security features.

All new software and upgrades must be tested prior to installation in a production environment.

The Division of ITS must approve all servers deployed on Shelby County's network.

Software installed on workstations will comply with the standard software configuration for workstations developed by the Division of ITS.

Users may use only those versions of software licensed to Shelby County and supported by the Division of ITS.

Freeware and shareware will not be downloaded from the Internet or otherwise installed unless approved by the Division of ITS. Software that is free for personal use shall not be installed on Shelby County equipment without proper licensing.

Computers attached to Shelby County's network will have their operating systems configured to fully utilize appropriate security features.

d) Applicability of Other Policies:

This document is part of the County's cohesive set of security policies. Other policies may apply to the topics covered in this document and as such the applicable policies should be reviewed as needed.

e) Enforcement:

The Security Officer will enforce this policy. Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities are suspected, the county will report such activities to the applicable authorities.

f) Policy Owner:

Shelby County Government

g) Policy Administrator:

Chief Information Officer, Department of Information Technology Services

h) Policy Approval Date:

Current Revision Review Date:			08/01/2016
Current Revision	1.0	Approval Date:	10/10/2014
Original Version	1.0	Approval Date:	06/25/2013

i) Policy Effective Date:

Current Revision	1.0	Approval Date:	10/10/2014
Original Version	1.0	Approval Date:	06/25/2013

j) Compliance:

k) Supporting Forms:

l) Definitions:

m) Appendices:

2. Disposal of Obsolete Computer Equipment

a) Purpose:

It is the intent of this policy to define an optimal method of disposing obsolete, broken or damaged computing equipment after all other efforts have been made to use and repurpose equipment.

b) Scope:

This policy applies to all Shelby County organizations, officials, employees, contractors and any other organization using Shelby County's technology resources. Shelby County's technology resources include, but are not limited to networks, servers, data, applications, personal computers, personal digital assistants, tablets, cellular devices, data storage devices, software, printers, telecommunications equipment and digital data. It applies to all Shelby County facilities and any device, software or data that may be owned by the County or connected to a County asset.

c) Policy:

It is the policy of the Division Information Technology Services (ITS) to utilize all computing devices in the most efficient manner possible. All efforts will be given to extend the life and repurpose these devices in order to obtain maximum efficiency and economy. When a computer approaches the end of its useful life, the below procedures will be exercised to attempt to extend its value to the County.

There are three primary ways to dispose of obsolete technology equipment:

1. Repurposed in another Shelby County department
2. Use for spares
3. Transfer the device to Materials Control for disposal

d) Procedures:

1. Repurposed:
   With the assistance of the ITS Staff, a department determines that a computer can no longer be used in that department. The computer will then be transferred to the ITS Division.
   The ITS Staff will remove all programs and data from the device.
2. Use for spares
   When applicable, the ITS Staff will attempt to utilize working computers as spares, for areas that we have a financial responsibility.
   If no individual department has a use for the device, then ITS will place the device in inventory to be deployed as spares. They will be deployed to areas that are not due for an upgrade and have a single system failure.
3. Transfer the device to Materials Control for disposal
   The equipment transferred from the fixed asset accounts, via a fixed asset form, will be declared obsolete equipment and turned over to Materials Control for disposal. (The Fixed asset form will be completed by the requesting Division/Department/Section.)

When all computer components have been exhausted, and it is determined that there is no value the ITS Division, will record the item and turned over to Materials Control for disposal.

Before sending a hard drive to Materials Control for disposal, it must be erased or destroyed as outlined in the Disposal of Media document.

e) Applicability of Other Policies:

This document is part of the Shelby County Government Information Technology Services cohesive set of security policies. Other policies may apply to the topics covered in this document and as such the applicable policies should be reviewed as needed.

f) Enforcement:

The Security Officer will enforce this policy. Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities are suspected, the county will report such activities to the applicable authorities.

g) Policy Owner:

Shelby County Government

h) Policy Administrator:

Chief Information Officer, Department of Information Technology Services

i) Policy Approval Date:

Current Revision Review Date:			08/01/2016
Current Revision	1.0	Approval Date:	10/10/2014
Original Version	1.0	Approval Date:	06/26/2013

j) Policy Effective Date:

Current Revision	1.0	Approval Date:	10/10/2014
Original Version	1.0	Approval Date:	06/26/2013

k) Compliance:

l) Supporting Forms:

m) Definitions:

Computer Equipment – Any technology related equipment such as personal computers, servers, scanners, portable hard drives, flash drives, cellular devices, printers, telecommunications devices, and tablets.

n) Appendices:

3. Disposal of Media

a) Purpose:

This policy will provide a guideline for disposing of the most common types of media.

b) Scope:

This policy applies to all Shelby County organizations, officials, employees, contractors and any other organization using Shelby County's Information Technology Services (ITS) resources. Shelby County's technology resources include, but are not limited to networks, servers, data, applications, personal computers, personal digital assistants, tablets, cellular devices, data storage devices, software and digital data. It applies to all Shelby County facilities and any device, software or data that may be owned by the County or connected to a County asset.

c) Policy:

When disposing of damaged, unusable, or obsolete media, Shelby County ITS requires the guidelines outlined herein to be followed:

d) Procedures:

Hard drives must be completely erased using a DoD 5220.00-M wipe utility to remove all data, or degaussed if unable to access the drive with a PC.
Portable USB drives (flash media) must be destroyed, or erased using a DoD 5220.00-M wipe utility.
Backup media must be erased and properly disposed of.
Compact Disc and DVD media must be shredded, cut up or physically destroyed.
These guidelines protect the Shelby County's data from inadvertent theft or misuse.
No media should be discarded without first removing the data from the media as cleanly as possible. The ITS staff will be responsible for cleaning any data from media to be disposed of.
There are both hardware and software tools available to properly erase hard drives and USB devices before discarding them. These will aid in assuring that no Shelby County data leaves the County during equipment disposal [PCI DSS 9.10.2].

e) Definitions:

DoD 5220.22-M is the Shelby County standard for sanitization to counter data reminisce.

f) Enforcement:

Any employee who fails to comply with the policy and/or procedures may be subject to disciplinary action, up to and including termination of employment.

g) Policy Administrator:

Shelby County Government

h) Policy Administrator:

Chief Information Officer, Department of Information Technology Services

o) Policy Approval Date:

Current Revision Review Date: 08/01/2016
Current Revision 1.0 Approval Date: 07/25/2013
Original Version 1.0 Approval Date: 07/25/2013

p) Policy Effective Date:

Current Revision 1.0 Approval Date: 10/10/2014
Original Version 1.0 Approval Date: 07/25/2013

4. Removal of Property

a) Purpose:

To create a set of guidelines that will document the circumstances under which computer equipment or other property belonging to Shelby County can be removed from County property.

b) Scope:

This policy applies to all Shelby County organizations, employees, and contractors, and any other individuals or organizations that use Shelby County technology resources. Shelby County technology resources include, but are not limited to: networks, servers, data, applications, and information. It applies to all Shelby County facilities.

c) Policy:

Employees of Shelby County will be provided the tools and computer equipment needed to perform the tasks assigned. Based on the requirements of position and discussions with appropriate management, including the employee's direct supervisor, this equipment may be permitted to leave the organization. The following document outlines the equipment that can leave the premises and the equipment that cannot.

d) Procedures:

What Is Allowed to Be Removed from the Property?

Equipment belonging to Shelby County that is portable in nature including but not limited to:

- Laptop computers
- Digital projectors
- Flash drives
- Headphones
- Tablet Computers
- Cellular devices

Other items may also fall into this category. Prior to removing the equipment, you must have it assigned to ITS' inventory tracking system and assigned to the individual or department.

What Is Not Allowed to Be Removed from the Property?

Equipment belonging to Shelby County that is not designed to be portable, including but not limited to:

- Desktop computers
- Monitors
- Desk telephones
- Servers and network equipment

Exceptions:

There may be circumstances that will allow certain non-portable items to be taken off site, for example a multi-day training being held at a conference center to minimize distraction while training employees. For these types of circumstances, the ITS department and the employee's direct supervisor must be consulted.

e) Applicability of Other Policies:

This document is part of the Shelby County Government Information Technology Services cohesive set of security policies. Other policies may apply to the topics covered in this document and as such the applicable policies should be reviewed as needed.

f) Enforcement:

The Security Officer will enforce this policy. Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities are suspected, the county will report such activities to the applicable authorities.

g) Policy Owner:

Shelby County Government

h) Policy Administrator:

Chief Information Officer, Department of Information Technology Services

i) Policy Approval Date:

Current Revision Review Date:			08/01/2016
Current Revision	1.0	Approval Date:	10/10/2014
Original Version	1.0	Approval Date:	11/04/2013

j) Policy Effective Date:

Current Revision	1.0	Approval Date:	10/10/2014
Original Version	1.0	Approval Date:	11/04/2013

k) Compliance:

l) Supporting Forms:

m) Definitions:

n) Appendices:

D. Backup, Recovery, Data Retention, Archiving

1. Data Classification Policy

a) Policy Intent:

Shelby County Government (SCG) has adopted the following Data Classification Policy to establish guidelines for data classification and risk mitigation. The practical intent of this policy is to establish a layered framework to secure the SCG's data.

b) Scope:

The scope of this policy covers all Shelby County Government data stored on county-owned, county-leased, and otherwise county-provided systems and media, regardless of location. Also covered by the policy are hardcopies of county data, such as printouts, faxes, notes, microfilm or microfiche.

c) Policy:

This policy provides a method for classifying and handling data. Information assets are assets to SCG just like physical property. In order to determine the value of the asset and how it should be handled, data must be classified according to its importance to county operations and the confidentiality of its contents. Once this has been determined, the county can take steps to ensure that data is treated appropriately.

Physical records containing PAN will be securely stored, limiting access to them, prior to physical destruction according to the Data Destruction requirements section [PCI DSS 9.10.1.b].

d) Data Classification Procedure:

Data residing on county systems must be continually evaluated and classified into the following categories [PCI DSS 9.7.1]:

(1) Personal: includes user's personal data, emails, documents, etc. This policy excludes personal information, so no further guidelines apply.

(2) Public: includes already-released material, commonly known information, classified and handled in accordance with County Technical Assistance Service (CTAS) Manual and Data Retention Schedule. Public information can and often does include information of other classifications including "Confidential". Please see Data Retention Policy and Stored Cardholder Data Policy for more detailed information about how to handle Public Information.

(3) Operational: includes data for basic county business operations, communications with vendors, employees, etc. (non-confidential). The majority of data will fall into this category.

(4) Critical: any information deemed critical to county business operations (often this data is operational or confidential as well). It is extremely important to identify critical data for security and backup purposes.

(5) Confidential: any information deemed "sensitive" or proprietary to county business, including but not limited to protected health information (PHI) and Credit Cardholder Data (CHD). See the Data Retention Policy and Stored Cardholder Data Policy for more detailed information about how to handle confidential data.

e) Data Storage Procedure:

The following guidelines apply to storage of the different types of county data [PCI DSS 9.9].

(1) Personal - There are no requirements for personal information.

(2) Public - Public information can and often does include information of other classifications including "Confidential". Please see Stored Cardholder Data Policy for more detailed information about how to handle Public Information containing Cardholder Data (CHD).

(3) Operational - Operational data must be stored where the backup schedule is appropriate to the importance of the data, at the discretion of the user.

(4) Critical - Critical data must be stored on a server that gets the most frequent backups (refer to the Backup Policy for additional information). System- or disk-level redundancy is required.

(5) Confidential - Confidential information must be removed from desks, computer screens, and common areas unless it is currently in use. Confidential information should be stored under lock and key (or keycard/keypad), with the key, keycard, or code secured. Confidential information containing Credit Cardholder Data (CHD) is to be secured in accordance with County Stored Cardholder Data Policy.

f) Data Transmission Procedure:

The following guidelines apply to transmission of the different types of company data.

(1) Personal - There are no requirements for personal information.

(2) Public - Public information can and often does include information of other classifications including "Confidential". Please see Media Control Policy for more detailed information about how to handle Public Information media containing Cardholder Data (CHD).

(3) Operational - No specific requirements apply to transmission of Operational Data, however, as a general rule, the data should not be transmitted unless necessary for county business purposes.

(4) Critical - There are no requirements on transmission of critical data, unless the data in question is also considered operational or confidential, in which case the applicable policy statements would apply.

(5) Confidential - Strong encryption must be used when transmitting confidential data electronically, regardless of whether such transmission takes place inside or outside the county's network. Confidential data must not be left on voicemail or text messaging systems, either inside or outside the county's network, or otherwise recorded. Physical media containing confidential data must be transported within a locked container, and "Media Removal Log" form must be signed and dated and destination noted by person receiving media as stated in Media Control Policy [PCI DSS 4.1.d / 9.7.1].

g) Data Destruction:

The following guidelines apply to the destruction of the different types of county data [PCI DSS 9.10].

(1) Personal - There are no requirements for personal information.

(2) Public - Data classified as "Public Record" must be reviewed and approved for destruction by the Public Records Commission in accordance with Records Manual set

forth by Tennessee State Library and Archives (TLSA) and County Technical Assistance Service (CTAS). Public information containing Confidential Data is destroyed as noted below, and in accordance with Periodic Media Destruction Policy, once approval for destruction is acquired.

(3) Operational - Cross-cut shredding is required for paper documents [PCI DSS 9.10.1.a]. Storage media should be appropriately sanitized/wiped or destroyed [PCI DSS 3.1.1.c] [PCI DSS 9.10.2].

(4) Critical - There are no requirements for the destruction of Critical Data, though shredding is encouraged. If the data in question is also considered operational or confidential, the applicable policy statements would apply.

(5) Confidential - Confidential data must be destroyed in a manner that makes recovery of the information impossible. For destruction of media containing confidential data in accordance with Media Destruction Policy, the following guidelines apply [PCI DSS 9.10.1.a]:

(i) Paper/documents: cross cut shredding is required [PCI DSS 9.10.1.a].

(ii) Storage media (CD's, DVD's, USB Flash Drives): physical destruction is required [PCI DSS 9.10.2].

(iii) Hard Drives/Systems/Mobile Storage Media: where sanitizing / wiping of media to DoD Standards cannot be done, physical destruction is required. If physical destruction is not possible, the Security Officer must be notified [PCI DSS 9.10.2].

h) Applicability of Other Policies:

This document is part of the Shelby County Government Information Technology Services cohesive set of security policies. Other policies may apply to the topics covered in this document and as such the applicable policies should be reviewed as needed.

i) Enforcement:

The Security Officer will enforce this policy. Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities are suspected, the county will report such activities to the applicable authorities.

j) Policy Owner:

Shelby County Government

k) Policy Administrator:

Chief Information Officer, Department of Information Technology Services

l) Policy Approval Date:

Current Revision Review Date:			08/01/2016
Current Revision	1.0	Approval date:	10/10/2014
Original Version	1.0	Approval date:	11/04/2013

m) Policy Effective Date:

Current Revision	1.0	Approval date:	10/10/2014
Original Version	1.0	Approval date:	11/04/2013

n) Compliance:

PCI DSS Requirement 3.1
PCI DSS Requirement 8.5.15
PCI DSS Requirement 9.7.1
PCI DSS Requirement 9.10
PCI DSS Requirement 9.10.2

o) Supporting Forms:

Media Removal Log

p) Definitions:

(1) Authentication - A security method used to verify the identity of a user and authorize access to a system or network.

(2) Backup - To copy data to a second location, solely for the purpose of recovery of that data.

(3) Encryption - The process of encoding data with an algorithm so that it is unintelligible without the key. Used to protect data during transmission or while stored.

(4) Mobile Data Device - A data storage device that utilizes flash memory to store data. Often called a USB drive, flash drive, or thumb drive.

(5) Two-Factor Authentication - A means of authenticating a user that utilizes two methods: something the user has, and something the user knows. Examples are smart cards, tokens, or biometrics, in combination with a password.

(6) U.S. DoD Standards - Stands for United States Department of Defense Standards. Standards on data destruction detailed in DoD 5220.22-M. Most data wiping software packages provide an option for wiping to this standard.

q) Appendices:

2. Data Retention Policy

a) Policy Intent:

Shelby County Government (SCG) has adopted the following Data Retention Policy to be utilized by Shelby County Government for the retention of different classifications and types of data. SCG strives, through the guidelines in this policy to, minimize the cost of data retention, adhere to data retention and compliance requirements of applicable state and federal regulations, support SCG business interests, and provide for the maintenance of data as required to support SCG legal interests.

b) Scope:

This policy applies to all Shelby County employees accessing data on Shelby County systems, and to all data stored on county-owned, county-leased, or county-provided systems and media, regardless of type of media, type of data, or location of data. Certain data retention requirements can be mandated by local, industry, state, or federal regulations. Where this policy differs from applicable regulations, the policies specified in the regulations will apply.

c) Policy:

It is the policy of SCG to provide the following minimum data retention for data types defined within this policy. Locations containing CHD will be scanned on at least a quarterly basis and any CHD identified exceeding retention requirements will be removed [PCI DSS 3.1.1.d]. Data retention and destruction will be achieved according to the "SCG ITS Data Retention and Disposal Procedures".

d) Reasons for Data Retention:

It is the policy of Shelby County Government to minimize the cost of data retention with its business need; therefore the Shelby County Government retains data only for the duration of the valid business or legal need of the data, and deletes the data once it is no longer required [PCI DSS 3.1.1.b]. Some data however must be kept in order to protect Shelby County Government's business interests, comply with applicable local, state, and federal regulations, and preserve evidence in the case of litigation [PCI DSS 3.1.1.a]. Archives section of County Register maintains a current Records Retention Schedule as part of the Records Manual set forth by Tennessee State Library and Archives (TLSA) and County Technical Assistance Service (CTAS) in accordance with Tennessee Code.

e) Data Duplication:

It is the policy of Shelby County Government to minimize the duplication of data during identification and classification. Owners and users of the data are to understand that this policy applies to all duplicates of the information as well as the original, regardless of data type, media, or location.

f) Retention Requirements:

The following are guidelines for the minimum retention of data based upon data classification set forth in the Shelby County Data Retention Policy.

(1) Personal - There are no retention requirements for personal data. In fact, Shelby County Government encourages that it be deleted or destroyed when it is no longer needed.

(2) Public - Information classified as "Public Record" is retained in accordance with current Records Retention Schedule in the Records Manual set forth by Tennessee State Library and Archives (TLSA) and County Technical Assistance Service (CTAS).

(3) Operational - Operational data must be retained in accordance with the current Records Retention Schedule in the Records Manual set forth by Tennessee State Library and Archives (TLSA) and County Technical Assistance Service (CTAS). This includes check or credit card transaction data, but does not include cardholder data (see Confidential).

(4) Critical - Critical data must be retained in accordance with the current Records Retention Schedule with a minimum of three months immediately available for analysis (for example, online, archived, or restorable from backup).

(5) Confidential - Confidential data must be retained in accordance with the current Records Retention Schedule with a minimum of three months immediately available for analysis (for example, online, archived, or restorable from backup). Where confidential data contains ePHI, the data is retained for 9 years in accordance with Shelby County HIPAA policy. Where confidential data contains credit cardholder data (CHD), the data is retained only as long as needed by the processing organization, and then is permanently deleted immediately [PCI DSS 3.1.1.e]. Confidential data containing cardholder data is reviewed quarterly to ensure cardholder data does not exceed retention requirements [PCI DSS 3.1.1.d].

g) Protection Requirements:

The following are guidelines for the minimum protection measures for data based upon data classification set forth in the Shelby County Data Retention Policy.

(1) Personal - Personal data is protected for individual view and use of the owner of the data by means of file system access control measures in accordance with Shelby County Network Security Policy. Personal data is not backed up by Shelby County ITS.

(2) Public - Information classified as "Public Record" is to be made available to the public in accordance with "Open Records" laws, however confidential information including but not limited to Credit Card Primary Account Numbers (PAN), and Social Security Numbers (SSN), should be masked when redacting the documents for public review. Public information is backed up to ensure data retention values in accordance with current Records Retention Schedule in the Records Manual set forth by Tennessee State Library and Archives (TLSA) and County Technical Assistance Service (CTAS), and to ensure the Recover Point Objectives (RPO) and Recover Time Objectives (RTO) established in the Shelby County Business Continuity Plan.

(3) Operational - Operational data is protected for use of the owning department or departments by means of file system access control measures in accordance with Shelby County Network Security Policy. Operational data is backed up daily to ensure data retention values in accordance with current Records Retention Schedule, and to ensure the Recover Point Objectives (RPO) and Recover Time Objectives (RTO) established in the Shelby County Business Continuity Plan.

(4) Critical - Critical data is protected for use of the owning department or departments by means of file system access control measures, and such access is audited and reported in accordance with Shelby County Network Security Policy. Critical data is backed up daily to ensure data retention values in accordance with current Records Retention Schedule, and to ensure the Recover Point Objectives (RPO) and Recover Time Objectives (RTO) established in the Shelby County Business Continuity Plan.

(5) Confidential - Confidential data is protected for use of the owning department or departments by means of strong encryption and file system access control measures, and such access is audited and reported in accordance with Shelby County Network Security Policy. Confidential data is backed up daily to ensure data retention values in

accordance with current Records Retention Schedule, and to ensure the Recover Point Objectives (RPO) and Recover Time Objectives (RTO) established in the Shelby County Business Continuity Plan. Where confidential data contains CHD, the backup copies of the data are purged at the end of the retention period in accordance with Periodic Media Destruction Policy [PCI DSS 3.1.1.e].

h) Retention of Encrypted Data:

Confidential data retained under this policy is stored in encrypted format. Encryption keys are archived, stored, renewed, revoked, and maintained in accordance with the Shelby County Network Security Policy. Encryption keys and Recovery Agent keys are retained as long as the data that the keys decrypt is retained [PCI DSS 3.6.a / 3.6.b / 3.6.c / 3.6.1 / 3.6.2 / 3.6.3 / 3.6.4 / 3.6.5 / 3.6.6 / 3.6.7 / 3.6.8].

i) Data Destruction:

(1) Data of all classifications covered by Records Retention Schedule in the Records Manual is destroyed only with approval of Public Records Commission in accordance with Tennessee Code Annotated (TCA) 10-7-404(a).

(2) Credit cardholder data (CHD) is destroyed in accordance with the Shelby County Data Retention Policy and Periodic Media Destruction Policy and Procedures so that the data cannot be recovered [PCI DSS 3.1.1.e]. When the retention timeframe expires, the department must actively destroy the data covered by this policy.

(3) If a user feels that certain data should not be destroyed, he or she should identify the data to his or her supervisor so that an exception to the policy can be considered. Since this decision has long-term legal implications, exceptions are subject to approval of Chief Information Officer (CIO) and Chief Administrative Officer (CAO) will approve exceptions.

(4) Shelby County Government specifically directs users not to destroy data in violation of this policy. Particularly forbidden is destroying data that a user may feel is harmful to himself or herself, or destroying data in an attempt to cover up a violation of law or county policy.

j) Exceptions to Policy:

Data retention, regardless of classification, is changed under the following standing exceptions and within the following guidelines:

(5) Litigation Hold - Upon receipt of notice of litigation hold from the County Attorney, the retention of all data listed in the litigation hold notice is to be changed to "Permanent". The retention change applies to the listed data in all forms, locations, and including backup copies. The requested data is to be quarantined, identified as "litigation hold", and maintained in a read-only state for the duration of the active hold. The data may return to normal retention upon notice that the case is no longer active.

(6) Administrative Hold - Upon receipt of notice of administrative hold from Chief Information Officer (CIO) or Chief Administrative Officer (CAO), the retention of all data listed in the administrative hold notice is to be changed to "Permanent". The retention change applies to the listed data in all forms, locations, and including backup copies. The requested data is to be quarantined, identified as "administrative hold", and maintained in a read-only state for the duration of the active hold. The data may return to normal retention upon notice that the case is no longer active.

(7) Service Level Agreement – Upon establishment through the Service Level Agreement between SCG ITS and the SCG Business Unit, the retention of specifically identified data may be increased. Minimum retention and protection periods may not be changed and will be enforced for all data. All SLA-based retention changes apply to the listed data in all forms and locations including, but not limited to, backup copies and servers as identified by the client and ITS.

k) Applicability of Other Policies:

This document is part of the Shelby County Government Information Technology Services cohesive set of security policies. Other policies may apply to the topics covered in this document and as such the applicable policies should be reviewed as needed.

l) Enforcement:

The Chief Security Officer (CSO) will enforce this policy. Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities are suspected, the company will report such activities to the applicable authorities. The data custodian for each department will review the department's data at least quarterly for relevancy and value.

m) Policy Owner:

Shelby County Government

n) Policy Administrator:

Chief Information Officer, Department of Information Technology Services

o) Policy Approval Date:

Current Revision Review Date:			08/01/2016
Current Revision	1.0	Approval date:	07/05/2014
Original Version	1.0	Approval date:	07/05/2013

p) Policy Effective Date:

Current Revision	1.0	Effective Date:	07/05/2014
Original Version	1.0	Effective Date:	07/05/2013

q) Supporting Form(s):

SCG ITS Data Retention and Disposal Procedures [PCI DSS 3.1.1.b] [PCI DSS 3.1.1.c] [PCI DSS 3.1.1.d]

r) Compliance:

PCI DSS Requirements 3.1.1, 3.6
Health Insurance Portability and Accountability Act of 1996 (HIPAA)
Privacy Act of 1974, 5 U.S.C. § 552a

s) Supporting Forms:

t) Definitions:

The following terms are used throughout this document as defined below:

(1) Backup: To copy data to a second location, solely for the purpose of safe keeping of that data.

(2) Cardholder Data: PCI DSS defines cardholder data (CHD) as full data contained on the magnetic stripe of the credit card including Primary Account Number (PAN), expiration date, security code or card validation code (CVC), cardholder name.

(3) Media: Material containing the data (e.g. fixed or removable magnetic or optical disk, non-volatile memory or flash drive, paper, microfiche, magnetic tape).

(4) Encryption: The process of encoding data with an algorithm so that it is unintelligible and secure without the key. Used to protect data during transmission or while stored.

(5) Strong Encryption is a process of encrypting data using a key with an algorithm and key length that is highly resistant to re-creation of the key for decryption purposes.

(6) Encryption Key: An alphanumeric series of characters that enables data to be encrypted and decrypted.

(7) Recover Point Objective (RPO): The point in time to which data and/or the systems on which the data resides are to be returned to availability or functionality.

(8) Recover Time Objective (RTO): The elapsed time within which the data and/or the systems on which the data resides are to be returned to availability or functionality.

u) Appendices:

E. Internet and Email Usage

1. Download Media and Streaming

a) Policy Intent:

The intent of this policy is to provide an approved guideline for downloading and streaming media from the internet. It will let employees know which applications are acceptable, which are not, and what to do if they are unsure.

b) Scope:

This policy applies to all Shelby County organizations, employees, and contractors, and any other individuals or organizations that use Shelby County technology resources. Shelby County technology resources include, but are not limited to: networks, servers, data, applications, and information. It applies to all Shelby County facilities.

c) Policy:

This policy has been established to set guidelines in an effort to clarify the type and nature of files that employees are allowed to download from third-party sources onto their local computers (desktops, laptops, Pocket PCs, Tablet PCs, tablet, and cellular phones). Although it would be impossible to name every executable or download file in this policy, users should adhere to these guidelines:

- The download enhances the employee's productivity.
- The download is from a reputable source.
- The file does not subject Shelby County to potential liability.
- The application, tool, or template has been approved by ITS.

Remote workers who access network resources using their own equipment will be required to maintain the applications that are installed on their computers.

An Internet Service Provider (ISP) can attach to Shelby County's network only with the approval of the Department of Information Technology Services.

Access to the Internet is provided to accommodate County business. Limited personal use is not inherently a violation of this policy, provided such use may be restricted or terminated by a supervisor for abuse, or for jeopardizing the security of Shelby County's computing environment.

Internet access from Shelby County's network will be granted only to individuals whose Supervisor completes a request for access.

All inbound and outbound Internet traffic will go through a web-access server maintained by the ITS department.

Bypassing the proxy server is not permitted, except by approval of the ITS Department. Users who are authorized to bypass the web-access server should do so only for those operations for which they were granted approval to bypass the web-access server.

Inappropriate web sites will be blocked from access. Examples include pornography, gambling, and entertainment.

Internet usage that poses a security threat will be blocked. Examples of such usage may include instant messaging, peer-to-peer, and public email.

Spyware and other stealth information gathering programs should not be knowingly installed on networked workstations, and will be blocked from Internet access.

d) Procedures:

Please note, this list is subject to change at any time.

Approved download guideline – for You Tube and similar downloads

The following is a list of files that employees can download onto their local machines.

The user will submit the links to the media needed via the original request (for example, a training video from You Tube).

The media will be downloaded and provided to the user if there is no copyright violation (user has to verify via due diligence).

The mechanism used to download the media from the Internet will not be provided to the user (i.e. video-downloader add-on, etc.)

As an alternative, the user is welcome to use an embedded link to access the content.

Prohibited downloads

The following downloads are not allowed on County computer resources unless approved by ITS.

Any third-party screen saver or wallpaper

Use of 3rd party screensavers, wallpapers, and screensaver managers are prohibited. These applications or wallpaper may display images that are deemed offensive by other staff members. They also may contain Malware, Adware, Trojans, or other infections that will negatively affect PC performance. Employees will use the default screen savers available on their computers. Additionally, most of the screen saver/screen saver managers available on the Internet are "Free for personal/private use". Use on a Shelby County computer violates the "free for personal/private use agreement" by installing them on corporate machines.

Games

Games provide no benefit to our organization and have a tendency to affect productivity. Games are not allowed on County machines. Additionally, online and

Internet-based games, whether requiring a download or not, are not permitted to be played on SCG machines.

.EXE files
These are prohibited because they are prone to have viruses and malware embedded in them. Once viruses and malware are installed on a County machine it will drastically affect productivity and can cause other machines on the network to be effected.

Tool Bars
Third party toolbars may contain popup blockers and/or other functions contrary to our normal operations. Many of our required applications may not function properly with these toolbars installed. They also may contain Malware, Adware, Trojans, or other infections that will negatively affect PC performance. Installation of 3rd party toolbars is prohibited.
*** If an approved application is downloaded from the internet, the user must make sure that there is not a box agreeing for installation of a particular toolbar. This is the practice of many software companies.*

Browsers
Internet Explorer is the browser that SC ITS supports. Other 3rd party browsers are "NOT SUPPORTED", but have been allowed to be installed an many cases. Almost all of your techs use Chrome and/or Firefox for several applications, but IE is still the application of choice. Other 3rd party browsers do not integrate with our management tools (SCCM, Group Policies, etc.) and do not allow SC ITS to control the way they function. Security holes, violations of policy and application lockups/malfunctions are more likely with these browsers.

iTunes
iTunes is not an allowed application for SC users but is authorized for users with SC purchased/provided iPhones or iPads only.

Personal Pictures and Music
Personal pictures and music provide no benefit to our organization and have a tendency to affect productivity, they are not allowed on County machines.
They also consume vital space on the computer that could affect the efficiency of the PC.

Additional Questions
As this document grows and changes for your organization, continue to bring any questions you may have to ITS. Also, if there is an application that you feel should be added to this list, suggest the change to ITS.

e) Applicability of Other Policies:

This document is part of the Shelby County Government Information Technology Services cohesive set of security policies. Other policies may apply to the topics covered in this document and as such the applicable policies should be reviewed as needed.

f) Enforcement:

The Security Officer will enforce this policy. Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties

up to and including termination of employment. Where illegal activities are suspected, the county will report such activities to the applicable authorities.

g) Policy Owner:

Shelby County Government

h) Policy Administrator:

Chief Information Officer, Department of Information Technology Services

i) Policy Approval Date:

Current Revision Review Date:			08/01/2016
Current Revision	1.0	Approval Date:	08/11/2014
Original Version	1.0	Approval Date:	11/04/2013

j) Policy Effective Date:

Current Revision	1.0	Approval Date:	08/11/2014
Original Version	1.0	Approval Date:	11/04/2013

k) Compliance:

l) Supporting Forms:

m) Definitions:

Internet Service Provider - a County who provides the connection that allows a person or organization to access the Internet.

Web-access server – a device or program which communications with the Internet on behalf of users, generally providing increased security.

Spyware – any technology that aids in gathering information about a person or organization without their knowledge. On the Internet, it is used to secretly gather information about the user and relay it to advertisers or other interested parties.

Stealth – computer programs that operate without the knowledge of the computer user. Many spyware programs operate in a stealth mode.

Downloads - to transfer (software, data, character sets, etc.) from a distant to a nearby computer, from a larger to a smaller computer, or from a computer to a peripheral device either via transfer or streaming media.

n) Appendices:

2. Email and Digital Document Searches

a) Policy Intent:

The purpose of this policy is to ensure that proper procedures be followed for searching an employee's documents or emails. This policy is not intended to otherwise restrict management's authority to view an employee's electronic communications or other data used on County equipment and systems.

b) Scope:

This policy applies to all Shelby County organizations, employees, and contractors, and any other individuals or organizations that use Shelby County technology resources. Shelby County technology resources include, but are not limited to: networks, servers, data, applications, and information. It applies to all Shelby County facilities.

c) Policy:

To assure the propriety of email record requests and to avoid unnecessary loss of ITS staff time, it is the policy of the Shelby County Department of Information Technology Services to only search employees' emails when written requests originate with the County Attorney or, the Office or Department's Elected Official, Director, Deputy Director, Administrator, or the County's CAO, or Deputy CAO are received sanctioning the search.

d) Procedures:

Searches will be made, based on the requests of the County Attorney, for many reasons, below are a few:

- Request from a Department Head, based on just cause, as determined by the County Attorney
- Sending emails with any libelous, defamatory, offensive, racist or obscene remarks
- Forwarding emails with any libelous, defamatory, offensive, racist or obscene remarks.
- If you unlawfully forward confidential information.
- If you unlawfully forward or copy messages without permission
- To fulfill a subpoena request.
- An unauthorized mass mailing
- Conducting unlawful activities
- If there is evidence that you are not adhering to the guidelines set out in the Email Use and Accountability Policy

A Department Head should contact the County Attorney to discuss if there is a just cause to search an individual's email or documents. The County Attorney will determine the justification of a search. If it is determined that there is justification, then the County Attorney will forward the request, in writing, to the ITS Department Head for processing. ITS staff will perform the search quickly and discretely, track time and expenses for the search, and provide a copy of the results of a search to the County Attorney on removable electronic media. ITS procedure is as follows:

- Create work order to track time and effort for the request
- Using GFI MailArchiver Bulk Export tool, enter the search criteria and perform the searches, saving the resulting emails to PST files in temporary folder on C: drive.

e) Applicability of Other Policies:

This document is part of the Shelby County Government Information Technology Services cohesive set of security policies. Other policies may apply to the topics covered in this document and as such the applicable policies should be reviewed as needed

f) Enforcement:

The Security Officer will enforce this policy. Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities are suspected, the county will report such activities to the applicable authorities.

g) Policy Owner:

Shelby County ITS

h) Policy Administrator:

CIO, Department of Information Technology Services

i) Policy Approval Date:

Current Revision Review Date:			08/01/2016
Current Revision	1.1	Approval date:	10/03/2014
Original Version	1.0	Approval date:	08/03/2013

j) Policy Effective Date:

Current Revision	1.1	Effective Date:	10/03/2014
Original Version	1.0	Effective Date:	08/03/2013

k) Compliance:

l) Supporting Forms:

m) Terms and Definitions:

n) Appendices:

3. Email Use and Accountability

a) Policy Intent:

The purpose of this policy is to ensure the proper use of the Shelby County Government (SCG) Electronic Messaging System (email) and that applicable procedures and guidelines are adhered to. This policy is not intended to otherwise restrict management's authority to view an employee's electronic communications or other data used on County equipment and systems.

b) Scope:

This policy applies to all SCG organizations, employees, contractors, and any other individuals or organizations using SCG technology resources. SCG technology resources include, but are not limited to: networks, servers, data, applications, and information. It applies to all SCG facilities.

c) Policy:

It is the policy of the SCG Information Technology Services (ITS) Department to administer, protect and secure the SCG Electronic Messaging Systems as follows:

(a) ITS maintains Electronic Messaging Data retention for at least five (5) calendar years in accordance with Public Records Commission Retention Schedule, # 15-014, CTAS Manual.

(i) Every Electronic Mail Message sent or received by SCG email addresses in the County Electronic Messaging System is copied into an archive, and kept for at least five (5) calendar years.

(ii) Upon receipt of notification of Litigation Hold or Administrative Hold, ITS extends the retention value to "Permanent" for all pertinent Electronic Messaging Records and all media containing all pertinent Electronic Messaging Records. Retention reverts back to five (5) calendar years at the end of the Litigation Hold or Administrative Hold.

(iii) ITS provides, upon written request by the County Attorney or, the Office or Department's Elected Official, Director, Deputy Director, Administrator, or the County's CAO, or Deputy CAO, sanctioning the export, copies of email records meeting search criteria specifically pertinent to the request

(iv) ITS provides upon, written request by Department Administrator or County Attorney, for the expressed purposes of Open Records, Legal or Administrative Discovery, exported copies of email records meeting search criteria specifically pertinent to the request.

(b) ITS secures access to Electronic Messaging Data through use of SCG-provided logon ID and password, the use of Secure Socket Layer (SSL) or Transport Layer Security (TLS) certificate for access and transmission of Electronic Messages.

(i) Web and Mobile access to Electronic Message System requires use of SSL.

(ii) Use of User Certificate or Public/Private Key to encrypt or digitally sign Electronic Messages requires authorization by ITS Administrator.

(iii) Users may only access their own email messages unless explicitly permitted by ITS Administrator.

(c) ITS enforces the SCG Acceptable Use Policy and "Electronic Media Communication Policy" in Personnel Management System Policy HR-318 as pertains to Electronic Messaging Systems.

(d) ITS employs limitations on the Electronic Messaging System to ensure Data Leakage Prevention (DLP), Information Security, and Messaging System serviceability.

(i) Total message size (message body plus sum of all attachments) is limited to 50MB.

(ii) Total mailbox size (including all messages, folders, attachments, appointments, tasks, and notes) is limited as follows with the following size increase authorities:

- 50MB Initial mailbox size
- 250MB Manager approval
- 500MB Department Administrator approval
- 1GB Division Director approval
- 2GB or larger CIO / CAO approval

(iii) Sensitive Information, including but not limited to Social Security Numbers (SSN), Electronic Protected Health Information (EPHI), and Credit Cardholder Data (CHD), must be encrypted to be sent.

(iv) Mailbox Store databases will be periodically serviced to ensure their total size does not exceed the Microsoft recommendation of 32GB.

(v) Electronic Mail messages sent to or from the Electronic Messaging System are scanned for viruses and harmful content, SPAM, and Phishing Scams, and resulting positive detected email messages are cleaned, quarantined, or prevented from entering the system.

d) Procedures:

The following procedures implement the policy above.

(1) Establish and maintain Electronic Messaging Data Retention

(i) GFI MailArchiver application uses MS Exchange Journal account "Journal.01" to archive each message

- Logged into GFI MailArchiver application as Administrator, navigate browser to "Configuration" tab > "Mail Servers to Archive"
- Ensure "Journal.01" journaling mailbox is Active (has green check mark) and points to Mailbox server "SCANTMSE01.shelby.enet" using IMAP Connection Type.

(ii) GFI MailArchiver application is configured for at least two (2) calendar years of data "On-Line"

- Logged into GFI MailArchiver application as Administrator, navigate browser to "Configuration" tab > "Archive Stores"
- Ensure "Archive Stores" database listing (displays oldest at top) shows all monthly archive databases dating back to at least two calendar years before current month, and that Indexing column shows "green checkmarks" and Status column shows "Online".

(iii) If no "Legal Hold" or "Administrative Hold" in place, Network Administrator submits request for records destruction for records older than five (5) calendar years previous to the current Public Records Commission meeting, held twice yearly in April and October.

- Requested date range on quarter boundaries beyond the 5 years.
- Cite "Continuing Approval" established on request "2011-002".
- Acquire ITS Administrator signature.

(iv) Upon receipt of valid Open Records, Legal or Administrative Discovery Request, Network Administrator exports records meeting search criteria to PST files presented to the requestor on CD-R or DVD-R.

- Search Criteria should be used to narrow the search to specific date range with specific text to or from specific email addresses.
- Network Administrator uses GFI Bulk Export tool to perform the targeted extract of records to PST files.
- PST files are copied to County Attorney Folder structure at \\SCFNTNAS3\VOL1\ATTY\Data Exports for redaction if necessary.

- PST files are copied in un-redacted form to CD-R or DVD-R and kept in file drawer.
- Upon notice of completion of redaction, resulting PST files are copied to "Delivery" set of CD-R or DVD-R for the requester, and copied to "File" set of CD-R or DVD-R and kept in file drawer.

(v) Secure access to Electronic Messaging System

- Network Administrator provides user's ADS logon name and password.
- SSL/TLS Certificates for each Exchange server are installed and TLS is enabled for the "Connectors" under "Administrative Groups > "First Administrative Group" > "Routing Groups" in Exchange System Manager.
- SSL/TLS Certificates for each Exchange Front-end server are installed and SSL is enabled and required for default website.
- Users utilize https://webmail.shelbycountytn.gov/exchange for web access and specify "Use SSL" or "Use Secure Connection" for mobile access.

(2) Enforce Acceptable Use and Electronic Communications policies

(3) Ensure Messaging Data Protection and Messaging System Serviceability

(i) Network Administrator employs anti-virus, anti-spam, and data leak prevention measures.

- Ensure the SMTP Gateway in the DMZ is configured to send and receive with MS Exchange bridgehead server SCANTMSE01 and with TrendMicro Hosted Email Security Service for Anti-Virus and Anti-Spam.
- Ensure correct DNS "A" records, "PTR" records, and "MX" records for domain shelbycountytn.gov.
- Ensure all desktop / laptop / tablet computers have TrendMicro OfficeScan / DeepScan client for local anti-virus and data leak prevention.

(ii) Network Administrator employs message and mailbox size limits.

- Initial mailbox limit is set at 50MB on the "Issue Warning and "Prohibit send…" settings on the Storage Limits page on the "Exchange General" tab of the ADS properties in ADUC.
- Subsequent mailbox limits are entered in the same way upon approval of the authority for the limit level (see policy above)

- Total Message Size limit is set to 51200 KB (50MB) in Exchange System Manager on the "Defaults" tab of the Message Delivery Properties under "Global Settings".

(iii) Network Administrator performs monthly Messaging System Maintenance measures.

- ESEUTIL and ISINTEG utilities are executed each month upon the Exchange System mailbox store databases of one or two selected mailbox storage groups to defragment and test the mailbox stores (the folder for defragged databases must be on a separate drive from the original mailbox store with the original store dismounted).

  i. **eseutil /d /p "*location of store*" /t"*folder for defragged databases*"**

  ii. **isinteg –s *Servername* –verbose –l "*logfile location*" –test allfoldertests**

- To keep the Mailbox Store databases at or below the MS recommended 32GB size, mailboxes are re-distributed to other smaller mailbox stores.
- Backup copies of GFI Mailarchiver SQL database and log files, GFI index files, and File Store backend folders are made to \\SCFNTNAS3\VOL1\Backups\GFI folder structure.
- New GFI Mailarchiver databases, indexes, and file folder back-end folder structures are created each month for upcoming months.

e) Applicability of Other Policies:

This document is part of the county's cohesive set of security policies. Other policies may apply to the topics covered in this document and as such the applicable policies should be reviewed as needed.

f) Enforcement:

The Security Officer will enforce this policy. Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities are suspected, the county will report such activities to the applicable authorities.

g) Policy Owner:

Chief Information Officer, Department of Information Technology Services

h) Policy Administrator:

Shelby County Government Security Officer

i) Policy Approval Date:

Current Revision Review Date:		08/01/2016
Current Revision	1.1 Approval date:	10/07/2014
Original Version	1.0 Approval date:	08/30/2013

j) Policy Effective Date:

Current Revision	1.1 Effective Date:	10/07/2014
Original Version	1.0 Effective Date:	11/30/2012

k) Compliance:

l) Supporting Forms:

Public Records Commission Retention Schedule, # 15-014, CTAS Manual
HIPAA Administrative Simplification Regulations 45 CFR 160, 162, and 164

m) Definitions:

(1) Electronic Messaging System is the computer hardware and software used to compose, transmit, receive, store, or display messages in electronic form, including but not limited to electronic mail and instant messaging.

(2) Electronic Collaboration is the sharing of information electronically between users across electronic communications networks.

(3) Electronic Mail (email) is an electronic communication or message consisting of text with or without attached documents that is transported from one user to another or to many others, via electronic communications media.

(4) EPHI (Electronic Protected Health Information) is health information maintained or transmitted in an electronic format.

(5) The Health Insurance Portability and Accountability Act (HIPAA) of 1996 was enacted by the U.S. Congress in 1996 to protect health information (EPHI).

(6) Payment Card Industry Data Security Standard (PCI DSS) is a worldwide information security standard defined by the Payment Card Industry for the protection of credit card information.

(7) Instant Message (IM) is an electronic communication or text message transported from one user to another or to many others over a specific electronic connection via electronic communications networks.

(8) SCAM email is electronic messages designed to trick someone into giving out protected information for the purpose of exploiting the information. These are

sometimes called "Phishing Scams" because the perpetrator is "fishing" for information.

(9) SPAM email is unsolicited commercial electronic messages.

4. Appendices:

5. Mobile System Use

a) Purpose:

This policy will cover the use of laptop computers, tablets, smart phones and cellular devices by employees of Shelby County.

b) Scope:

This policy applies to all Shelby County organizations, employees, and contractors, and any other individuals or organizations that use Shelby County technology resources. Shelby County technology resources include, but are not limited to: networks, servers, data, applications, and information. It applies to all Shelby County facilities.

c) Policy:

Mobile access to e-mail and other data has become common place.

Mobile Workers and Laptops
Shelby County will supply laptop computers, tablets, and smart phones to truly mobile employees as determined by management.

Cellular Devices
The organization recognizes that laptops, tablets and cellular devices can enable workers to achieve more in less time. For critical positions, Shelby County will supply a laptop, tablet, cellular device and/or smart phone equipped with a data plan to facilitate access to e-mail and calendar items.

Third-party applications that are not business related will not be supported by ITS.

d) Procedures:

Data Access
Some services will be available via any Internet connection to employees. These items include the following:

- E-mail
- Web site
- VPN

Other services will be available to ITS staff to facilitate the management of Shelby County's systems remotely. These include the following:

- Remote desktop access – access to a desktop session or terminal server to allow maintenance of Shelby County's systems or support
- SSH access to infrastructure equipment – firewalls and other devices that support secure shell

Public Access
Any services that are available to employees only will require authentication from any connection that is not internal to Shelby County.

If an employee needs direct access to Shelby County resources, a request can be made to use a VPN connection to Shelby County's systems through the access request process. This will provide more access to data than using publicly available resources but will not be made available for everyone.

Wireless Access

Shelby County will provide wireless access to the Shelby County network in areas where an approved business need has been established. Only devices approved by ITS will be allowed to connect wirelessly to the Shelby County network.

Shelby County will also provide guest wireless access for authorized visitors in areas with wireless coverage. The guest wireless access will provide a wireless connection to the Internet, allowing access to basic Internet services, while prohibiting access to secure Shelby County resources. Guest wireless access will require registration, according to the "Shelby County Guest Wireless Network Pre-Shared Keys" procedure located on the County Intranet, and:

- Biannual Guest Wireless Network Pre-Shared (WPA2) key changes are made in January and July.
- Re-authentication (login) is required every 8 hours.
- Registration verification and renewal ir required 30 days after the previous registration.

e) Applicability of Other Policies:

This document is part of the Shelby County Government Information Technology Services cohesive set of security policies. Other policies may apply to the topics covered in this document and as such the applicable policies should be reviewed as needed.

f) Enforcement:

The Security Officer will enforce this policy. Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities are suspected, the county will report such activities to the applicable authorities.

g) Policy Owner:

Shelby County Government

h) Policy Administrator:

Chief Information Officer, Department of Information Technology Services

i) Policy Approval Date:

Current Revision Review Date:			08/01/2016
Current Revision	1.2	Approval date:	06/10/2015
Original Version	1.0	Approval date:	08/11/2013

j) Policy Effective Date:

Current Revision	1.2	Effective Date:	07/01/2015
Original Version	1.0	Effective Date:	11/30/2012

k) Compliance:

l) Supporting Forms:

Network Security Policy
Information Security Policy
Shelby County Guest Wireless Network Pre-Shared Keys

m) Definitions:

(1) Mobile Broadband Connection types: is the marketing term for wireless Internet access through a portable modem, mobile phone, USB wireless modem, or other mobile devices.

(2) Wi-Fi Connection types: (also spelled Wifi or WiFi) is a popular technology that allows an electronic device to exchange data wirelessly (using radio waves) over a computer network, including high-speed Internet connections.

(3) Cellular Devices/Smart Phones: A mobile device that offers advanced computing ability and connectivity.

(4) Intranet: the term is used in contrast to internet, a network between organizations, and instead refers to a network within an organization.

(5) Extranet: A computer network that allows controlled access from the outside of an organizations internal network for specific business or educational purposes. An extranet can be viewed as an extension of an organization's intranet that is extended to users outside the organization, usually partners, vendors, and suppliers, in isolation from all other internet users.

(6) Remote Desktop Access: refers to a software or operating system feature that allows a personal computer's desktop environment to be controlled remotely.

(7) SSH: A network protocol for secure data communication and remote command execution.

(8) VPN: A secure connection established over an insecure network commonly used to access company resources.

n) Appendices:

F. Privacy

1. Employee Privacy Policy

a) Policy Intent:

This policy will outline how Shelby County handles employee privacy.

All organizations must ensure the successful operation of their business. Allowing employees free reign over their time and not maintaining controls over business operations and time of employees is not a best practice, but allowing some privacy to employees and trusting them to get their needed work completed can improve morale and productivity of the workforce.

b) Scope:

This policy applies to all Shelby County organizations, employees, and contractors, and any other individuals or organizations that use Shelby County technology resources. Shelby County technology resources include, but are not limited to: networks, servers, data, applications, and information. It applies to all Shelby County facilities.

c) Policy:

Allowing employees some privacy while they work is a good way to boost productivity and morale within Shelby County. Other "POLICY" in place within Shelby County establish rules and consequences for when those "POLICY" aren't followed. This policy reviews employee privacy during their time at work.

Privacy Rights

Employees of Shelby County can expect a reasonable amount of privacy during the work day. The organization and management trust employees to work on County business while at work with the exception of break periods or observed lunches.

During work, an employee may receive phone calls, email messages, or communications that are not related to work if these do not interfere with the regular performance of job duties for that employee or otherwise adversely affect the operations of SCG business.

Electronic communication and documents

Shelby County reserves the right to retain and review all communication sent through the corporate communication system as well as any documents created and stored on county resources.

If there are messages that are not suitable for work, it is advised that they not be sent to a Shelby County owned mailbox or account.

All documents stored on county resources are subject to review. It is not to be assumed that personal documents will not be used, read, or obtained by Shelby County if they are stored on Shelby County owned information systems or equipment.

Constant use of a personal email account or other messaging technology that interferes with regularly assigned duties will result in disciplinary action where appropriate, up to and including termination. Checking personal email or voicemail during scheduled breaks or briefly during the workday, as long as this does not affect performance, is allowed by employees using the Shelby County information system.

Use of Internet Access

Using the Internet during County time when not required by job duties for research or other purposes should be limited to break periods. Any use for non-work purposes that interferes with productivity and performance will not be allowed.

d) Procedures:

e) Applicability of Other Policies:

This document is part of the Shelby County Government Information Technology Services cohesive set of security policies. Other policies may apply to the topics covered in this document and as such the applicable policies should be reviewed as needed.

f) Enforcement:

The Security Officer will enforce this policy. Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities are suspected, the county will report such activities to the applicable authorities.

g) Policy Owner:

Shelby County Government

h) Policy Administrator:

Chief Information Officer, Department of Information Technology Services

i) Policy Approval Date:

Current Revision Review Date:			08/01/2016
Current Revision	1.0	Approval date:	10/10/2014
Original Version	1.0	Approval date:	10/10/2014

j) Policy Effective Date:

Current Revision	1.0	Effective Date:	10/10/2014
Original Version	1.0	Effective Date:	10/10/2014

k) Compliance:

l) Supporting Forms:

Acceptable Use Policy
Web Privacy Policy
Web Privacy Statement

m) Definitions:

n) Appendices:

2. Web Privacy Policy

a) Policy Intent:

This policy defines how personal and/or confidential information is collected from visitors to this site.

b) Scope:

This policy applies to all Shelby County organizations, employees, and contractors, and any other individuals or organizations that use Shelby County technology resources. Shelby County technology resources include, but are not limited to: networks, servers, data, applications, and information. It applies to all Shelby County facilities.

c) Policy:

Non-sensitive information provided by visitors to our site (e.g., name, email address, etc.) is used for the purposes of customer service and user request fulfillment. Information of this type may be internally forwarded (electronically or in print) to appropriate parties in order to resolve inquiries or visitor-supplied requests. Additionally, we may collect non-personal information regarding your visits to the County's website(s) for the purpose of statistical analysis

This data collection includes, but is not limited to:

- The frequency, date and time of visits to our site
- Pages and/or areas of the site visited
- Browser type and operating system used during site visitation
- Screen Resolution
- Number of pages viewed during each site visit

Confidential (private) information, where credit card/bank information is collected, (e.g., vehicle registration) is used solely for the purpose of conducting online transactions. Information collected is administered and supervised by Shelby County.

In addition to defining its purpose, the Shelby County Privacy Policy examines the applicability of the following:

- Cookies
- Compliance
  - Health Insurance Portability and Accountability Act (HIPAA)
  - Sarbanes-Oxley Act Compliance (SOX)
  - Children's Online Privacy Protection Act (COPPA)
- Third-Party Involvement
- Modifications to the Shelby County Privacy Policy

d) Procedures:

e) Applicability of Other Policies:

This document is part of the Shelby County Government Information Technology Services cohesive set of security policies. Other policies may apply to the topics covered in this document and as such the applicable policies should be reviewed as needed.

f) Enforcement:

The Security Officer will enforce this policy. Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities are suspected, the county will report such activities to the applicable authorities.

g) Policy Owner:

Shelby County Government

h) Policy Administrator:

Chief Information Officer, Department of Information Technology Services

i) Policy Approval Date:

Current Revision Review Date:			08/01/2016
Current Revision	1.0	Approval date:	10/10/2014
Original Version	1.0	Approval date:	10/10/2014

j) Policy Effective Date:

Current Revision	1.0	Effective Date:	10/10/2014
Original Version	1.0	Effective Date:	10/10/2014

k) Compliance:

l) Supporting Forms:

Acceptable Use Policy
Web Privacy Statement

m) Definitions:

n) Appendices:

G. Security

1. Establishment of Security Program

a) Policy Intent:

The Shelby County Commission desires that the Department of Information Technologies protect Shelby County's internal and external information resources including the wide area networks, local area networks and central computer platforms.

This Shelby County Information Technology Services Security Program will assign responsibility and clarify behavioral expectations to safeguard technology-related information and tools. It also provides guidance for administering the Shelby County Information Technology Services Security Policy. This policy is designed to protect Shelby County's internal and external information resources.

b) Scope:

This policy applies to all Shelby County organizations, employees, and contractors, and any other individuals or organizations that use Shelby County technology resources. Shelby County technology resources include, but are not limited to: networks, servers, data, applications, and information. It applies to all Shelby County facilities.

c) Policy:

It will be the policy of the Shelby County Commission to establish and maintain an Information Technology Services Security Program to create policy and procedures to protect Shelby County's information and technology resources.

The Commission is the final authority for policy and procedures relating to technology security.

The Department of Information Technology Services will act as the Commission's controlling authority in matters of data security, internet security, security policy development, security standards, security services, and compliance.

The Department of Information Technology Services will create standards and procedures, consistent with sound business practices that support and enforce the Shelby County Information Technology Services Security Policy.

Standards and procedures will consist of usual, customary, and reasonable security practices, and should not inflict undue hardship on the Shelby County computing community.

Because an item or activity is not expressly prohibited does not mean the item or activity is permitted. The security of such items or activities will be decided by the Department of Information Technology Services on a case-by-case basis.

This policy will be reviewed twice a year by the Department of Information Technology Services, and changes will be recommended that keep it current as information technology evolves and changes.

d) Procedures:

e) Applicability of Other Policies:

This document is part of the Shelby County Government Information Technology Services cohesive set of security policies. Other policies may apply to the topics covered in this document and as such the applicable policies should be reviewed as needed.

f) Enforcement:

The Security Officer will enforce this policy. Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities are suspected, the county will report such activities to the applicable authorities.

g) Policy Owner:

Shelby County Government

h) Policy Administrator:

Chief Information Officer, Department of Information Technology Services

i) Policy Approval Date:

Current Revision Review Date:			08/01/2016
Current Revision	1.1	Approval date:	10/03/2014
Original Version	1.0	Approval date:	11/04/2013

j) Policy Effective Date:

Current Revision	1.1	Effective Date:	10/03/2014
Original Version	1.0	Approval date:	11/04/2013

k) Compliance:

l) Supporting Forms:

m) Definitions:

n) Appendices:

2. Clear Screen Policy

a) Policy Intent:

This policy covers the unsecure storage of passwords and access credentials.

b) Scope:

This policy applies to all Shelby County organizations, officials, employees, contractors and any other organization using Shelby County's technology resources. Shelby County's technology resources include, but are not limited to networks, servers, data, applications, personal computers, personal digital assistants, data storage devices, software and digital data. It applies to all Shelby County facilities and any device, software or data that may be owned by the County or connected to a County asset.

c) Policy:

Because the password "POLICY" required by ITS departments in many organizations are becoming more complex as technology advances, end users have come up with inventive (or not so inventive) ways to store their passwords where they can easily find them if they are forgotten.

This policy aims to curb the use of such methods, especially for initial logon passwords, to keep data within Shelby County more secure.

What Does "Clear Screen" Mean?

"Clear screen" refers to the edges of a computer monitor and the surrounding area where passwords might be stored.

Shelby County ITS is working to ensure the security of its systems and the data stored there. Keeping passwords written where they can easily be located and used to access network resources is a risk to the security of the organization's information technology systems.

d) Procedures:

Keeping Passwords

The following items should not be written down in unsecure locations:

- Usernames
- Passwords
- Obvious password hints

Shelby County will not allow passwords or password hints to be displayed as the screensaver text on a workstation or stored in the work area on a sticky note.

Making Passwords Easier to Remember

While storing passwords in readily accessible places is not an acceptable practice using easier passwords that the user is more likely to remember is a good idea. When a password policy is assigned to require seven characters and three numbers and special characters, the ITS department that is used to remembering passwords has no trouble with the requirement, but this can lead to sticky notes.

A better method for setting password requirements is to require multiple capital letters and 10-12 characters. This way a user can choose a password that they are more likely to remember. They can use a passphrase rather than a password. If the employee has a hobby or an activity that they participate in outside of work, they might use this as their password. For example, here are two passwords:

- Fese2008

- IEnjoyPhotography247 or IEnj07Ph0t0gr@ph7247 (with a mix of special characters and numbers)

The first is the run-of-the-mill combination of capitals, letters, and numbers that meets the usual eight-character requirement. However unless these are a user's initials, the likelihood that this might be remembered is less than the second password. The second password is a passphrase that may indicate a hobby. An individual's hobby is likely easy for them to remember.
A favorite song title or book title is also a good idea to get employees thinking about longer phrases that satisfy less rigid requirements.

Found Passwords
In the event that passwords or access information is found near a workstation, the item will be removed and the employee and their supervisor will receive a written warning to let them know that the information was found and removed.

Subsequent offenses will result in discussions with the employee and their supervisor. Passwords may be changed during these meetings, being replaced by a passphrase, and disciplinary action will be discussed with the user and their supervisor.

Training and New Methods
Simple training sessions with the user population can help alleviate this issue and help employees understand that security is a top priority at all levels. Also it may help to make them aware that a secure passphrase they can remember is one way that each employee can help keep the data of Shelby County safe and secure.

e) Applicability of Other Policies:

This document is part of the Shelby County Government Information Technology Services cohesive set of security policies. Other policies may apply to the topics covered in this document and as such the applicable policies should be reviewed as needed.

f) Enforcement:

The Security Officer will enforce this policy. Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities are suspected, the county will report such activities to the applicable authorities.

g) Policy Owner:

Shelby County Government

h) Policy Administrator:

Chief Information Officer, Department of Information Technology Services

o) Policy Approval Date:

Current Revision Review Date:			08/01/2016
Current Revision	1.1	Approval date:	08/11/2014
Original Version	1.0	Approval date:	08/11/2014

p) Policy Effective Date:

Current Revision	1.0	Effective Date:	08/11/2014
Original Version	1.0	Effective Date:	08/11/2014

i) Compliance:

j) Supporting Forms:

k) Definitions:

Change Management Process – a documented practice whereby changes to systems, applications, or procedures are closely monitored and managed to ensure the desired outcome.

l) Appendices:

3. Network Security Policy

a) Policy Intent:

This policy exists to provide instruction for the protection and securing of Shelby County data, information, and software systems from unauthorized access.

b) Scope:

This policy applies to all persons accessing county information across the Shelby County Network, regardless of division, department, office, section, agency, board, or organization. For persons accessing protected health information, the Shelby County Health Insurance Portability and Accountability Act (HIPAA) Policies will additionally apply. For persons accessing Payment Cardholder Data, Payment Card Industry Data Security Standard (PCI DSS) will additionally apply.

c) Policy:

"It shall be the responsibility of the Information Technology Services (ITS) to provide adequate protection and confidentiality of all County data and software systems, whether held centrally, on local storage media, or remotely, to ensure the continued availability of data and programs to all authorized members of staff, and to ensure the integrity of all data and configuration controls."

d) Summary of Main Security Policies:

(1) Confidentiality of all data is to be maintained through discretionary and mandatory access controls, and wherever possible these access controls should meet with C2 class security functionality.

(2) Primary Account Numbers (PANs) are not to be transmitted in an unencrypted state by end user messaging technologies (for example, e-mail, instant messaging or chat) [PCI DSS 4.2.b].

(3) Primary Account Numbers (PANs), when shown, will not display more than the first 6 digits and the last 3 digits.

(4) End user computing devices may not connect to the Shelby County network until ITS approves the connection and affects the switch-port security configuration [PCI DSS 9.1.2].

(5) Internet and other external service accesses are restricted to authorized personnel only.

(6) Access to data on all laptop computers is to be secured through two-factor authentication, encryption or other means, to provide confidentiality of data in the event of loss or theft of equipment.

(7) Only licensed software, authorized by ITS, may be installed, and installation may only be performed by ITS staff or ITS-authorized personnel. In the event of

unauthorized software being discovered it will be removed from the workstation immediately.

(8) Data may only be transferred for the purposes determined in the organization's data-protection policy.

(9) All removable media will be virus checked before the files they contain are used.

(10) Passwords must consist of a minimum of eight (8) alphanumeric characters, and must be changed at least every 90 calendar days and must be unique [PCI DSS 8.5.9.b / 8.5.11].

(11) The physical security of computer equipment will conform to recognized loss prevention guidelines.

(12) Workstation configurations may only be changed by ITS staff or ITS-authorized personnel.

(13) To prevent the loss of availability of ITS resources, configurations of all workstations will conform to standard images, and locally stored user profile data on identified work stations will be replicated on shared network storage.

(14) A business continuity plan will be developed and tested on a regular basis.

(15) ITS will annually perform a risk assessment to identify threats and vulnerabilities on the network and its endpoints.

(16) The ITS Security and Network Design teams will review the router and firewall rule sets at least every 6 months [PCI DSS 1.6.6.a].

(17) Physical access policies and procedures for SCG-ITS offices and data centers (sensitive areas) are controlled according to the Physical Security of Computer Equipment subsection of the ITS Network Security policy [PCI DSS 9.1 & 9.1.1].

(18) All SCG Offices and Departments are responsible for creating, implementing, maintaining, policing, and where necessary, reporting on, their own physical access policies and procedures for their respective "sensitive areas" [PCI DSS 9.1 & 9.1.1].

e) End-Point Protection:

(1) In the event of a possible virus infection the user must inform the ITS and/or ITS authorized personnel immediately. ITS will then disconnect and scan the infected machine and any removable media or other workstations to which the virus may have spread and eradicate it.

(2) Information Technology Services will have available up to date virus scanning software for the scanning and removal of suspected viruses. Only End-Point virus scanning software for which Shelby County Government has a current "license to use" will be installed / used on county file-servers and workstations under the management of the ITS [PCI DSS 5.2.a].

(3) All county servers and workstations, especially those holding or handling credit cardholder data, must be protected with virus scanning software, the patch levels and virus signature databases of which must be kept up to date. Exceptions and exclusions for folder and file scanning must be justified in writing and approved by ITS Administration [PCI DSS 5.2.a].

(4) Anti-virus logs on all county servers will be forwarded to county logging server for analysis and reporting. The logs are to be retained for a period of one (1) year [PCI DSS 5.2.a].

(5) All county servers and workstations, especially those holding or handling credit cardholder data, must have OS and service software patch levels up to date. All OS and service software patches are to be tested for functionality before being implemented. Exceptions and exclusions for patches must be justified in writing and approved by ITS Administration.

(6) County electronic mail will be protected with virus scanning software capable of scanning attachments and archives, even inside of forwarded messages.

(7) All removable media will be virus checked before the files they contain are used [PCI DSS 9.7].

(8) All systems will be built from original, clean master copies or master images whose write protection has always been in place. Only original master copies will be used until virus scanning has taken place.

(9) All demonstrations by vendors will be run on the vendor's machine and not on Shelby County's machines.

(10) As shareware is one of the most common infection sources, it will only be used if it is absolutely necessary, and it must be thoroughly scanned before use.

(11) To enable data to be recovered in the event of a virus outbreak regular backups of servers will be taken by the ITS.

(12) Users will be kept informed of current procedures and policies, and users will be notified of virus incidents.

(13) Employees will be accountable for any breaches of the organization's anti-virus policies within their area of responsibility.

(14) Anti-virus policies and procedures will be reviewed regularly.

f) Physical Security of Computer Equipment

(1) The required physical security precautions for each designated Security Level include:

(i) All security level areas must have locked doors when the area is unoccupied and, if ground floor windows are present, window blinds or obscure filming.

(ii) Security levels 2, 3, and 4 must be placed away from public access and must have blinds closed or obscure filming to obstruct view of systems from the windows if ground floor windows are present.

(iii) High-risk situations must have the following security measures implemented;

- bars, key operated locks, or lockable shutters on ground level, opening windows,
- windows to external elevations should be fitted with security shutters or bars instead of locks.
- systems must be placed at least 10 feet from external windows, and
- electronic card-access security locks with manual key override, and access cards are only to be issued to authorized personnel.

(2) Computer Sites must have the following security measures and guidelines implemented and followed;

(i) Sites must be placed away from public access.

(ii) Ground floor windows must have blinds closed or obscure filming to obstruct view of systems within.

(iii) Windows to external elevations should be fitted with security shutters or bars,

(iv) The site must have electronic card-access security locks with manual key override, and access cards issued only to authorized personnel.

(v) Sites must be monitored using video surveillance.

(vi) Fire Suppression systems and local fire extinguisher equipment must be present and functional.

(vii) A Monitored Building Alarm with the following features must be in place;

- Protection of Signal Transmission
- Location of Intruder Alarms
- Break Glass Alarm Sensors
- Alarm Zoning
- Intruder Alarm Sensors on Access Routes
- Alarm Shunt Lock
- Alarm Confirmation

(viii) The computer site should be housed in a purpose built room.

(ix) Partitions separating the room or **AREA** from adjoining rooms and corridors should be heavy-duty block-work or brick-work devoid of openings except for protected doors as defined below.

(x) Secure doors giving access to the room or **AREA**, from within the building, should be solid security doors. Door fittings should include 3 hinges.

(xi) The computer site should contain an adequate air conditioning system to provide a stable operating environment to reduce the risk of system crashes due to component failure.

(xii) No water, rain water or drainage pipes should run within or above the computer site to reduce the risk of flooding.

(xiii) The floor within the computer site should be a raised false floor to allow computer cables to run beneath the floor, and should have sub-floor water sensors to reduce the risk of damage to computer equipment in the case of flooding.

(xiv) Emergency Power Off (EPO) switches should be installed at two opposite ends of the **COMPUTER SITE** to affect complete power shutdown of the site in the event of an emergency situation.

(xv) All **COMPUTER EQUIPMENT** should be protected by Uninterruptible Power Supply (UPS) capable of sustaining power long enough for the generators to stabilize and begin providing power in the event of main power failure.

(xvi) Generator power should be provided to the **COMPUTER SITE** to help protect the computer systems in the case of a main power failure.

(xvii) Access to the **COMPUTER SITE** is restricted to authorized personnel only.

(xviii) All ITS employees are required to wear their I.D. card clearly visible at all times at or above the waist while at areas assigned to ITS

(xix) All Visitors to the COMPUTER SITE are to be met at the secure entrance, where the visitors will [PCI DSS 9.2.a / 9.4.b];

- Sign the "Visitors Register", which is retained for a period of at least ninety (90) calendar days,
- Be given a "Visitor" badge, which the visitor must display at all times,
- Be escorted to their destination,
- Be monitored by an ITS employee during their visit,
- Be escorted out to the secure entrance when their visit is complete [PCI DSS 9.2.a], and

- Un-accompanied visitors must be queried; the employee they have come to visit must be called [PCI DSS 9.2.a].

(xx) All contractors and vendors working within the COMPUTER SITE, who are not permanently assigned to SCG ITS support functions, are to be met at the secure entrance, where they will [PCI DSS 12.3.8 / 12.3.9 / 12.3.10.a];

- Sign the "Visitors Register", which is retained for a period of at least thirty (30) calendar days,
- Sign the Vendor Acknowledgement Agreement (VAA),
- Be given a "Visitor" badge, which the visitor must display at all times, and
- Be escorted to their destination (as identified by the vendor).
- Vendors may be left unattended at their destination if;
  - The Vendor has signed the VAA and
  - The location is monitored via video surveillance.
- Upon completion of the scheduled task, the vendor must contact their ITS escort and be escorted from the COMPUTER SITE to the secure entrance where they will sign out and return their visitor's badge.
- ITS is to be notified at least twenty-four (24) hours in advance of their presence and provided with details of all work to be carried out.
- Un-accompanied contractors and vendors must be queried; the employee they have come to visit must be called to assure they are in the appropriate location or to escort the vendor to the appropriate location.
- No contractors or vendors are to be left unattended unless a signed VAA is on file.

(xxi) Permanently Assigned Contractor and Vendor Employees (PAVEs) supporting SCG ITS functions are permitted access to ITS COMPUTER SITES for legitimate service purposes without the need for a visitor's badge or an escort, under the following conditions.

- The Security Officer has reviewed and approved the PAVE's access, approving the issuance of a SCG vendor id badge and physical access card with appropriate access.
- The PAVE must display their SCG badge at all times while on site.
- A current VAA is on file with SCG ITS for the vendor employee. It is the responsibility of the ITS Manager overseeing the functions of a given PAVE to provide the ITS Security group with the signed VAA for each PAVE. VAAs for PAVEs must be renewed annually.
- In the event that a VAA for a given Vendor employee is not on file or has expired, physical access cards will be immediately disabled until a current VAA is received.
- In the event that the vendor has forgotten or misplaced their badge or physical access card, the vendor must;
  - Follow all requirements of section xx as a standard contractor of vendor to gain access to SCG ITS facilities and

- Report the loss of the badge and physical access card to the ITS Manager overseeing their support functions.
- Any ITS Manager informed of a badge or physical access card loss will disable the physical access card immediately and notify the Security Officer.

- Any violation of these requirements will result in immediate review of the PAVEs status and may result in permanent removal of PAVE status by the Security officer.

g) Access Control

(1) Access Security Levels

(i) Access Level 1 - This level describes access to information deemed "Public", freely accessible by anyone.

(ii) Access Level 2 - This level describes access to information deemed "For Official Use Only", accessible based upon verified County business need.

(iii) Access Level 3 - This level describes access to information deemed "Confidential" to include but not limited to:

- Information in Access levels 2 and 3 if accessed from mobile computer (Laptop, Notebook, hand-held).
- Personal Information covered by Privacy Act of 1974 and Privacy and Personal Information Protection Act of 1998
- Personal Health information covered by Health Insurance Portability and Accountability Act (HIPAA)
- Payment Card Industry Cardholder Data covered by Payment Card Industry Data Security Standard (PCI DSS)
- Security information pertaining to physical and logical connectivity to and access of the network and its resources

(2) Tiered Authentication

(i) SCITS will restrict each entity's access and privileges to its own data environment. Enterprise domain access will be restricted to SCITS personnel [PCI DSS 7.1.2].

(ii) Users and System Administrators will only be granted permissions to access systems and applications sufficient to enable them to perform their job function [PCI DSS 7.1.2].

(iii) Access Level 1 requires no authentication measures, however registration and identification may be required.

(iv) Access Level 2 requires single factor authentication comprised of a County-provided logon ID and password meeting the following requirements:

- Logon ID is comprised of first name and last name of user, with middle initial and second letters added to resolve duplication issues.
- Passwords must be at least eight (8) characters in length, and shall be a combination of at least three (3) of the following character types:
  - Capital letters (A – Z)
  - Lower-case letters (a – z)
  - Numbers (0 – 9)
  - Special characters (! @ # $ % ^ & * - = +)
- Passwords must not contain any portion of your logon name, nor may it contain dictionary words or proper names.
- Initial passwords must be unique and are required to be changed immediately upon first use [PCI DSS 8.2.6].
- Upon password reset, temporary passwords will be set to a unique value for each user, and will be forced to change immediately after the first use [PCI DSS 8.2.6].
- Passwords are required to be changed every ninety (90) calendar days, and may not be changed within the first seven (7) days after the last change (by user).
- Passwords must be unique for at least four (4) iterations where technically feasible. [PCI DSS 8.5.12.b].

(v) Access Level 3 requires single factor authentication comprised of a County-provided logon ID and password meeting the following requirements:

- Logon is comprised of first name and last name of user, with middle initial and second letters added to resolve duplication issues.
- Passwords must be at least eight (8) characters in length and shall be a combination of at least three (3) of the following character types:
  - Capital letters (A – Z)
  - Lower-case letters (a – z)
  - Numbers (0 – 9)
  - Special characters (! @ # $ % ^ & * - = +)
- Passwords must not contain any portion of your logon ID or name, nor may it contain dictionary words or proper names.
- Initial passwords must be unique and are required to be changed immediately upon first use. Passwords are required to be changed every forty-five (45) calendar days, and may not be changed within the first seven (7) days after the last change (by user).
- Passwords are required to be unique for at least six (6) iterations.

(vi) Users are responsible for changing and remembering their passwords.

(vii) Users requesting password resets must provide three pieces of identifying information [PCI DSS 8.5.2]:

- The last four (4) digits of the user's Social Security Number (SSN).
- The user's Shelby County Employee Identification Number.
- The user's Supervisor or Manager's full name.

(viii) Users are responsible for the security of their Logon ID and password, and will not write down or share their Logon ID or passwords with anyone.

(ix) The ITS will be notified of all employees leaving the Organization's employment at least one business day prior to their effective termination dates. The ITS will remove the employees' permissions to all systems and disable the users accounts at close of business on clients' final day of employment with Shelby County Government. If an employee is terminated against their wishes, the terminating department must call ITS prior to notification to employee. Department is to notify ITS of date/time to remove or disable employee's network account.

(x) Auditing will be implemented on all systems to record login attempts/failures, successful logins and changes made to all accesses.

(3) Local Machine Access

(i) Intruder detection will be implemented where possible. The user account will be locked after six (6) incorrect attempts, and will not be unlocked for a period of at least 30 minutes, or until an ITS account administrator unlocks the account [PCI DSS 8.5.13].

(ii) Where possible no one person will have full rights to any system. The ITS will control user and network/server passwords.

(iii) ITS staff will not login as root on to UNIX, Linux systems, but will use the "su" command to obtain root privileges.

(iv) Server Local Administrator accounts will be renamed and "dummy" Administrator accounts having no access will be created in their places.

- Server Local Administrator accounts will be used only for server generation tasks or in emergencies where access is only achievable through use of the server Local Administrator account.
- Server Local Administrator accounts will not be utilized to perform general maintenance tasks.
- Services will be installed and run using Service Accounts, not Server Local Administrator accounts.

(v) Network/server supervisor passwords and system supervisor passwords will be stored in a secure location in case of an emergency or disaster, for example a fire safe in the ITS.

(vi) On UNIX and Linux systems, rights to rlogin, ftp, telnet, ssh will be restricted to ITS staff only.

(vii) On NetWare and Windows systems, rights to remote console, remote desktop, ftp, telnet will be restricted to ITS staff or ITS-authorized personnel only.

(viii) Where possible users will not be given access to the UNIX, or Linux shell prompt.

(4) Generic, Vendor, Systems and Service Accounts

(i) Default passwords on systems such as Oracle and SQL Server will be changed after installation [PCI DSS 2.1.1.e / 6.3.1].

(ii) System and Service accounts will be configured to allow logon only from the local system on which their service function is required.

(iii) Generic user accounts will not be used to provide access to this network or its resources, and are expressly forbidden for access to systems and applications containing Cardholder Data [PCI DSS 6.3.1].

(iv) "Email Mailbox Only" accounts will be identified as such and access restricted to specific network resources, and will have permissions established for mailbox monitoring by specific users identified in writing by the requesting authority.

(v) Vendor and Contractor user accounts will be enabled and the password changed at the beginning of the contracted time period, will be monitored for logon, logout and access in security logs, and will be disabled when no longer in use. Vendor accounts for critical applications requiring 24-hour support are exempted from the requirement to be disabled when not in use [PCI DSS 8.5.6.a / 8.5.6.b].

(5) Data Access Requirements

(i) All usernames and accounts providing access to ITS technology resources will be approved and issued according to "Access Request Submission Procedure" using a standardized, documented access request procedure [PCI DSS 12.5.4].

(ii) Requests for usernames or accounts with access to ITS technology resources must be made through the submission of a fully executed Computer Access Form accompanied by an Acceptable Use Policy signed by the end user [PCI DSS 7.1.3].

(iii) All usernames and accounts granted access to SCG ITS technology resources will be created by the Department of Information Technology Services (ITS).

(iv) All requests for usernames and accounts will be vetted and approved by a member of the ITS security group prior to being enabled and released to the end user.

(v) Requests for access must originate from the office or department's primary or secondary customer contacts, as identified in the established SLA agreements, or from a manager or higher-level authority within the office or department. The Business Relationship Primary and Secondary Contact

listing will serve as the ITS Access Authorization Matrix for Shelby County Government.

(vi) Computer Access Forms will be retained for at least the duration of the access granted plus one year after termination of the access.

(vii) Access to networks and servers will be restricted to the department's normal established working hours. Users requiring access outside normal working hours must request such access in writing to the ITS Administrator.

(viii) File system access will have the maximum security implemented allowing users permissions only to directories containing data to which they have a business need for access.

(6) Access Inactivity and Revocation

(i) User accounts and all access for employees who are terminated will be disabled by ITS immediately upon notification, and the accounts will be deleted after a period of ninety (90) days unless identified as "Hold" for legal or administrative purposes by County Administration in writing.

(ii) User and Computer accounts will be audited for inactivity on a monthly basis, and if found to be inactive for a period of ninety (90) consecutive days, will be disabled and investigated as to cause of inactivity [PCI DSS 8.5.5].

h) Network Security

(1) Network Routers & Switches

(i) User accounts on the router are configured as Shelby County Network ADS user accounts with membership in "Dom ITEC Technical Support" and "Dom ITEC Customer Support" domain security groups. LDAP connectivity with ADS is affected via Cisco ACS servers using TACACS protocol. Router security levels are based on user account access levels.

(ii) The enable password on the router must be kept in a secure encrypted form. The router must have the enable password set to the current production router password from the router's support organization. Network device passwords are to be kept in an encrypted format in a secure location off the network.

(iii) The following are to be disallowed on all routers / switches [PCI DSS1.1.5.b]:

- IP directed broadcasts
- Incoming packets at the router sourced with invalid addresses
- TCP small services
- UDP small services
- All source routing
- BOOTP service

(iv) Unnecessary protocols will be removed from routers. Currently this include MOP (DECNET).

(v)

(vi) Access rules are to be added as business needs arise.

(vii) Switch and Router equipment must be secured within the Computer Site or in locked switch rooms, or at the least within a locked cabinet. Only ITS staff is to have physical access to switch and router equipment.

(viii) The router must be included in the corporate enterprise management system with designated primary and backup points of contact. Routers / switches will use corporate standardized SNMP community strings.

(ix) Each router / switch must have the following Message of the Day (MOTD) statement posted upon login:

```
&&&
```

(iv) Internet accessible network interfaces must have appropriate Domain Name Server (DNS) records (minimum of A and PTR records).

(v) Connection of equipment to Shelby County's Extranet and DMZ Networks require approval of ITS, and approved equipment must be documented to include the following information [PCI DSS 2.2.c]:
- Host contacts and location.
- Hardware and operating system configuration.
- Main functions and applications.

(vi) Hardware, operating systems, services and applications must be approved by ITS prior to deployment, and all Operating System configurations and all patches/hot-fixes recommended are to be completed following approved Shelby County baseline installation procedures.

(vii) Services and applications not for general access must be restricted by access control lists, and those services and applications not serving business requirements must be disabled.

(viii) Trust relationships between autonomous systems may only be introduced according to business requirements, must be documented, and must be approved by ITS.

(ix) Remote administration and host content updates must be performed over secure channels (e.g., encrypted network connections using SSH or IPSEC). Exceptions must be approved by ITS and documented.

(x) Security-related events must be logged and audit trails saved to ITS-approved logs. Security-related events include (but are not limited to) the following [PCI DSS 10.4.2.b]:
- User login failures.
- Failure to obtain privileged access.
- Access policy violations.

(xi) The responsibility for the security of the equipment deployed by external service providers must be clarified in the contract with the service provider and security contacts, and escalation procedures documented. Contracting departments are responsible for third party compliance with this policy.

(3) Network Wiring

(i) All network wiring will be deployed to established standards and fully documented.

(ii) Users must not place or store any item on top of network cabling.

(iii) Redundant cabling schemes and communication protocols providing redundancy will be used at the core, distribution blocks, and horizontal access points of the network.

(4) Virtual Private Network (VPN)

(i) It is the responsibility of employees with VPN privileges to secure their authentication credentials such that unauthorized users are not allowed access to Shelby County internal networks.

(ii) VPN use is to be controlled using two (2) factor authentication including but not limited to public/private key system with a strong passphrase [PCI DSS 8.2 / 8.3].

(iii) When actively connected to the Shelby County network, VPNs will force all traffic to and from the PC over the VPN tunnel: all other traffic will be dropped. Dual (split) tunneling is NOT permitted; only one network connection is allowed [PCI DSS 1.3.8.b].

(iv) All computers (personal or corporate) connected to Shelby County internal networks via VPN or any other technology must comply with all rules and regulations that apply to Shelby County-owned or leased equipment, i.e., must be configured to comply with ITS Security Policies.

(v) VPN users will be automatically disconnected from Shelby County's network after thirty (30) minutes of inactivity. The user must then logon again to reconnect to the network. Pings or other artificial network processes are not to be used to keep the connection open.

(vi) Users of devices that are not Shelby County owned equipment must configure the equipment to comply with Shelby County's VPN and Network policies.

(vii) Only Shelby County ITS approved VPN clients or clientless connection technologies with ITS approved encryption may be used.

(5) Wireless Networks [PCI DSS 2.1.1.d]

(i) Wireless LAN's with access to Shelby County internal network will make use of the most secure encryption and authentication facilities available. Specific wireless encryption standards are documented in the SCITS "Data Encryption Policy".

(ii) All wireless access points and wireless network interfaces must be registered and approved by ITS. Users will not install their own wireless access points under any circumstances.

(iii) Shelby County ITS will detect, identify, and notify security personnel of unauthorized wireless access points on at least a quarterly basis [PCI DSS 11.1.a / PCI DSS 11.1.c] detecting:

- WLAN cards inserted into system components [PCI DSS 11.1.b].
- Portable wireless devices connected to system components [PCIS DSS 11.1.b].
- Wireless devices attached to a network port or network device [PCI DSS 11.1.b].

(iv) All computers with wireless LAN devices must utilize an ITS administered SSID to communicate with the appropriate wireless access points. All implementations must support a hardware address that can be registered and tracked, i.e., a MAC address.

(v) Users are prohibited from connecting devices simultaneously to Shelby County network and any other network. Dual (split) tunneling is NOT permitted; only one network connection is allowed.

(vi) Shelby County Government wireless devices owned by SCG and managed by SCG ITS will be permitted wireless access through SCWLAN.

(vii) Shelby County Government wireless devices owned by SCG, but not managed by SCG ITS, will be permitted wireless access through SCWLAN2.

(6) Remote Access

(i) It is the responsibility of Shelby County employees, contractors, vendors and agents to ensure that their remote access connection and activity complies with Shelby County Security and Acceptable Use Policies. The Shelby County employee, contractor, vendor or agent bears responsibility for the consequences should the access be misused. This requirement must be stated in any contracts with third parties involving remote network access.

(ii) While connected remotely to Shelby County's network, employees, contractors, vendors and agents will ensure their computers are not connected to any other network at the same time. Dual (split) tunneling is NOT permitted; only one network connection is allowed.

(iii) Routers for dedicated ISDN lines configured for access to the Shelby County network must meet minimum authentication requirements of Challenge-Handshake Authentication Protocol (CHAP).

(iv) Dial-in modems will not be used. Exceptions must be approved by ITS and documented.

(v) Where leased lines are used, the associated channel service units will be physically located within locked telephone/switch rooms to prevent access to their monitoring ports.

(vi) All connections made to the Organization's network by outside organizations will be logged.

(7) Encryption

(i) Only proven, standard encryption algorithms will be approved by ITS. Symmetric cryptosystem key lengths must be at least 1024 bits. Asymmetric crypto-system keys must be of a length that yields equivalent strength. Shelby County's key length requirements will be reviewed annually and upgraded as technology allows.

(ii) As export of encryption technologies is restricted by the U.S. Government, ITS and all approved entities deploying encryption algorithms within the Shelby County Network will secure the encryption technologies utilized from disclosure outside the U.S.

(iii) Default encryption keys on network devices will be changed from the default upon installation and again upon departure of individuals responsible for or with knowledge of said encryption keys [PCI DSS 2.1.1.a].

(iv) ITS maintains secure off-line archival copy of internal CA private keys and certificates, recovery agent keys and certificates, and all internal keys and certificates generated.

(v) ITS maintains a log of all keys and certificates generated, an on-line certificate enrollment, renewal and revocation process, and an on-line certificate revocation list (CRL).

(8) Monitoring Software

(i) The use of network monitoring and packet sniffing software is restricted to the ITS.

(ii) Intrusion detection systems will be implemented to detect unauthorized access to the network [PCI DSS 2.1.1.1.b].

(iii) Default SNMP community strings on all network devices will be changed from the default upon installation [PCI DSS 2.1.1.1.c].

(9) Electrical Security

(i) All servers and network communication devices will be protected by UPS's with power conditioning.

(ii) In the event of a main power failure, the UPS's will have sufficient power to keep the network and servers running, until the generator takes over.

(iii) All UPS's will be tested by ITS periodically.

i) Workstation Security

(1) Workstations

(i) Workstations will adhere to ITS image-based deployment, management, application and data storage.

(ii) Shelby County business-related data files and structures are to be stored on Shared Network Media; files stored directly on Local machine may not be recoverable.

(iii) Major Workstation hardware failures will be remedied via comparable replacements.

(iv) Only properly licensed software, approved and installed by ITS will be allowed on workstations.

(v) Only ITS–approved hardware and software required for the performance of official Shelby County business duties will be allowed.

(2) Workstation Security

(i) Users must logout of their workstations when they leave their workstation for long periods of time, and Windows workstations (while connected to the network) will be configured to lock after a minimum of fifteen (15) minutes of inactivity, requiring the entry of the user's network password to resume function. This timeframe maybe increased to sixty (60) minutes on a case by case basis as approved by the CIO and/or ITS Security Team.

(ii) Kiosk access to network resources shall be controlled via network security provisioning.

(iii) Guest accessible SCG devices shall provide guest access to guest network resources for non-SCG personnel as controlled by network security provisioning, and shall be subject to an inactivity timeout lock after 60 minutes or less of inactivity depending on access granted through the device.

(iv) Guest Devices (wired and wireless) shall be managed as follows [PCI DSS 1.4.a / 1.4.b];

- All owners and users of guest devices will be required to review and acknowledge the SCG Acceptable Use statement prior to being permitted access to network resources.

- Guest Wireless Devices will only be connected to the SCG Guest Network.
- They shall be granted access to SCG network resources based upon need and function.
- They will be required to go through a SCG Firewall for all network resource access.
- They shall not be permitted direct access to internal secure network environments and resources. Access to internal resources will be limited to Guest Devices connecting via approved remote desktop access technologies through SCG network devices.
- They are subject to automatic disconnection after a period of inactivity not to exceed 15 minutes, as specified in the SCG ITS Information Security Policy [PCI DSS 12.3.8].
- Guest Device access to network resources will be removed upon expiration of the approved access timeframe.

(v) Workstations connected to the Shelby County network will adhere to the provisions of the "Wireless Networks" section of this security policy (section 7.5 above).

(vi) Printers and Workstations are not allowed to connect to network until the MAC address of the workstation's NIC has been enabled in the end-point switch-port configuration (see section 7.1.9 above).

(vii) All Shelby County workstations, especially those holding or handling credit cardholder data, must be protected with virus scanning software, the patch levels and virus signature databases of which must be kept up to date. Exceptions and exclusions for folder and file scanning must be justified in writing and approved by ITS Administration.

(viii) Functionality of Public Access computing devices will be limited to the minimum data and application access required.

(ix) All Shelby County workstations, especially those holding or handling credit cardholder data, must have OS and service software patch levels up to date. All OS and service software patches are to be tested for functionality before being implemented. Exceptions and exclusions for patches must be justified in writing and approved by ITS Administration.

j) Server Specific Security

(1) Server Security

(i) All Shelby County servers, especially those holding or handling credit cardholder data, must have OS and service software patch levels up to date. All OS and service software patches are to be tested for functionality before being implemented. Exceptions and exclusions for patches must be justified in writing and approved by ITS Administration.

(ii) All Shelby County servers, especially those holding or handling credit cardholder data, must be protected with virus scanning software, the patch levels and virus signature databases of which must be kept up to date. Exceptions and exclusions for folder and file scanning must be justified in writing and approved by ITS Administration.

(iii) Security logs on all Shelby County servers will be forwarded to ITS logging server for analysis and reporting. The logs are to be restorable for at least three (3) months, and retained for a period of one (1) year. The logs/alerts are reviewed daily [PCI DSS 10.7.a / PCI DSS 10.7.b].

(iv) Servers will be located in the secured computer site designated for the network campus they service.

(v) Servers storing or processing PCI DSS data will be implemented with no more than one primary function resident per server. This serves to prevent functions that require different security levels from co-existing on the same server [PCI DSS 2.2.d / 2.2.1.a].

(vi) Where appropriate the server console feature will be activated, and only System Administrators or ITS-authorized support staff members will be permitted to logon locally at the console. This access will be controlled and monitored using ADS groups.

(vii) Remote management passwords will be different from the Admin/Administrator/root password.

(viii) Users possessing Admin/Administrator/root permissions will be limited to trained members of the ITS staff or support staff that has been authorized by the department identified as "owner" of a server.

(ix) Use of the Admin/Administrator/root accounts will be kept to a minimum.

(x) Access control features will be enabled ensuring users access to file system data and applications will be limited to the minimum permissions needed.

(xi) Server consoles will employ inactivity timeout of ten (10) minutes, locking the console such that the console user's network password is required to re-activate access through the console.

(2) UNIX and Linux Servers

(i) ITS staff requiring root access must make use of the "su" command.

(ii) All UNIX and Linux system and service accounts will be limited in access and password protected.

(iii) rlogin facilities will be restricted to authorized ITS staff only.

(iv) FTP and SSH facilities will be restricted to authorized ITS staff only.

(v) Telnet facilities will be restricted to authorized users.

(vi) User's access to data and applications will be limited by the access control features.

(vii) Servers storing or processing PCI DSS data will be implemented with no more than one primary function resident per server. This serves to prevent functions that require different security levels from co-existing on the same server [PCI DSS 2.2.1.a].

(viii) System logs on all Shelby County servers will be forwarded to ITS logging server for analysis and reporting. The logs are to be restorable for at least three (3) months, and retained for a period of one (1) year. The logs/alerts are reviewed daily.

k) Voice Systems Security

(1) DISA port access (using inbound 0800 numbers) on the PBX will be protected by a secure password.

(2) The maintenance port on the PBX will be protected with a secure password.

(3) The default DISA and maintenance passwords on the PBX will be changed to user defined passwords.

(4) Call accounting will be used to monitor access to the maintenance port, DISA ports and abnormal call patterns.

(5) DISA ports will be turned off during non working hours.

(6) Internal and external call forwarding privileges will be separated, to prevent inbound calls being forwarded to an outside line.

(7) The operator will endeavor to ensure that an outside call is not transferred to an outside line.

(8) Use will be made of multilevel passwords and access authentication where available on the PBX.

(9) Voice mail accounts will use a password with a minimum length of four (4) digits.

(10) The voice mail password should never match the last four digits of the phone number.

(11) The caller to a voice mail account will be locked out after three attempts at password validation.

(12) Telephone bills will be checked carefully to identify any misuse of the telephone system.

l) Card Reader Device Security

(1) All SCG Offices and Divisions accepting Credit Card payments through Credit Card Terminals, Credit Card Readers, or Point of Sale Terminals will maintain a list of these devices to include at a minimum [9.9];

(i) The system connected to by the device,
(ii) The system processor,
(iii) The device location [9.9.1.a],
(iv) The device model [9.9.1.a],
(v) The serial number [9.9.1.a],
(vi) The departmental contact, and
(vii) And the Office or Division's Merchant ID.

(2) All SCG Offices and Divisions accepting Credit Card payments through Credit Card Terminals, Credit Card Readers, or Point of Sale Terminals will maintain policies and procedures requiring that;

(i) Devices that capture payment card data via direct physical interaction are periodically inspected for tampering or substitution [9.9.2].
(ii) Personnel are trained to be aware of suspicious behavior and to report tampering or substitution of devices [9.9.3].
(iii) Suspicious behavior and tampering or substitution of devices are reported to the Office or Division and the ITS Security Services Department (9.9).

m) Applicability of Other Policies

This document is part of the county's cohesive set of security policies. Other policies may apply to the topics covered in this document and as such the applicable policies should be reviewed as needed.

n) Enforcement:

The Security Officer will enforce this policy. Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities are suspected, the county will report such activities to the applicable authorities.

o) Policy Owner:

Shelby County Commission

p) Policy Administrator:

Chief Information Officer, Department of Information Technology Services

q) Policy Approval Date:

Current Revision Review Date: 08/01/2016
Current Revision 2.8 Approval Date: 10/03/2014
Original Version 1.0 Approval Date: 11/17/2003

r) Policy Effective Date:

Current Revision 2.8 Effective Date: 10/03/2014
Original Version 1.0 Effective Date: 11/17/2003

s) Compliance:

PCI DSS Requirement 8.5
PCI DSS Requirements 1.4.a and 1.4.b
PCI DSS Requirement 2.2.1.a
PCI DSS Requirement 9.9
PCI DSS Requirement 9.9.a
PCI DSS Requirement 9.9.b
PCI DSS Requirement 9.9.c
PCI DSS Requirement 12.3.8
PCI DSS Requirement 12.3.9
PCI DSS Requirement 12.3.10.a

t) Supporting Form(s):

Access Request Form
Acceptable Use Policy
Access Request Submission Procedure
Card Reader Inspection Procedure

u) Definitions:

(1) Access Control - The process of limiting access to the resources of a system only to authorized programs, processes, or other systems.

(2) ADS - A Microsoft directory used in Windows environments that stores information about an organization's attributes and provides a number of network functions. An Active Directory consists of a variety of objects which are organized for easy access by administrators and end users. The AD has a hierarchical structure that separates objects into three categories: resources, such as printers and other hardware; services, such as email; and user account information. Administrators are able to control access to these objects and set securities.

(3) Alarm Zoning - The ability to zone the intruder alarm from the main control panel should be provided to enable authorized usage of other areas of the

building outside normal hours, while retaining alarm detection within the room or AREA.

(4) Area - Two or more adjacent linked rooms which, for security purposes, cannot be adequately segregated in physical terms.

(5) Audit Trail - A chronological record of system activities that is sufficient to enable the reconstruction, reviewing, and examination of the sequence of environments and activities surrounding or leading to an operation, a procedure, or an event in a transaction from its inception to final results

(6) Authenticate - To verify the identity of a user, device, or other entity in a computer system, often as a prerequisite to allowing access to resources in a system

(7) Authorization - The granting of access permission to a user, program, or process

(8) C2 Security - American security classification generally accepted world-wide, classifying the level of security provided

(9) Categories of Risk

(i) SECURITY LEVEL 1: the security measures detailed in Level 1 are guidelines for public access PC's or all COMPUTER EQUIPMENT not described below.

(ii) SECURITY LEVEL 2: these guidelines apply where a single room or AREA contains PC's where the total replacement value of this hardware is LESS than $20,000 per room or AREA.

(iii) SECURITY LEVEL 3: these guidelines apply where a single room or AREA contains PC's where the total replacement value of this hardware is between $20,000 and $50,000 per room or AREA.

(iv) SECURITY LEVEL 4: these guidelines apply where a single room or AREA contains PC's where the total replacement value of this hardware is in excess of $50,000 per room or AREA.

(10) COMPUTER SITE - These guidelines apply to the location or room comprising the purpose built computer site.

(11) CE - Products which meet the essential requirements of European Community directives for safety and protection carry this mark. Products which carry the CE mark may be sold anywhere in the community.

(12) Computer Equipment - All computer equipment not contained within the Computer Site which will include PC's, monitors, printers, disk drives, modems and associated and peripheral equipment.

(13) Computer Site - Mainframe, minicomputer, file or application server plus all inter-connected wiring, fixed disks, telecommunication equipment, ancillary, peripheral and terminal equipment linked into the mainframe, contained within a purpose built computer site.

(14) DISA - Direct inward system access. DISA is used to allow an inward-calling person access to an outbound line. Many PBXs have inbound 0800 numbers for employee use. Employees use them to retrieve their voice mail and to speak to people in the office

(15) Discretionary Access Control - A means of restricting access to objects based upon the identity and need to know of the user, process, and/or groups to which they belong

(16) File Security - The means by which access to computer files is limited to authorized users only.

(17) Fire Suppression - Fire suppression systems and local fire extinguisher equipment. Firewall - A device and/or software that prevents unauthorized and improper transit of access and information from one network to another

(18) Ftp - File transfer protocol. Protocol that allows files to be transferred using TCP/IP

(19) Guest Access – Access to SCG administered resources by non-SCG personnel.

(20) Guest Device – Any untrusted device not administered by SCG or SCG approved business partners accessing SCG guest network resources. Guest devices may also be referred to as Bring Your Own Device (BYOD) devices [PCI DSS 1.4.a / 1.4.b].

(21) Guest Network Resources – Access permitted via the SCG network to the internet and to designated guest-accessible SCG devices and systems.

(22) High Risk Situation(S) - This refers to any room or AREA which is accessible;

(i) At ground floor level.

(ii) At any level accessible from adjoining roof, external fire escapes, or other features providing access.

(iii) Rooms in remote, concealed or hidden areas.

(23) Hub - Network device for repeating network packets of information around the network

(24) Identification - The process that enables recognition of an entity by a system, generally by the use of unique machine-readable user names.

(25) Internet - Worldwide information service, consisting of computers around the globe linked together by telephone cables

(26) Kiosk – A multi-user device granted specific access to SCG ITS resources based upon its function. Kiosks are utilized in all environments ranging from secure offices to public locations, depending upon their function.

(27) LAN Analyzer - Device for monitoring and analyzing network traffic. Typically used to monitor network traffic levels. Sophisticated analyzers can decode network packets to see what information has been sent

(28) Malware - Malware is a general term for software programs that have been designed with or can be used for malicious intent. These include viruses, worms and Trojans.

(29) Mandatory Access Control - A means of restricting access to objects based upon the sensitivity of the information contained in the objects and the formal authorization of subjects to access information of such sensitivity.

(30) Modem - Device which allows a computer to send data down the telephone network.

(31) Password - A protected, private character string used to authenticate an identity.

(32) PBX - Private branch exchange - small telephone exchange used internally within an organization.

(33) Personal Computers (PC's) - Individual computer units with their own internal processing and storage capabilities.

(34) Rlogin - Remote login. Protocol that allows a remote host to login to a UNIX host without using a password.

(35) Sensitive areas - Refers to any data center, server room or any area that houses systems that store, process, or transmit cardholder data. This excludes the areas where only point-of-sale terminals are present, such as the cashier areas in a retail store.

(36) Shareware - Software for which there is no charge, but a registration fee is payable if the user decides to use the software. Often downloaded from the Internet or available from PC magazines. Normally not that very well written and often adversely effects other software.

(37) Surveillance - Security surveillance and video recording in accordance with Shelby County Video Surveillance Policy.

(38) Telnet - Protocol that allows a device to login in to a UNIX host using a terminal session.

(39) UPS - Uninterruptible power supply. A device containing batteries that protects electrical equipment from surges in the mains power and acts as a temporary source of power in the event of a mains failure.

(40) Username - A unique symbol or character string that is used by a system to identify a specific user.

(41) Virus - Computer software that replicates itself and often corrupts computer programs and data.

(42) Voice Mail - Facility which allows callers to leave voice messages for people who are not able to answer their phone. The voice messages can be played back at a later time.

(43) Workstation - An electronic computing device, for example, a laptop or desktop computer, or any other device that performs similar functions, and electronic media stored in its immediate environment. Workstations, whether owned by SCG or outside parties, intended to be accessed by non-SCG employees, shall be provisioned as kiosks or guest workstations.

v) Appendices:

4. Firewall and Router Configuration Standard

a) Policy Intent:

The purpose is to describe the minimum required firewall and router configurations to protect internal network resources from unauthorized access.

b) Scope:

This policy applies to all firewall and routers connected to Shelby County Government's network.

c) Policy:

(1) Firewall and Router Rulesets will be reviewed at least once every six months and the results will be documented in the "Firewall Router Ruleset Review Log".

(2) Changes to routers and firewalls follow this process:

(i) The customer requests modification of functionality through a work order.

(ii) Requests requiring Router or Firewall Access Control List (ACL) configuration changes affecting VLANs are;

- Defined by ITS Netdesign
- Reviewed and approved by ITS Security
- Implemented by ITS NetDesign

(iii) Requests requiring Router or Firewall configuration changes not related to ACLs are defined, reviewed, approved, and implemented by ITS Netdesign

(3) Physical Security

(iv) Physical access to all firewalls and routers must be restricted by lock and key mechanism either physically or electronically.

(v) Only members of the NetworkDesign AD group or Dom ITEC Customer Support AD group may install, uninstall, move, perform maintenance upon, or change the physical configuration of a firewall or router.

(vi) Only members of the NetworkDesign AD group may make physical connections to a firewall including direct access ports, console ports, etc.

(vii) Only members of the NetworkDesign AD group or Dom ITEC Customer Support AD group may make physical connections to a router including direct access ports, console ports, etc.

(viii) In the event a firewall or router suffers physical damage or there is evidence of tampering, it will be fully evaluated by hardware diagnostics and the physical configuration checked with existing documentation.

(4) Configuration Requirements

(i) Only members of the NetworkDesign AD group or Dom ITEC Customer Support AD group may do the following:

- Log in directly to a network device's console port or other direct access port.
- Assume administrative privileges on a network device
- Log in to the network device remotely

(ii) Any configuration changes will be approved and implemented in accordance with the Shelby County Information Technology Services Change Management Policy.

(iii) Firewall and router password policies shall comply with the Shelby County Information Technology Services password policies.

(iv) Firewall and routers shall limit administrative access to Shelby County Government networks that are firewalled from any untrusted source.

(v) A demilitarized zone (DMZ) will be used to filter and screen all traffic and to prohibit direct routes for inbound and outbound Internet traffic [PCI DSS 1.3.1].

(vi) Firewall and/or router configurations will restrict outbound traffic from payment card applications to IP addresses within the DMZ [PCI DSS 1.3.5].

(vii) Port address translation (PAT) or network address translation (NAT) will be used to prevent internal addresses from being revealed on the Internet.

(viii) Firewalls are to be placed at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone [PCI DSS 1.1.3.a].

(ix) Firewalls will restrict inbound Internet traffic to IP addresses within the DMZ.

(x) Firewalls will not allow internal IP addresses to pass from the Internet into the DMZ.

(xi) Stateful inspections will be enabled on each firewall. The protocols that will use stateful inspections will depend on business needs [PCI DSS1.3.6].

(xii) Firewalls will be installed between any wireless networks and the cardholder data environment. These firewalls will be configured to deny any traffic from the wireless environment or from controlling any traffic [PCI DSS 1.2.3].

(xiii) Personal firewall software will be installed on any mobile and employee-owned computers with direct connectivity to the Internet which is used to access Shelby County Government's network [PCI DSS 1.4.a].

(xiv) No local user accounts will be configured on the router except one emergency account. Routers will use TACACS+ for all user authentication and only members of the Network Design AD group will have administrative access to these devices.

(xv) The enable password on the router must be kept in a secure encrypted form. The router must have the enable password set to the current production router password standard.

(xvi) Firewalls must deny all inbound traffic not specifically allowed.

(xvii) Router access control list will be added as business needs arise.

(xviii) All access control list on firewalls and routers must end with an implicit deny all.

(xix) Each router will have the following statement in clear view after a successful login:

```
&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&
&&&&       Shelby County Government      &&&&
&&&&        Information Technology       &&&&
&&&&                                     &&&&
&&&&      -- Unauthorized Access is --   &&&&
&&&&      !!! STRICTLY PROHIBITED !!!    &&&&
&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&&
```

(xx) The protocols SSH, HTTPS, and VPN are allowed to be used for administering all firewalls and routers.

(xxi) A documented list of services and ports that are necessary for business will be identified on the Firewall Application Traffic Ruleset Form. Documentation will include justification for protocols besides hypertext transfer protocol (HTTP) and secure sockets layer (SSL), secure shell (SSH), and virtual private network (VPN). Justification includes reason for use of protocol and security features implemented. All protocols are only approved by Information Technology Services Network Design group or the Technical Support Manager only after completion of a risk assessment are risky protocols permitted [PCI DSS1.1.5.a / 1.1.5.b].

(xxii) All firewall changes follow the standard Shelby County Government change management procedures. Additionally, only authorized full time staff can request firewall changes. The request must be submitted on a "Firewall Change Request Form" signed by an authorized requestor. Only the Information Technology Services Network Design group or the Technical Support Manager will approve the change control request form and ensure the firewall change request form has been completed. Each request is then considered for final approval and implementation following the standard change management procedures. All requests are evaluated and assessed against current industry best practices [PCI DSS1.1.1].

(5) Network Diagram

(i) A current network diagram will be maintained which displays all connections to cardholder data, including wireless networks.

(ii) Diagram must show credit card databases segregated from the DMZ and Internet.

(6) Monitoring

(i) All firewalls and router access control lists will be reviewed on a quarterly basis.

(ii) The List of Approved Access Control Lists will be reviewed on a quarterly basis.

(7) Procedure

(i) See the Shelby County Policy for Firewalls.doc

d) Applicability of Other Policies:

This document is part of the county's cohesive set of security policies. Other policies may apply to the topics covered in this document and as such the applicable policies should be reviewed as needed.

e) Enforcement:

The Security Officer will enforce this policy. Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities are suspected, the county will report such activities to the applicable authorities.

f) Policy Owner:

Shelby County Government

g) Policy Administrator:

Chief Information Officer, Department of Information Technology Services

h) Policy Approval Date:

Current Revision Review Date: 08/01/2016
Current Revision 1.0 Approval date: 10/03/2014
Original Version 1.0 Approval date: 09/04/2012

i) Policy Effective Date:

Current Revision 1.0 Effective Date: 10/03/2014
Original Version 1.0 Effective Date: 09/04/2012

j) Compliance:

PCI DSS Requirement 1.1.4 and 1.1.5.a, 1.1.6, 1.1.7

k) Supporting Form(s):

Firewall Router Ruleset Review Log
Firewall Application Traffic Ruleset Form

Protocol	Source (IP or hostname)	Source Ports	Destination (IP or hostname)	Destination Ports	Work Order #	Business Justification

l) Definitions:

m) Appendices:

5. Acceptable Use Policy v1.4.b

1. Purpose:

Shelby County Government (SCG) has adopted the following Acceptable Use Policy (AUP) to protect SCG and its employees from liability and business interruptions due to inappropriate use of Information Technology Services (ITS) resources and breaches of computer security.

2. Scope:

This policy applies to all SCG employees, vendors, contractors, business partners, consultants, interns, temps, and other workers (herein termed "users") using SCG provided ITS resources, network, hardware and/or software, in their assigned job responsibilities.

This policy applies to the use of all devices utilized to access SCG ITS resources. This includes but is not limited to the usage of network, devices, software, authentication credentials, and other SCG ITS resources. This applies to all usage whether on or off network.

This policy applies to the access and use of SCG ITS managed data and sensitive data. The term "sensitive data" within this policy is defined as SCG confidential data, Payment Card Industry cardholder data, Protected Health Information, or other compliance-related data.

3. Policy:

It is the policy of SCG ITS to define the acceptable and unacceptable uses of SCG ITS resources to facilitate SCG business functions. Acceptable use of SCG ITS resources will result in continued accessibility and reliability of the resources. Unacceptable use of SCG ITS resources will result in reduced accessibility to resources, increased overhead, and increased liability risks to SCG. All users are expected to take an active role in ensuring that this policy is followed and that SCG ITS resources are used in the acceptable manner.

1. Acceptable Use and Responsibilities:

a. Users are permitted access to SCG computer resources for the purpose of conducting SCG business processes upon approval by the appropriate SCG designated approving authorities.

(i) Access is activated upon receipt and approval of a properly completed and approved access request form.

(ii) Access is be limited to the timeframe requested and will be disabled at the requested time or upon notification of termination of the user's relationship (employment, contractual or otherwise) with SCG.

(iii) User access privileges are granted on a need-to-know (least privilege) basis [PCI DSS 7.1.1 / 10.4.2.a].

(iv) Users are responsible for all access and communications originating from equipment and accounts assigned to them.

b. Users shall take an active role in securing their access credentials, the data to which they are granted access, and the hardware utilized to access said data.

(i) Users are responsible for the security of their assigned passwords and accounts. The sharing of assigned user identification or password information with anyone is strictly prohibited [PCI DSS 8.5.8.b].

(ii) Users assigned portable devices shall exercise special care to assure they are not misused, lost or stolen.

(iii) Users shall secure all assigned PCs, laptops and workstations by activating the password-protected screensaver or logging-off of the host when leaving it unattended

(iv) Users shall ensure that any device utilized by them to access SCG ITS resources, whether owned by the user or SCG, is continually executing approved virus-scanning software with current virus signatures.

(v) Users shall not open any unexpected email attachments received from any sender without first validating the authenticity of the message with the sender. Unauthenticated suspect emails should be reported to the SCG ITS Service Desk.

(vi) Users shall immediately report any suspected security breach or loss of data to the SCG ITS Service Desk and, where ever possible, take appropriate action to mitigate and contain the effect of such breaches.

C. Users shall take an active role in maintaining the security of sensitive data.

(i) Users are responsible for utilizing appropriate measures to prevent unauthorized access to sensitive data.

(ii) Users of SCG ITS systems are prohibited from unauthorized copying, moving, or storing of sensitive data, to or on local hard drives, removable electronic media, or Internet and cloud based storage.

(iii) Users of SCG ITS systems are prohibited from unauthorized copying, moving, or storing of sensitive data via remote access technologies.

(iv) Users shall not request or send credit card data or PAN via fax, phone, written format, verbally, or using other electronic messaging technologies [PCI DSS 4.2.b].

(v) Users shall not send sensitive data including unencrypted Protected Health Information via email. Users that receive any email containing sensitive data must report the email to the SCG ITS Service Desk.

(i) Users shall not leave voicemail messages containing SCG sensitive data on any phone system utilized to conduct Shelby County business including County office extensions, County-provided cell phones, personal land lines, and personal cell phones.

(ii) Users shall delete and not duplicate any messages containing sensitive data from any phone system utilized to conduct Shelby County business including County office extensions, County-provided cell phones, personal land lines, and personal cell phones.

(iii) Users shall report the receipt of voicemails containing sensitive information to the SCG ITS Service Desk.

(iv) Users shall only leave voicemail messages containing sensitive data on the phone systems of Shelby County Government business partners, business associates, or contractors who; 1) have current contracts or business associate agreements in place with SCG, 2) where there is a need to know directly related to the data, and 3) where

the partner, associate, or contractor permits the disclosure of sensitive data via voicemail. Card Holder Data is never appropriate to leave or receive in a voicemail.

(v) Users shall not post or make available to newsgroups, social media, or other public forums any SCG sensitive data.

(vi) Users shall only post to newsgroups, social media, or other public forums as required to fulfill SCG assigned duties. Utilization of SCG email addresses to facilitate such postings must have prior SCG administrative approval.

d. SCG shall ensure compliance with this policy.

(i) SCG shall secure and maintain the privacy of all data stored or transmitted by SCG ITS systems to comply with applicable legal requirements and SCG policy. All data not protected by these requirements may be discoverable through public records request or other applicable methods.

(ii) SCG will gather and report on information regarding the usage of SCG ITS resources for SCG business or management purposes. Usage reports include, but are not limited to, resources utilization, Internet accesses, and security-related activities.

(iii) SCG shall utilize various data capture, analysis techniques, and tools to facilitate maintenance, audit, and installation functions on behalf of its customers. Such tools and techniques shall be used in accordance with the established iSLA agreement.

e. Personal use of SCG ITS resources is restricted in accordance with SCG policy.

(i) Users shall minimize personal use of SCG ITS resources.

(ii) Users are responsible for exercising good judgment regarding the reasonableness of minimal personal use. If users are uncertain about the reasonableness of a given use, they must consult with their supervisor or manager.

(iii) Personal use must not interfere with employees fulfillment of their job responsibilities, interfere with other users' access of resources, be excessive (as determined by management), result in significant added costs to SCG, disrupt SCG business processes, or cause any other disadvantage to SCG.

(iv) Reasonable personal use does not state or imply SCG endorsement and must not interfere with an employee's job performance or activities which directly support the County's mission.

(v) Users shall have no expectation of privacy for any usage of SCG ITS resources not specifically related to the performance of SCG business functions.

2. Unacceptable Uses:

a. Users shall not knowingly or through carelessness breach or attempt to breach SCG ITS security measures or adversely impact the normal functioning of SCG ITS resources.

(i) Users shall not circumvent the user authentication or security of any device, application, or other resource.

(ii) Users shall not attempt to access data for which the user is not authorized, or attempt to access a resource or account the user is not expressly authorized to use.

(iii) Users shall not utilize any form of device or application to intercept or capture data in transit.

(iv) Users shall not utilize any program, script, command, message, or other technique to interfere with or impede any SCG business process.

(v) Users shall not remove, disable, or render non-functional any identifying labels or tracking devices from SCG ITS resources.

b. Users shall not utilize SCG ITS resources to engage in any activity that is illegal under local, state, federal or international law.

(i) Users shall not violate the legal rights of any person while utilizing SCG ITS resources.

(ii) Users shall not violate copyright, trade secret, patent or other intellectual property, or similar laws or regulations through the installation or distribution of "pirated" (unlicensed or copyrighted) software or software products that are not appropriately licensed for use by SCG.

(iii) Users shall not install or utilize any unlicensed, pirated, or illegally obtained software on SCG ITS resources.

(iv) Users shall not install or utilize any software on SCG ITS resources without prior approval of the appropriate SCG ITS authority.

(v) Users shall not utilize SCG ITS resources to connect to any external systems without the approval of the appropriate SCG ITS authority.

(vi) Users shall not make copies of copyrighted material such as photographs, magazines, books, or music.

(vii) Users shall not export software, technical information, or encryption software or technology which is illegal under international or regional export control laws.

(viii) Users shall not utilize SCG ITS resources or credentials to actively engage in the procurement or transmission of material that is in violation of sexual harassment or hostile workplace laws.

(ix) Users shall not utilize SCG ITS resources or credentials to make fraudulent offers of products, items, or services.

c. Users shall not utilize any devices to access SCG ITS resources without prior approval of the appropriate SCG ITS authority.

d. Users shall not utilize SCG ITS resources in an inappropriate manner that disrupts SCG business processes or causes any other disadvantage to SCG.

e. Users shall not utilize SCG ITS messaging systems in an inappropriate manner.

(i) Users shall not provide SCG internal contact lists or employee personal information to outside parties.

(ii) Users shall not utilize SCG ITS resources or SCG email accounts to distribute bulk messages for any purpose other than SCG business.

(iii) Users shall not utilize SCG email accounts to register for email notifications not directly related to their SCG responsibilities. These include, but are not limited to, news, social media, coupon, Sales Circulars or Notifications, and any other email communications not directly related to the employee's duties with SCG.

(iv) Users shall not alter or otherwise forge any message header information.

(v) Users shall not utilize SCG ITS resources to harass any person, group, or organization.

(vi) Users shall not create or forward any "chain letter" messages.

f. Users shall not make statements about warranty, express or implied, concerning SCG ITS resources unless such statements are required as part of the user's job duties and are approved by the appropriate SCG ITS authority.

g. Users shall not utilize SCG resources to participate in online or Internet-based gaming.

3. Applicability of Other Policies:

This document is part of the SCG Information Technology Services cohesive set of security policies. Other policies may apply to the topics covered in this document and as such the applicable policies should be reviewed as needed.

4. Enforcement:

Any user who fails to comply with this policy may be subject to loss of access to SCG ITS resources and disciplinary action, up to and including termination of employment. Shelby County Government actively restricts receipt of specific email types including but not limited to coupon, sales circulars or other such notifications.

5. Policy Owner:

Shelby County Government

6. Policy Administrator:

Chief Information Officer, Department of Information Technology Services

7. Policy Approval Date:

Current Revision Review Date:	08/01/2016
Current Revision 1.4.b Approval date:	09/01/2016
Original Version 1.1 Approval date:	01/09/2013

8. Policy Effective Date:

Current Revision 1.4.b Effective Date:	09/01/2016
Original Version 1.1 Effective Date:	01/09/2013

9. Compliance:

PCI DSS Requirement 12.3.1.

10. Acceptable Use Policy 1.4.b Sign-off:

As an employee, vendor, or third party user of Shelby County Government Information Technology Services provided resources, I certify, by signing below, that I have been given a copy of the Shelby County Government Information Technology Services Acceptable Use Policy.

I understand that it is my responsibility to thoroughly read the policy and request additional information or clarification from my supervisor or Shelby County Government contact if I do not understand any information contained in the policy.

_____ _____
Print Name Print Title

_____ _____
Signed Date

Data Security – Vendor/Business Partner Acknowledgement Agreement

It is the policy of Shelby County Government (SCG) to do business only with Vendors and SCG Business Partners (Business Partners) who safeguard and maintain the security of SCG's confidential data in accordance with applicable standards. All SCG Business Partners, and their employees, whether working onsite at SCG locations, or having access to SCG secure network and cardholder environment, must agree to meet the spirit and intent of all compliance requirements relating to the content of data accessed. This includes, but is not limited to, Payment Card Industry (PCI) data, Protected Health Information (PHI), and Personally Identifiable Information (PII) in electronic and paper format.

Payment Card Industry (PCI) Data:
Either of the following constitutes PCI Data:

1. Data including the complete or partial Primary Account Number (PAN)
2. Data including the complete or partial PAN stored in conjunction with the Cardholder Name, Security Code, and/or Expiration date.

Protected Health Information (PHI):
Information relating to an individual's past, present or future physical or mental health or condition, the provision of health care to the individual, or, the past, present, or future payments for the provision of health care to the individual.

Personally Identifiable Information (PII):
Any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.

The Business Partner shall continuously monitor their network for breaches and will, in the event of a discovered breach, immediately apply appropriate corrective actions to contain and prevent recurrence, and, notify the SCG ITS Security Officer of the breach. The Business Partner additionally agrees to, upon request from SCG ITS, provide a report on the Business Partner's controls relevant to security, confidentiality, integrity and privacy of data. The Business Partner or employee thereof, agrees not to appropriate sensitive data for their own use or to disclose such information to third parties unless specifically authorized by SCG in writing.

As an SCG Business Partner or employee thereof, I acknowledge that I have read these requirements and will comply at all times.

Company Name: _____
Name: _____
Signature: _____
Title: _____ Date: _____

SCG-ITS Sponsor: _____
Signature: _____
Title: _____ Date: _____
Time Period: From: _____ To: _____

6. Data Encryption and Key Management Policy

a) Policy Intent:

Shelby County Government (SCG) has adopted the following Data Encryption Policy to establish guidelines for the acquisition and use of keys to encrypt and decrypt sensitive data. The practical intent of this policy is to secure the SCG's data.

b) Scope:

The scope of this policy covers all Shelby County Government network users, computers, and sensitive data stored on county-owned, county-leased, and otherwise county-provided systems and media, regardless of location.

c) Policy:

It is the policy of Shelby County Government that data classified as sensitive or confidential be encrypted at rest, in motion, and in use, and that the Public Key Infrastructure and the keys and certificates used for data encryption within Shelby County will be requested, issued, and secured in accordance within the following guidelines:

(1) Certification Authority (CA) keys and certificates will be secured through use of a protected off-line Root CA, the certificates and keys for which are archived in an encrypted form using a Key Encryption Key (KEK) and stored on a CD-R or encrypted USB "thumb-drive" kept in a locked container in the locked vault at the East Data Center.[PCI DSS 3.6.3 / PCI DSS 3.6.5.a / 3.5.2.a / 3.5.2.b]
(2) Root CA and Issuing subordinate CA keys and certificates are issued for 5-year period, require password and object identifier, and will use the highest bit-length and strongest hash algorithm readable by all computers currently in use on the Shelby County network (currently 2048-bit and SHA-1 algorithm). [PCI DSS 2.3.c / 3.4.1.b / 3.6.1 / 4.1 / 4.2.a / 8.4.a]
(3) Two CA Administrators, a primary and a backup, are appointed by the Technical Support Manager. The two CA Administrators, after signing the Key Custodian Acceptance Form, act as the sole Key Custodians for the Shelby County Government encryption system. [PCI DSS 3.5.1 / 3.6.8]
(4) Virtual machines hosting root and subordinate CAs are only accessible by Security Officers and CA Administrators, and all logon/logoff, privilege use, object access events are logged in the Logging and Event Management (LEM) system.
(5) User and machine data, session and email encryption certificates and keys are issued only as needed for 3-year period, and require password and object identifier. Default certificates and keys provided by vendors are replaced by certificates and keys issued in-house.[PCI DSS 2.1.1.a]
(6) Digital Signature certificates and keys are issued only as needed for 3-year period, but do not require password or object identifier.
(7) All keys and certificates will be secured in the Active Directory database and will use the highest bit-length and strongest hash algorithm readable by all computers currently in use on the Shelby County network (currently 2048-bit and SHA-1 algorithm).[PCI DSS 2.3.c / 3.4.1.b / 4.1 / 4.2.a / 8.4.a / 3.5.2.a / 3.5.2.b / 3.6.3]
(8) Key encryption keys (KEK), used to encrypt symmetric keys for secure distribution, must use a stronger algorithm with a key of the longest key length for that algorithm. [PCI DSS 3.6.2]. If the keys being encrypted are for the strongest algorithm, then the key must be split, each portion of the key encrypted with a different KEK that is the longest key length authorized and the each encrypted portion is transmitted using different transmission mechanisms. Key encryption keys, when at rest, must be protected with security measures at least as stringent as the measures used for distribution of that key.
(9) Public key cryptography, or asymmetric cryptography, uses public-private key pairs. The public key is passed to the certificate authority to be included in the digital certificate issued to the end user. The digital certificate is available to everyone once it issued. The

private key is available only to the end user to whom the corresponding digital certificate is issued.

(10) User certificates are revoked and keys destroyed by the CA Administrator when the user no longer needs it or the user leaves the employ of the Shelby County Government, and machine certificates are revoked and keys destroyed when the computer or application no longer needs it or the computer is decommissioned.

(11) Certificates are revoked and keys destroyed by the CA Administrator when compromise of the key is suspected, and new keys and certificates are issued to replace the destroyed keys and certificates.

(12) Certificate Revocation List (CRL) is published by the CA Administrator whenever a certificate is revoked, or at least monthly, to web-based on-line responder accessible from Internet and private network. [PCI DSS 3.6.5.a / 3.6.5.b / 3.6.5.c]

(13) Certificate renewal is a manual process requiring CA Administrator approval.

d) Procedure:

(1) Request / Acquisition of Certificates

(a) User or Machine requiring Certificates for encryption of email, files, or authentication are added to security groups in Active Directory Services based upon need for certificate processing through auto-enrollment.

(b) Web servers and email servers requiring SSL/TLS certificates will be enrolled manually through a certificate signing request.

(c) Applications requiring Code-Signing certificates will be enrolled manually through a certificate signing request, and will require CA Administrator to issue and distribute the certificates.

(2) Generation of Key Pairs

(a) Private key is generated by the requesting computer when the Certificate Signing Request is created.

(b) The public key is generated by the issuing subordinate CA in the issuing of the certificate.

(3) Securing Keys and Certificates

(a) Keys and certificates are secured in Microsoft Active Directory Services database.

(b) Backup copies of the Microsoft Active Directory Services database are encrypted.

(c) CA signing certificate for Root CA is archived onto CD or encrypted USB "thumb drive" and stored in locked cabinet in locked vault at East Data Center. Root CA is disconnected and powered off virtual machine.

(d) CA signing certificate for issuing subordinate CAs are archived onto CD or encrypted USB "thumb drive" and stored in locked cabinet in locked vault at East Data Center.

(4) Renewing Certificates

(a) Certificate renewal requests are made by the requesting computer through the web enrollment server.

(b) The certificate is renewed for an additional 3 years by the Certification Administrator at the issuing subordinate CA.

(5) Changing Keys

(a) Keys and certificates are changed by revoking the old and submitting a new certificate signing request.

(b) The new certificate is issued for 3 years by the Certification Administrator at the issuing subordinate CA.

(6) Revocation of Certificates

(a) Keys and certificates are revoked by the Certification Administrator at the issuing subordinate CA.

(b) A new Certificate Revocation List (CRL) is then published by the Certification Administrator at the issuing subordinate CA.

(7) Destruction of Keys and Certificates

(a) Keys and certificates are revoked by the Certification Administrator at the issuing subordinate CA.

(b) Keys and certificates are then deleted by the user at the local computer where they were used.

(c) A new Certificate Revocation List (CRL) is then published by the Certification Administrator at the issuing subordinate CA.

e) Applicability of Other Policies:

This document is part of the Shelby County Government Information Technology Services cohesive set of security policies. Other policies may apply to the topics covered in this document and as such the applicable policies should be reviewed as needed.

f) Enforcement:

The Security Officer will enforce this policy. Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities are suspected, the county will report such activities to the applicable authorities.

g) Policy Owner:

Shelby County Government

h) Policy Administrator:

Chief Information Officer, Department of Information Technology Services

i) Policy Approval Date:

Current Revision Review Date:			08/01/2016
Current Revision	1.0	Approval date:	10/03/2014
Original Version	1.0	Approval date:	09/22/2013

j) Policy Effective Date:

Current Revision	1.0	Effective Date:	10/03/2014
Original Version	1.0	Effective Date:	09/22/2013

k) Compliance:

PCI DSS Requirement 3.1
PCI DSS Requirement 3.5
PCI DSS Requirement 3.6

l) Supporting Forms:

Key Custodian Acceptance Form [PCI DSS 3.6.8]
Key Management Procedures - MVR Dealer

m) Definitions:

(1) Authentication - A security method used to verify the identity of a user and authorize access to a system or network.

(2) Backup - To copy data to a second location, solely for the purpose of recovery of that data.

(3) Encryption - The process of encoding data with an algorithm so that it is unintelligible without the key. Used to protect data during transmission or while stored.

(4) Mobile Data Device - A data storage device that utilizes flash memory to store data. Often called a USB drive, flash drive, or thumb drive.

(5) Two-Factor Authentication - A means of authenticating a user that utilizes two methods: something the user has, and something the user knows. Examples are smart cards, tokens, or biometrics, in combination with a password.

(6) U.S. DoD Standards - Stands for United States Department of Defense Standards. Standards on data destruction detailed in DoD 5220.22-M. Most data wiping software packages provide an option for wiping to this standard.

n) Appendices:

Shelby County Government

Date: _____

Name: _____

Job Description: _____

Supervisor: _____

I have read and understand the Shelby County Government Encryption Key Management Procedures, and I agree to adhere to said procedures.

I understand and accept the responsibilities of the key custodian as defined in the Shelby County Government Encryption Key Management Procedures.

Signature of Key Custodian _____ Date: _____

Approval of CIO _____ Date: _____

7. PKI Certificate Policy Statement

a) Policy Intent:

Shelby County Government (SCG) has adopted the following PKI Certificate Policy to provide client and server authentication and data encryption/decryption certificates for sole use of the internal Shelby County Government Network devices and users. Properly authenticated consumers may request certificates via Shelby County AD DS certificate enrollment processes or via the Web Enrollment Service.

b) Scope:

The scope of this policy covers all Shelby County Government Network devices and users and properly authenticated consumers requesting certificates via the Shelby County Active Directory Domain Server certificate enrollment processes or via the Web Enrollment Service.

c) Policy:

The below PKI functions are explicitly approved for the normal conduct of County business within Shelby County Government network. All other uses are implicitly forbidden:

(1) Server Authentication—

- (a) SSL/TLS certificates for internal-facing web services.
- (b) Computer certificates for identify verification.
- (c) Subject Alternative Name certificates will be issued instead of "wildcard" certificates to provide better security and ensure authentic identity.

(2) Client Authentication—

- (a) User certificates for identify verification (digital signature).
- (b) Email certificates for identity verification.
- (c) Smart-card certificates for user authentication and identification.

(3) Data Encryption—

- (a) Email encryption / decryption for internal emails only.
- (b) File and folder encryption / decryption for internal files.
- (c) ipsec network traffic encryption / decryption.

(4) Private Key Management –

- (a) Private key shall not be copied to any medium other than the device on which it is created.
- (b) The Private Key shall not be exported from the originating device.
- (c) Private keys shall not be exportable with the certificate.
- (d) If a user's private key becomes compromised, the user is required to notify the Shelby County Information Technology Services department at:

  Service.Desk@shelbycountytn.gov <mailto:Service.DesK@shelbycountytn.gov>
  Phone: (901) 222-2700

(5) Certificate enrollment / renewal

- (a) Certificates issued by the Shelby County PKI are valid for a period not to exceed 5 calendar years.

(b) Certificates may be requested via the "Certificates.msc" mmc snap-in, via the Certificate Enrollment Service or,

(c) Via the Web Enrollment Portal (http://wca.shelby.elink/CertSrv <http://wca.shelby.elink/CertSrv>), authentication is required.

(6) Public/private key pairs: Supported public and private keys shall have the following minimum and maximum parameters:

(a) Minimum key length 2048-bits (for RSA keys)

(b) Minimum key length 256-bits (for Eliptical Curve)

(c) Maximum key length 4096-bits (for RSA keys)

(d) Maximum key length 512-bits (for Eliptical Curve)

d) Applicability of Other Policies:

This document is part of the Shelby County Government Information Technology Services cohesive set of security policies. Other policies may apply to the topics covered in this document and as such the applicable policies should be reviewed as needed.

e) Enforcement:

The Security Officer will enforce this policy. Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities are suspected, the county will report such activities to the applicable authorities.

f) Policy Owner:

Shelby County Government

g) Policy Administrator:

Chief Information Officer, Department of Information Technology Services

h) Policy Approval Date:

Current Revision Review Date:			08/01/2016
Current Revision	1.0	Approval date:	08/01/2016
Original Version	1.0	Approval date:	08/01/2016

i) Policy Effective Date:

Current Revision	1.0	Effective Date:	08/01/2016
Original Version	1.0	Effective Date:	08/01/2016

j) Compliance:

PCI DSS Requirement 3.1
PCI DSS Requirement 3.5
PCI DSS Requirement 3.6

k) Supporting Forms:

Not Applicable

l) Definitions:

Not Applicable

8. Information Security Policy

a) Policy Intent:

This policy defines procedures providing clearly defined measures to protect the confidentiality, integrity and availability of Data and the Information Systems that store, process, or transmit the Data.

b) Scope:

This Policy applies to all employees and third-party Agents of Shelby County Government (SCG) as well as any other SCG affiliate who is authorized to access Institutional Data.

This policy applies to SCG in its entirety, including all systems, network, and applications that process, store or transmit sensitive information.

c) Policy:

Shelby County Government Information Technology Services (SCGITS) has adopted the following Information Security Policy addressing information security for employees and contractors of Shelby County Government (SCG).

d) Procedure

(1) The SCG ITS Information Security Policy will be reviewed updated annually, or as needed to reflect changes to business objectives or the risk environment [PCI DSS 12.1.3], and disseminated to all relevant employees and third-party agents of SCG, annually, by the SCGITS Security Officer [PCI DSS 12.1 / 12.5.1].

(2) SCGITS will conduct an annual risk assessment, utilizing the NIST SP800-30 methodology identifying threats and vulnerabilities in a formal risk assessment of the desktop, network, data center and application environments of Shelby County Government managed by SCGITS.

(3) SCGITS will develop and maintain administrative and technical daily operational procedures that are consistent with SCGITS policies and which include at a minimum, Data Retention and Disposal, Backup and Disaster Recovery, Change Management, System Maintenance, Incident Response/Security Breach, Service Provider Management, and Vulnerability Management procedures [PCI DSS 12.1.3 / 12.2].

(4) SCGITS will develop and maintain usage policies for critical employee-facing technologies (such as modems and wireless) defining their proper use for all employees and contractors. These usage policies require, at a minimum:

(i) Explicit management approval is required prior to the granting of authentication credentials to approved personnel [PCI DSS 12.3.1 / 12.3.5].

(ii) Access to all systems and technology containing, processing, or transmitting PCI-DSS data, regardless of location, will utilize an access control system approved by Shelby County Information Technology Services based upon unique IDs and/or other unique identifiers as defined in the Network Security Policy [PCI DSS 12.3.2 / 8.1].

(iii) Listings of devices handling, storing, or transmitting PCI-DSS data will be maintained by SCGITS within the approved Customer Support inventory management system according to the "Inventory Control Policies and Procedures". Listings of personnel permitted to access SCGITS-managed PCI-DSS data resources will be maintained within the approved Access Control Lists as documented in the Shelby County Network Security Policy respectively [PCI DSS 12.3.3].

(iv) SCGITS will utilize existing unique identifiers on devices, including but not limited to serial numbers, and/or custom labels to permit the correlation of said identifiers with the owner, their contact information, and the purpose of the device through cross reference of the host name and recorded in the inventory management system, as documented in the Acceptable Use Policy [PCI DSS 12.3.4].

(v) All network infrastructure equipment will be secured in acceptable locations for the technologies limiting access to Information Technology Services personnel and approved providers or contractors, through appropriate control methods including but not limited to electronic and physical key access methods [PCI DSS 12.3.6].

(vi) SCGITS maintains a comprehensive list of approved Information Technology products [PCI DSS 12.3.7].

(vii) All approved SCGITS remote access connections will be automatically disconnected after a period of inactivity not to exceed 30 minutes [PCI DSS 8.6.5.a / 12.3.8].

(viii) Activation of remote access devices or accounts required for use by SCGITS vendors must be approved by SCGITS. All remote access will be immediately revoked upon cessation of need, expiration of access request time frame (established upon initial request or periodic update), or cancellation or expiration of contracts with the vendor [PCI DSS 12.3.9].

(ix) SCITS policy prohibits the copying, moving, or storing of confidential data, including but not limited to, cardholder data and protected health information, onto local hard drives and removable electronic media when accessing such data via remote access technologies. Whenever possible, systems have been configured to disable copy capabilities, including cut-and-paste and print functions, during remote access.

(5) SCITS maintains policies and procedures clearly defining information security responsibilities for all employees and contractors.

(6) SCITS performs quarterly review of users granted domain administrator access to Servers and administrative access to Network Devices. These audits are performed by the ITS Security Officer and are documented on the "Approved Network Device Administrators" and "Approved Network Server Administrators" forms [PCI DSS 7.1.2].

(7) SCITS limits access to audit trails to employees with a job-related need [PCI DSS 10.5.1].

(8) SCIT requires the review of and processes audit log exceptions as defined in the "Audit Reports Review Procedure" [PCI DSS 10.6.a] [PCI DSS 10.6.b].

(9) SCITS has assigned the responsibility for information security management responsibilities to the current Security Officer (Shawn T. McClure as of April 2014) whose duties include the maintenance of the security policies and procedures, monitoring of security alerts and information, security incidence response and escalation procedures, administration of user accounts, and monitoring and control of all access to data [PCI DSS 12.5 / 12.5.1 / 12.5.2].

(i) The SCITS Security Officer (SO) is responsible for establishing and distributing security policies and procedures.

(ii) SCITS sections will be responsible for monitoring and analyzing threats relevant to their respective IT responsibilities and reporting the results to the SO [PCI DSS 12.5.5].

(iii) The SO is responsible for the creation and distribution of incident response and escalation procedures within SCG [PCI DSS 12.5.3].

(iv) Overall responsibility for controlling access to data is assigned to the SO and is supported through the SCGITS departments. The procedure for access request and approval is established in the Access Request Submission Procedure with data owner information being routinely maintained as a component of system documentation.

(10) Employee Security Education

(i) SCG conducts annual security awareness training to assure employees granted access to SCG data are aware of the importance of PCI cardholder [PCI DSS 12.6.1.b] and Protected Health Information data security.

(ii) Employees are required to attend security awareness training upon initial employment with SCG [PCI DSS 12.6.1.b].

(iii) All SCG employees are required to acknowledge, in writing, their receipt and understanding of the security awareness training and the SCG security policies and procedures [PCI DSS 12.6.2].

(11) Employee Screening

(iv) New employees and employees being promoted with access to card holder information and Protected Health Information will be subject to background checks as limited by law [PCI DSS 12.7].

(12) Service Provider Policy

(i) SCG requires all service providers with which cardholder data is shared to adhere to the PCI DSS requirements and to sign an agreement acknowledging that the service provider is responsible for the security of cardholder data the provider possesses [PCI DSS 12.8.2].

(ii) SCG Information Technology Services (ITS) exercises due diligence in the selection of vendors by meeting the requirements of the "Shelby County Government Purchasing Policy Rules and Regulations Manual", inclusion of the contract language in Appendix A in all ITS contracts, and one or more of the following review processes [PCI DSS 12.8.3];

- Solution and service documentation
- Industry reviews
- Customer interviews and testimonials
- Vendor interviews
- Proof of concept deployments

(13) Incident Response Policy

(i) SCG has implemented a response plan for immediate response to system breaches.

(ii) The SCG incident response plan addresses roles, responsibilities, and communication and contact strategies, specific incident response procedures, business recovery and continuity procedures, data backup processes, roles and responsibilities, and communication and contact strategies.

(iii) SCG tests the incident response plan on an annual basis.

(iv) The incident response plan designates specific personnel responsible for its execution and the training required and provided to those persons.

(v) The incident response plan addresses the actions to be taken for specific alerts from intrusion detection and monitoring systems [PCI DSS 11.1.e].

(vi) The incident response plan is modified and amended, as necessary, based upon lessons learned and industry developments.

e) Applicability of Other Policies

This document is part of the county's cohesive set of security policies. Other policies may apply to the topics covered in this document and as such the applicable policies should be reviewed as needed.

f) Enforcement:

The Security Officer will enforce this policy. Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities are suspected, the county will report such activities to the applicable authorities.

g) Policy Owner:

Shelby County Government

h) Policy Administrator:

Chief Information Officer, Department of Information Technology Services

i) Policy Approval Date:

Current Revision Review Date:	08/01/2016
Current Revision 1.1 Approval Date:	10/03/2014
Original Version 1.0 Approval Date:	10/25/2012

j) Policy Effective Date:

Current Revision 1.1 Effective Date:	10/03/2014
Original Version 1.0 Effective Date:	10/25/2012

k) Compliance:

PCI DSS Requirement 12.1.
PCI DSS 10.6.a / PCI DSS 10.6.b.

l) Supporting Form(s):

Acceptable Use Policy – Form 1010
Audit Reports Review Procedure
Security Incident Policy – Form 1020
Shelby County Network Security Policy
Shelby County ITS Patch Management Policy
Security Incident Procedures: Response and Reporting Policy – Form 1030
Inventory Control Policies and Procedures

Security Awareness Program
SCG Incident Response Plan
SCG Access Request Procedure
Approved Network Device Administrators
Approved Network Server Administrators
Shelby County Government Purchasing Policy Rules and Regulations Manual

m) Definitions:

(1) Institutional Data - A subset of Shelby County Government's information resources and administrative records including any information in print, electronic, or audio-visual format that meets the following criteria:

(i) Acquired and/or maintained by Shelby County Government (SCG) employees in performance of official job duties;

(ii) Created or updated via use of a SCG enterprise system or used to update data in an enterprise system;

(iii) Relevant to planning, managing, operating, or auditing a major function of SCG;

(iv) Referenced or required for use by more than one organizational unit; and

(v) Included in official SCG administrative reports or official SCG records.

(2) Sensitive Information - Privileged or proprietary information which, if compromised through alteration, corruption, loss, misuse, or unauthorized disclosure, could cause serious harm to the organization owning it.

(3) NIST SP800-30 - This guide was developed by the National Institute of Standards and Technology (NIST) to provide a foundation for the development of an effective risk management program, containing the definitions and practical guidance necessary for assessing and mitigating risks identified within IT systems to help organizations better manage IT-related mission risks

(4) Employee-Facing Technologies - System components and IT resources used by Shelby County Government employees and contractors to access Shelby County Government Institutional Data. Examples include but are not limited to [PCI DSS 12.3.5]:

(i) Remote access technologies

(ii) Wireless technologies

(iii) Removable electronic media

(iv) Laptops

(v) Personal Data Assistants (PDA)

(vi) Cell phones

(5) Payment Card Industry (PCI) Data Security Standard (DSS) – A widely accepted set of policies and procedures developed and implemented to optimize the security of credit, debit and cash card transactions and protect cardholders against misuse of their personal information.

n) Appendices:

(1) ITS contract compliance verbiage.

DATA SECURITY

CONTRACTOR warrants to the COUNTY and State that it agrees to meet the spirit and intent of all compliance requirements relating to the content of data accessed. This includes but is not limited to Payment Card Industry (PCI) data, as defined by PCI Security Standard v3.1, Protected Health Information (PHI), as defined under the Code of Federal Regulations, Title 45, Subtitle A, Subchapter C, Part 160, Subpart A, §160.103 (45 C.F.R. §160.103), and Personally Identifiable Information (PII), as defined in the National Institute of Standards and Technology Special Publication 800-122 sections 2.1 and 2.2, in electronic and/or paper format. CONTRACTOR will sign any documents that are reasonably necessary to keep the State and the COUNTY in compliance, including, but not limited to, Data Security - Vendor Acknowledgement agreement and Acceptable Use Policy, and to abide by SCG ITS security policies including, but not limited to, the SCG Network Security and Information Security policies.

CONTRACTOR shall apply all vendor-issued security updates for system hardware and software components maintained by the CONTRACTOR within 30 days of issuance.

Upon notification by the COUNTY, the CONTRACTOR shall assure that all vulnerabilities specific to the systems maintained and identified by the COUNTY Approved Scanning Vendor (ASV), using the common vulnerability scoring system (CVSS), as not meeting compliance requirements, including but not limited to

PCI Data Security Standards (DSS) and Health Insurance Portability and Accountability Act (HIPAA), are patched, updated, or otherwise modified to assure they meet said compliance requirements.

The Contractor shall promptly report to Information Technology Security Officer any breaches of Shelby County Government data and will implement immediate, appropriate corrective actions to contain and prevent recurrence.

Where the CONTRACTOR provides or Maintains systems containing Protected Health Information (PHI), Card Holder Data (CHD), or Personally Identifiable Information, the CONTRACTOR agrees that;

i) HIPAA

CONTRACTOR warrants to the COUNTY and State that it is familiar with the requirements of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and its accompanying regulations, and will comply with all applicable HIPAA requirements in the course of this Contract. CONTRACTOR warrants that it will cooperate with the COUNTY and State in the course of performance of the Contract so that all parties will be in compliance with HIPAA, including cooperation and coordination with COUNTY and State privacy officials and other compliance officers required by HIPAA and its regulations. CONTRACTOR will sign any documents that are reasonably necessary to keep the State and the COUNTY in compliance with HIPAA, including, but not limited to, business associate agreements.

ii) PCI-DSS

CONTRACTOR warrants to the COUNTY that it is familiar with the requirements established by the Payment Card Industry Security Standards Council for PCI Data Security Standards (PCI-DSS) and will comply with all applicable PCI-DSS requirements in the course of this Contract. CONTRACTOR agrees to indemnify and hold the COUNTY, its officers, employees, and agents, harmless for, from and against any and all claims, causes of action, suits, judgments, assessments, costs (including reasonable attorneys' fees) and expenses arising out of or relating to any breach of COUNTY or

COUNTY customer credit card or identity information due to the CONTRACTOR's actions.

iii) Personally Identifiable Information (PII)

CONTRACTOR warrants to the COUNTY that it will protect any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.

Notwithstanding the foregoing, County understands and agrees that the Services offered by Contractor and procured by County herein are exclusively for maintenance of a legacy software product to its existing product specifications and that to the extent that said product does not meet the standards described in Section 36 above, further development work to meet such standard is not included in the Services, and will not be provided by Contractor except at additional County expense. This section does not imply that continued development of the legacy software product is expected by Shelby County Government of the Contractor."

9. Shelby County ITS Patch Management Policy

a) Policy Statement:

Shelby County ITS will review, evaluate, and appropriately apply vendor provided patches in a timely manner. If patches cannot be applied in a timely manner due to hardware or software constraints, mitigating controls will be implemented based upon the results of the risk assessment.

b) Scope:

This policy covers all servers, workstations, network devices, operating systems, applications, and other information assets for which vendors provide system patches or security updates.

c) Policy:

Shelby County Government computers must be properly patched with the latest appropriate updates in order to reduce system vulnerability and to enhance and repair application functionality. New network devices must be patched to the current patch level, as defined by system vendor, prior to the device being connected to the production network.

ITS is responsible for proactively monitoring security sources for vulnerabilities and patches that correspond to the operating system or software within the organizational hardware and software inventory. A variety of sources should be monitored to ensure that they are aware of all newly discovered vulnerabilities, including Security Alerts.

Review and evaluation

Once alerted to a new patch, ITS will download and review the new patch within 24 hours to 10 days, depending on classification, of its release. ITS authorized personnel will prioritize the set of known patches and categorize the criticality of the patch according to the following:

- Emergency — an imminent threat to SCG network
- Critical — targets a security vulnerability
- Non Critical — a standard patch release update
- Not applicable to SCG network environment

Regardless of platform or criticality, all patch releases will follow a defined process for patch deployment that includes assessing the risk, testing, scheduling, installing, and verifying.

Patches will be tested on non-production systems prior to installation on all production systems. In addition, ITS will develop and maintain an organizational hardware and software inventory and a database of information on patches required and deployed on systems or applications for the purposes of proper internal controls and reporting.

If ITS categorizes a patch as an Emergency, the department considers it an imminent threat to Shelby County network. Therefore, the Shelby County network assumes greater risk by not implementing the patch than waiting to test it before implementing.

Implementation

SCITS will deploy Emergency patches within 48 hours of availability. As Emergency patches pose an imminent threat to the network, the release may precede testing. SCITS will obtain authorization for implementing Emergency patches from the ITS Administration.

SCITS will assure the review and implementation of patches rated as Critical within 30 days of patch issuance [PCI DSS 6.1.b].

For new network devices, each platform will follow established baseline procedures to ensure the installation of the most recent patches.

Auditing, assessment, and verification

Following the release of all patches, SCITS staff will verify the successful installation of the patch and that there have been no adverse effects.

d) Applicability of Other Policies:

This document is part of the Shelby County Government Information Technology Services cohesive set of security policies. Other policies may apply to the topics covered in this document and as such the applicable policies should be reviewed as needed.

e) Enforcement:

The Security Officer will enforce this policy. Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities are suspected, the county will report such activities to the applicable authorities.

f) Policy Owner:

Shelby County Government

g) Policy Administrator:

Chief Information Officer, Department of Information Technology Services

h) Policy Approval Date:

Current Revision Review Date:		08/01/2016
Current Revision	1.0 Approval date:	10/03/2014
Original Version	1.0 Approval date:	09/22/2013

i) Policy Effective Date:

Current Revision 1.0 Effective Date: 10/03/2014
Original Version 1.0 Effective Date: 09/22/2013

j) Compliance:

k) Supporting Forms:

l) Definitions:

(1) Network Devices - Any physical component that forms part of the underlying connectivity infrastructure for a network, such as a router, switch, hub, bridge, gateway, etc.

(2) Network Infrastructure - includes servers, network devices, and any other network related equipment

(3) Patch - A fix to a known problem with an OS or software program. For the purposes of this document, the term "patch" will include software updates.

(4) OS - Operating System such Windows, Mac, Linux

(5) Risk Assessment – An evaluation of the level of exposure to a vulnerability for which a patch has been issued

(6) Update – a new version of software providing enhanced functionality and/or bug fixes

(7) Vendor - Any organization or individual(s) that do business with Shelby County Government

m) Appendices:

10. Physical Security Standards and Personal Asset Management Policy

a) Policy Intent:

The intent of this policy section is to establish physical security standards for Shelby County's computer and communications assets, for Shelby County's network computing and telecommunications assets, and for Shelby County-provided personal productivity tools, which includes, but is not limited to: personal computers, keys, proximity cards, cellular devices, tablets and laptops, and card data capture devices.

b) Scope:

This policy applies to all Shelby County organizations, employees, and contractors, and any other individuals or organizations that use Shelby County technology resources. Shelby County technology resources include, but are not limited to: networks, servers, data, applications, and information. It applies to all Shelby County facilities.

c) Policy:

Assets used in the transmission, processing, and storage of Shelby County data will be physically secured at all times [PCI DSS 9.6].

Shelby County employees are responsible to exercise reasonable care to prevent the theft of or damage to Shelby County assets.

All personal computers, cellular devices, and other Shelby County-provided equipment or tools remains the property of Shelby County and must be returned when an employee departs from the County, takes a long-term leave of absence, when a contract person completes their assignment or when requested by management.

Access to secure areas will be limited to authorized users.

Visitors to secure areas will be escorted at all times.

Unauthorized users will not be allowed access to Shelby County computers. Shelby County employees have primary responsibility for preventing unauthorized access to their workstations.

Unattended computers will be properly secured and will be logged out, or have a keyboard/screen locking program that automatically invokes after a defined period of inactivity. See Network Security Policy and Procedure for more information.

d) Procedures:

What Systems Are Physically Secure?

The following servers are kept in a locked data center or closet with restricted access. The Physical Security Access Policy maintained by Shelby County outlines the employees who will have access to secure resources and the type of access they will have.

- E-mail and messaging servers – any servers hosting e-mail or instant messaging applications
- Web servers – any servers hosting intranet or Internet sites used by Shelby County
- Enterprise resource management and customer relationship management servers – any servers hosting the inventory and production management applications and customer relationship applications
- Any other server computers used within Shelby County

This list is by no means all inclusive. Services and information can be added as needed.

What Other Devices Are Physically Secure?
Any routers and firewalls are also kept in secure locations to prevent unnecessary access to these devices and ensure their constant operation. Backup drives and media are stored here as well. This will ensure that only appropriate access is allowed to these critical items.
As a general rule any server or device that is instrumental in ensuring the continuity of Shelby County should be kept in a secure location.

Access to the secure location is outlined in the Network Security policy that specifically addresses the issue of access.

e) Applicability of Other Policies:

This document is part of the County's cohesive set of security policies. Other policies may apply to the topics covered in this document and as such the applicable policies should be reviewed as needed.

f) Enforcement:

The Security Officer will enforce this procedure. Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities are suspected, the county will report such activities to the applicable authorities.

g) Policy Owner:

Shelby County Government

h) Policy Administrator:

Chief Information Officer, Department of Information Technology Services

i) Policy Approval Date:

Current Revision Review Date: 08/01/2016
Current Revision 1.0 Approval date: 10/03/2014
Original Version 1.0 Approval date: 10/03/2014

j) Policy Effective Date:

Current Revision 1.0 Effective Date: 10/03/2014
Original Version 1.0 Effective Date: 10/03/2014

k) Compliance:

l) Supporting Forms:

m) Definitions:

Asset Owner or Manager – A Shelby County employee or an agent of Shelby County who has physical possession of, or has responsibility for an asset.

n) Appendices:

11. Software Development Life Cycle Policy

a) Purpose:

The purpose of this document is to implement procedures ensuring that all systems and applications developed and maintained by Information Technology Services (ITS) are based on the Shelby County Government (SCG) SDLC Policy.

b) Scope:

These procedures apply to the development of all applications and databases by SCG. These procedures are to be followed when changes are deployed to either the production or development environments.

c) Procedures:

The Software Development Life Cycle Procedures document provides the framework for building and altering safe, secure and reliable information systems in a very deliberate, structured, and methodical way, using measurable and repeatable processes. It is designed to ensure privacy and security when developing information systems, to establish uniform privacy and protection practices, and to develop acceptable implementation strategies for these practices in compliance with the Software Development and Maintenance Policy.

(1) Initiation

All requests are made through management notification or a Service Desk ticket. Users either call the Service Desk or open a ticket. The Service Desk software automatically assigns each ticket a unique tracking number. Change requests initiated through the ticketing system are assessed and assigned a priority. All Service Desk tickets are assessed by first level ITS support personnel. If first level cannot resolve the request, then a ticket is opened and the request is directed to the responsible person including Oncall personnel after hours. A current Oncall rotation schedule is maintained to ensure everyone is aware of the primary, secondary, and tertiary backup person on call. A major feature request is classified as a project and follows the sprint process which includes approval and prioritization by the Change Control Board. The five defined priority levels are:

- Emergency,
- High,
- Medium,
- Low, and
- Scheduled.

Low priority means that addition of a new feature or modification to an existing feature is made as part of a planned release.

An emergency priority means the change is executed outside the standard release, the reason is documented in the ticket, and all managers automatically receive Electronic alerts on their cellular device. If the application processes personally

identifiable information (PII) or other sensitive information including credit card data, and communicates through, or is accessible over, the internet, then it will be subject to the security clearance requirements and PCI DSS 6.4.3. These applications require a sign off for security in testing and production phases.

(2) Service Level Agreement

A Service Level Agreement (SLA) is on file for each department defining the services provided by ITS. A quarterly SLA report is generated and used to assess service level and network availability.

(3) Change Control & Authorization [PCI DSS 6.4.5.a]

Change control is made up of team leaders and management. Team leaders review work orders with customers and employees to prioritize requests. Prioritized requests are then assigned to Developers by the Team Leaders. A work order is created from the request and assigned to the developers who are authorized to work on them with a mandated first response to the work order. TeamForge / Collabnet are used when the development effort is part of a larger project. Developers update tasks associated with the project and document hours spent on the development effort. Management dictates which customer gets worked on and the customer has input into what gets worked on first. If the priority of a request is uncertain, the team leader escalates the request to management for prioritization. All developers complete a status report which lists the work orders each person is assigned to work on. If management requests have already been discussed in advance, as in the case of a new report or a new screen, then the developer opens a work order ticket. All development activities must have an assigned work order. Reports are available in the ticketing system to monitor several levels and work orders.

(4) Software Development

(i) Application coding is performed during the development phase in the development environment and is separate from production.

(ii) Applications are developed based on current OWASP secure coding guidelines to prevent coding vulnerabilities.

(iii) Developers and Quality Assurance personnel will complete secure coding guideline training annually [PCI 6.5.a].

(iv) Only test credit card numbers provided by the vendor will be used for testing in the development environment.

(v) SCG-ITS development focuses on individuals and interaction over processes and tools. Development methods involve iterations rather than phases. The

output of each iteration results in working code used to evaluate and respond to changing and evolving user requirements. Users describe the need that the software should fulfill and the development team estimates the time and resources necessary to build a release and defines the user acceptance tests. To create a release plan, the team breaks up development tasks into iterations and the users perform acceptance testing.

(vi) Developers shall use approved development tools and tool configurations and will write their code consistent with secure coding standards and training. They shall not use deprecated functions, API's, tools, code, etc. They may scan their code with the provided static analyzer during the development.

(vii) Software is developed in sprints and moved into production as releases. At the center of each project is a backlog of work to be done. This backlog is populated into a series of short iterations called sprints. Each sprint aims to implement a fixed number of backlog items. The development team plans the sprint, identifying the backlog items and ITS management assigns tasks to individual developers. When enough backlogs have been implemented so that the end users believe the release is ready to be put into production, management closes development. The team performs integration testing, publishes modifications, and summarizes each change in a release document.

(5) Version Control

Application source is maintained in a central repository and modification to the source is made using a version control toolset called Subversion (SVN). Access to SVN is controlled by a security administrator who manages user and user permissions. Subversion uses a central database, or repository, which contains all version-controlled files with their complete history. The source repository is on the server where the subversion server program is running, which supplies content to Tortoise SVN clients when requested. Access to SVN is restricted to developers. Subversion trunks and branches are used for managing source. Branches are used to maintain separate lines of development and the branches are merged into a trunk. SVN provides feature options that makes it easy to identify changes that were made which allows a developer to undo or revert changes back to the previous point in time, if needed [PCI DSS 6.5.4.4]. Each developer has their own working copy (sandbox) on their local PC. The developer synchronizes files on their PC with files in the repository and completes coding, performs unit testing and documents the change. The latest version is pulled down from the repository and once the changes are validated they are committed back to the repository. A working copy for a branch is checked out and changes are merged into the branch. The branch is then merged into the trunk.

(6) Code Reviews

All significant modifications undergo code review prior to staging modifications to test environments for further QA testing. (See code review life cycle for more detail). Bugs or issues identified during coder reviews and unit testing are resolved prior to staging changes to the test environment for testing. Once unit testing is complete, the developer notifies the team leader that changes are ready for code review. Once code reviews are performed and approved by the team leader, the developer and/or a team leader requests that the changed source code be staged to the test environment. The project manager must sign off (approve code review) prior to sourced code being staged for production [PCI DSS 6.3.2.a].

(7) Testing

Developers perform unit tests and notify users when the modification is ready for testing. Users must review and approve changes before and after they are published and document approvals in the work order. A test site is setup that allows the assigned developer to make modifications in a test environment prior to making the change to production. All changes are first published to a beta environment before they are published into production. Published changes to web applications are verified in the test environment before changes are moved to production.

Execute security testing cases/plans created based on security standards to ensure the following.

(i) Security features and functionality work as specified. Ensure that all security features and functionality that are designed to mitigate threats perform as expected.

(ii) Security features and functionality cannot be circumvented. If mitigation can be bypassed, an attacker can try to exploit software weaknesses, rendering security features and functionality useless.

(iii) Ensure general software quality in areas that can result in security vulnerabilities. Validating all data input and parsing code against malformed or unexpected data is a common way attackers try to exploit software. Data fuzzing is a general testing technique that can help prevent such attacks.

(iv) Testing shall include all latest OWASP top 10 vulnerabilities [6.5.1]. Refer to OWASP website.

(v) Testing card readers or scanners must use the test card issued by the bank processor. The card may be checked out from team leader.

(vi) Testing entry of credit card numbers must use the test card numbers given by the bank processor. The card numbers can be obtained from team leader.

The level of testing, functional, user acceptance, and stress and load, is at the discretion of the project leader based on the type of change being made. Test plans are documented for all changes. Each customer receives a customer survey and has an opportunity to provide feedback on each work order completed. Production data used in the development and test environment is sanitized to remove card holder data prior to being used.

(vii) Performance testing requires a very large data set. Therefore, real time data, which is impossible to create manually, is refreshed in the test environment from production. The development team submits a request to have the DBA or Project Leader to run scripts that refresh the test environment. The scripts are written to exclude sensitive data. Test data is not copied to or synchronized with production.

(viii) Test data and accounts are removed before a production system becomes active [PCI DSS 6.4.4]. Custom application accounts, user ids, and/or passwords are removed before the system is released into production [PCI DSS 6.3.1]. Web applications use a custom account and password to connect to the database. Before the application is promoted to production, a new service account is created with a different password. These credentials and host address are then updated in the production environment.

(ix) Post - Implementation Testing

Once the developer provides source code to the server administrator to synchronize with the production environment; the developer verifies the installation was complete and accurate and that the program synchronized correctly. Data entry/conversion validation is performed when required. The program version and source code are locked as a permanent record, disaster recovery components are synchronized, and software items are archived.

(x) Defect Management

Defects identified are debugged and retested until all defects are resolved. Identified defects are documented and prioritized in relation to time by the team leader before assigning the work order to the developer. If a defect or bug is fixed, the developer will retest until the defect is resolved. If the defect is not a defect but a project scope issue, the team leader will schedule for a later release. If the team leader classifies a defect as "NO Bug", and the user still requires a fix, the Applications Services manager will be notified.

(8) Migration

The development and test environments are separate from the production environment with access control in place to enforce the separation. All changes are merged into a "trunk" and the trunk is compiled and published by the Change Publisher. The Change Publishers or server administrators publish code changes. The developer provides the server administrator with the Java .war file and

requests that the code be deployed to the production server. The server admin brings down the server, applies the files, and brings the server back up. The developer commits the change to Subversion to ensure it is not lost.

The branch serves as a snapshot of the currently published application. If there are minor bug fixes or changes that need to be made to the application between sprints these changes are made to the branch. Changes made during a sprint are made to the trunk. Once a sprint is complete the minor changes made to the branch are merged into the trunk and the trunk is published.

Prior to the release of any changes subject to security, the Team Leader shall perform a final security review. This review will ensure compliance with all security design requirements. The project team must provide contact information for people who respond to security incidents. After the software is released, the product development team shall be available to respond to any possible security vulnerabilities that are discovered.

(9) Roles and Responsibilities

R = Responsible **A = Accountable** **C = Consulted** **I = Informed**	**Requester**	**Change Request Manager**	**Change Control Board**	**Developer**	**Change Publisher**
Initiate a change request by creating a BMC ticket and document that appropriate business approval.	RA	I			
Collect BMC and ensure that all initial documentation is complete. Classify BMC ticket and prioritize based on urgency and number of people affected. Resolve or escalate for resolution.	C	RA		C	
Determine if the request/proposed changes are feasible and the impact of each of the changes on any potentially affected IT assets within the system.			IR	RA	
Approve or deny the request if development time is greater than a half day or if the request is for a new feature. If bug fix that requires less than a half day of development to resolve it approved at implementer's discretion.	I		IR	RA	I
If request is considered a project or new module, update the project log, confirm the date & time of the scheduled change, assign change request to implementer.	I		RA	C	
Modify system in development/test environment. Verify that modifications were made correctly and	I		I	RA	

without impacting existing system. Update BMC assigning ticket back to requester for testing.					
Publish changes to web environment for testing.	I		R	I	RA
Complete necessary testing in beta. Verify that modifications were made correctly and update JIRA indicating user acceptance testing is complete and modifications are ready for release.	RA		R	I	
Implement / publish the change as planned and scheduled then update the JIRA ticket.	I		R	I	RA
Complete post release testing to verify modifications to production were made correctly. Update JIRA and close ticket if testing was successful.	RA		R	I	
Update the project log.			RA	I	
Review the overall change management process	C	RA	C	C	

d) Applicability of Other Policies:

This document is part of the Shelby County Government Information Technology Services cohesive set of security policies. Other policies may apply to the topics covered in this document and as such the applicable policies should be reviewed as needed.

e) Enforcement:

The Security Officer will enforce this policy. Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities are suspected, the county will report such activities to the applicable authorities.

f) Policy Owner:

Shelby County Government

g) Policy Administrator:

Chief Information Officer, Department of Information Technology Services

h) Policy Approval Date:

Current Revision Review Date: 08/01/2016
Current Revision 1.0 Approval date: 10/03/2014

Original Version 1.0 Approval date: 04/23/2012

i) Policy Effective Date:

Current Revision 1.0 Effective Date: 10/03/2014
Original Version 1.0 Effective Date: 04/23/2012

j) Compliance:

PCI DSS Requirement 6.3.a, 6.3.b, 6.3.c, 6.3.2, 6.3.3, 6.3.4, 6.3.5, 6.3.6

k) Supporting Form(s):

OWASP top 10 - www.owasp.org
On Call Documentation for Programmers
SCG Injection Flaw Coding Procedure [PCI DSS 6.5.1]
SCG Buffer Overflow Coding Procedure [PCI DSS 6.5.2]
SCG Insecure Cryptographic Storage Coding Procedure [PCI DSS 6.5.3]
SCG Insecure Communications Coding Procedure [PCI DSS 6.5.4]
SCG Improper Error Handling Coding Procedure [PCI DSS 6.5.5]
SCG High Vulnerability Coding Procedure [PCI DSS 6.5.6]
SCG Cross-Site Scripting Coding Procedure [PCI DSS 6.5.7]
SCG Improper Access Control Coding Procedure [PCI DSS 6.5.8]
SCG Cross-Site Request Forgery Coding Procedure [PCI DSS 6.5.9]

l) Definition(s):

Bank Processor – Company that authorizes submitted payment. Ex: Elavon
BMC
Live Credit Card – PAN embossed and/or encoded on a plastic card that identifies the issuer and the particular cardholder account
OWASP – Open Web Application Security Project
PAN – Primary Account Number embossed and/or encoded on a plastic card that identifies the issuer and the particular cardholder account
PCI – Personal Card Industry
PCI DSS – PCI Data Security Standard
PII – Personally Identifiable Information
SLA – Service Level Agreement
SVN – Subversion

m) Appendices:

12. Security Incident Management and Response Policy

a) Policy Intent:

The purpose of the Incident Response Plan is to establish procedures in accordance with applicable legal and regulatory requirements to address instances of unauthorized access to or disclosure of Shelby County Government information. The Incident Response Plan (IRP) defines the policy, roles and responsibilities for involved personnel when responding to an information security threat [PCI DSS 12.9.1].

b) Scope:

This policy applies to Shelby County Government (SCG) in its entirety, including all workforce members. In addition, all third parties, such as contractors or vendors, are required to abide by this policy as required by Shelby County Government.

c) Policy:

It is the policy of SCG to return to a secure state as quickly as possible, while minimizing the adverse impact to SCG or its customers of incidents. To facilitate the return to a secure state, SCG has established the Computer Incident Response Team (CIRT). The CIRT is responsible for developing, maintaining, and executing the Incident Response Plan (IRP), taking appropriate action when a technology security incident occurs, and recommending revisions to processes, guidelines, and procedures that will help prevent future security incidents.

Depending on the circumstances, the CIRT may decide to modify or bypass one or more of the procedures outlined in this plan, or contained in the Incident Response Plan, in response to a particular security incident, with the understanding that the CIRT will take all reasonable steps to investigate and resolve any security issues. The capture and preservation of incident relevant data (e.g., network flows, data on drives, access logs, etc.) is performed primarily for the purpose of problem determination and resolution, as well as classification of the incident.

In the event that a Security Breach or Security Incident is found to have taken place, the notification requirements contained in this policy will be initiated to at least meet the required timeframes contained herein. Note that the Breach Notification Policy provides guidance for the notification of external government entities, departmental data owners, and affected customers.

d) Procedure:

(1) All workforce members of Shelby County Government will report any security incident they become aware of, or suspect, to the Information Technology Services Security Officer [PCI DSS 11.1.d / 12.9.5].

(2) SCG will implement, and monitor alerts from intrusion detection, Intrusion prevention, and file-integrity monitoring systems, following the applicable incident response procedure as required.

(3) SCG will maintain security policies that identify core activities in the area of Response and Reporting.

(4) Incidents will be classified as "serious" or "non-serious."

(5) SCG will maintain Incident Response Plans (IRP) for responding to serious and non-serious security incidents in order to prevent the escalation of the incident and to prevent future incidents of a similar nature. Incidents characterized as serious by the CIRT will be responded to immediately and reported to all upper-level management.

(i) The IRP designates specific positions responsible for its execution.

(ii) The IRP addresses the actions to be taken for specific alerts from intrusion detection and monitoring systems.

(iii) The IRP is modified and amended, as necessary, based upon lessons learned and industry developments.

(iv) SCG tests the IRP on an annual basis [PCI DSS 12.9.2].

(6) SCG will mitigate harmful effects, when possible, where a security incident affects customer information.

(7) The CIRT is headed by the Security Officer and is staffed by the members of SCG ITS on-call staff for the respective areas of expertise. Members will include personnel from;

Network Design
Network Administration
Programming
Network Systems
Web Administration

(8) Responsibility:

(i) All Workforce Members including individuals, groups, and organizations identified in the scope of this policy are responsible for:

- Staying aware of and identifying potential security incidents.
- Reporting suspected security incidents to the Security Officer utilizing the "Security Incident Reporting Form".
- Assisting the Security Officer in ending the security breach and mitigating its harmful effects, if possible.

(ii) The Security Officer is responsible for :

- Assuring that the incident response plan and communication policies and procedures are reviewed annually and upon modification, that they function as intended, and that the lessons learned and industry developments are incorporated into them.
- Assuring the CIRT is fully staffed with members as identified by ITS Administration and Management and that the CIRT staff receive periodic SCG incident response policy and procedure training [PCI DSS 12.9.4].
- Informing the administration of serious security incidents.
- Determining with the CIO and ITS administration the appropriateness of contacting law enforcement officials and payment brands concerning a serious security incident.

(iii) The Computer Incident Response Team is responsible for:

- Establishing and maintaining procedures for responding to security incidents including both communication and contact strategies and business recovery and continuity procedures covering all critical system components.
- Responding to reports of incidents, compromises and breaches of SCG computers, data, telecommunication, and network resources.
- Characterizing reported security incidents as "serious" or "non-serious".
- Mitigating, to the extent possible, any harmful effects of security incidents.
- Documenting all security incident response efforts and outcomes and providing said documentation to the Security Officer.
- Being available 24/7 to work with the ITS on-call personnel encountering serious incidents or events not documented in the Incident Response Procedures [PCI DSS 12.9.3].

(iv) The CIO's office will be responsible for all interactions with the public and the news media concerning incidents.

(9) General Incident Response Procedure

(i) Intrusion attempts, security breaches, or other technical security incidents perpetrated against SCG-owned computing, telecommunication, or networked resources must be reported to the Security Officer. Functional unit managers and/or systems personnel must:

- Report any security incidents in order to obtain assistance, guidance, and to notify the Security Officer and CIRT.
- Report any systematic unsuccessful attempts (e.g., login attempts, probes, or scans).
- Where feasible, given the circumstances, reports should be sent as soon as the situation is detected.

(vii) Upon receiving a report of a security incident, the Security Officer will:

- Mobilize the CIRT.
- Assist in the subsequent investigation as required.
- Report all incidents to the manager of the ITS department involved.
- Report "Serious" incidents to the ITS Administrator and Chief Information Officer (CIO). Upon approval from the CIO and Administrator, notify the following as appropriate:
    - The senior manager of the department or agency involved.
    - SCG Legal Counsel.
    - Serious incidents will be reported to the payment brands and legal authorities.
- Ensure that the incident is logged into the ITS work order system per applicable procedures.

(viii) Upon receiving a report of a security incident, the CIRT will:

- Immediately assess actual or potential disclosure or inappropriate access to institutional or personal information.
- Categorize the incident as serious or non-serious.
- Initiate steps to reduce or eliminate the impact of the incident.
- Initiate steps to warn other SCG systems personnel if it appears that the situation has the potential to affect other SCG systems.
- Confirm actual or probable disclosure or inappropriate access to institutional or personal information.
- Invoke formal incident response procedures commensurate with the situation.

(ix) The Functional Unit managing a system that has had an incident or has been compromised or breached is responsible for all monetary, staff, and other costs related to investigations, cleanup, and recovery activities resulting from the compromise, response, or recovery.

(x) In order to protect SCG data and systems, as well as to protect threatened systems external to SCG, the Security Officer may block, or place restrictions on technology services provided using any SCG owned systems and networks. Specifically:

- Limitations may be implemented through the use of policies, standards, and/or technical methods, and could include (but may not be limited to) usage eligibility rules, password requirements, or restricting or blocking certain protocols or the use of certain applications known to cause security problems.
- Restrictions may be permanently deployed based on a continuing threat or risk after appropriate consultation with affected constituents, or they may be temporarily deployed, without prior coordination, in response to an immediate and serious threat.
- Restrictions deployed temporarily will be removed when the risk is mitigated to an acceptable level, or where the effect on SCG functions caused by the restriction approaches or exceeds risk associated with

the threat, as negotiated between the affected constituents and the Security Officer.

(xi) In order to protect SCG data and systems, as well as to protect threatened systems external to SCG, the Security Officer may unilaterally choose to isolate specific systems from campus or external networks, given:

- Information in-hand reasonably points to the system as having been compromised.
- There is ongoing activity associated with the system that is causing or will cause damage to other SCG systems and/or data, or the assets of other internal or external agencies.
- All reasonable attempts have been made to contact the responsible systems personnel or department management, or such contact has been made where the technician or department managers are unable to (or choose not to) resolve the problem in a reasonable time.
- Isolation is removed when the risk is mitigated to an acceptable level, or where loss of access or function caused by the isolation approaches or exceeds risk associated with the threat, as negotiated between the responsible functional manager and the Security Officer.

(xii) In the event of a significant series of incidents, a compromise or a breach, the entire episode and response will be reviewed to determine which parts of the plan worked correctly. The "lessons learned" will be part of an After Action Review to determine areas that need to be changed (policies, system configurations, etc.) [PCI DSS 12.9.6].

e) Applicability of Other Policies:

This document is part of the County's cohesive set of security policies. Other policies may apply to the topics covered in this document and as such the applicable policies should be reviewed as needed.

Specific documents related to this cohesive incident response process include the Shelby County Incident Response Plan and the Breach Notification Policy.

f) Enforcement:

The Security Officer will enforce this policy. Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities are suspected, the county will report such activities to the applicable authorities.

g) Policy Owner:

Shelby County Government

h) Policy Administrator:

Chief Information Officer, Department of Information Technology Services

i) Policy Approval Date:

Current Revision Review Date: 08/01/2016
Current Revision 1.0 Approval date: 08/30/2013
Original Version 1.0 Approval date: 08/30/2013

j) Policy Effective Date:

Current Revision 1.0 Effective Date: 08/30/2013
Original Version 1.0 Effective Date: 08/30/2013

k) Compliance:

PCI DSS Requirement 12.9.1

l) Supporting Form(s):

Incident Response Plan
Security Incident Reporting Form
Shelby County Breach Notification Policy

m) Definitions:

(1) **Computer Incident Response Team (CIRT)** - is a unit within the SCG Information Technology Services department. The mission of the CIRT is to provide both incident response services and proactive security analysis, development, guidance and education. The CIRT are members of ITS. They receive, triage, resolve, classify and track incidents of technology abuse or security issues for the entire SCG enterprise. The CIRT coordinates the efforts of internal ITS resources as well as external Internet Service Providers, law enforcement agencies and other institutions.

(2) **Non-Serious Incidents** - Have both of the following characteristics:
   a. It is determined that there was no malicious intent (or the attack was not directed specifically at SCG networks or systems).
   b. It is determined that no sensitive information, (especially cardholder and protected health data), was used, disclosed, or damaged in an unauthorized manner.

(3) **Private Data** - Data about individuals that is classified by law as private or confidential and is maintained by the SCG in electronic format or medium. "Private data" means data classified as not public and available to the subject of the data, and "confidential data" means data classified as not public but not available to the subject of the data.

(4) **SCG ITS Resources or Systems** - Includes all SCG-owned computers, peripherals, networks and related equipment and software, and the voice and data communications infrastructure.

(5) **Security Breach** – A confirmed, unauthorized acquisition, modification or destruction of SCG or private data has taken place. At this point, a breach has been forensically determined and evidence supports that data was compromised.

(6) **Security Incident** – A security incident is a computer, network, telecommunication, or paper based activity which results (or may result) in misuse, violation of need-to-know, damage, denial of service, compromise of integrity, or loss of confidentiality or availability of a network, computer, application, telecommunication resource or data; and threats, misrepresentations of identity, or harassment of or by individuals using these resources.

(7) **Serious Incidents** - Have either of the following characteristics:

c. It is determined that there was malicious intent and/or an attack was directed specifically at SCG.

d. It is determined that sensitive information, especially cardholder and/or protected health data, may have been used, disclosed, or damaged in an unauthorized manner.

(8) **Systematic Unsuccessful Attempts** -- continual probes, scans, or login attempts, where the perpetrators obvious intent is to discover a vulnerability and inappropriately access and compromise that device.

(9) **Unauthorized acquisition** - For the purposes of this plan, this means that a person has obtained SCG data without statutory authority or the consent of the individual who is the subject of the data, and with the intent to use the data for non-SCG purposes.

n) Appendices:

Information Technology Services
Security Incident Reporting Form[v1]

Instructions: ***This form shall be used to report any acts or omissions that result in (1) The attempted or successful unauthorized access, use, disclosure, modification or destruction of Shelby County Government (SCG) Data or information, or (2) the interference with system operations in SCG information systems.***

REPORTING INFORMATION[i]

I. Incident Discovery:

Date of Discovery _____ Time of Discovery _____

Location of Incident _____

Incident Reporter _____ Date Reported _____

II. Entities Involved[ii]

Name	Employer Name	Phone Number

III. Incident Report[iii]

Incident Description:

_____

_____

_____

Affected Computer System/s :

_____

_____

Data Compromised :

_____

_____

Other Relevant Information :

_____

_____

Action Taken Upon Incident Discovery:

_____

_____

Additional Notes:

_____

SECURITY OFFICE USE ONLY

Security Office Recipient:		**Recipient Phone Number:**	
Date Received:		**Incident Number**[iv]**:**	
Work Order Number:			

i Submit Incident Reports to the ITS Security Officer.
ii This is subject to change based upon investigation results. If additional room is required please add information in the additional notes section.
iii Describe the events leading up to the discovery of the incident.
iv Incident numbers are sequential and based upon the month, day, and year and if necessary time will be incorporated. For example incident 02281419:30 occurred on the twenty-eighth of February at 7:30PM.

13. Shelby County Breach Notification Policy

a) Policy Intent:

The purpose of this Breach Notification Policy is to provide guidance to employees, vendors, contractors, business partners, consultants, interns, temps, and other workers (herein termed "users") of Shelby County Government (SCG) when there is a breach of County sensitive data and to ensure SCG is compliant with all Federal, State of Tennessee, and local legal requirements as well as all applicable compliance frameworks applicable to data maintained by SCG.

This policy is specifically amended to the "Security Incident Management and Response Policy" and serves as the notification component to that policy.

b) Scope:

This policy scope applies to all SCG employees, vendors, contractors, business partners, consultants, interns, temps, and other workers (herein termed "users") utilizing SCG provided ITS resources, network, hardware, and/or software, in their assigned job responsibilities to store, transmit, or process sensitive data.

This policy applies to all SCG ITS managed sensitive data with "sensitive data" being defined as SCG confidential data, Payment Card Industry cardholder data, Protected Health Information, Personally Identifiable Information, or other compliance-related data.

c) Policy:

It is the policy of Shelby County Government (SCG) to respond to security incidents to protect Shelby County held sensitive information to both protect County customers and to comply with all applicable legal and compliance framework notification requirements in the event of data breach. This document is specifically designed to address requirements for;

The Health Insurance Portability and Accountability Act (HIPAA)
The Health Information Technology for Economic and Clinical Health (HITECH) Act
Tennessee Code Annotated (TCA) § 47-18-2107
Payment Card Industry Data Security Standard (PCI DSS)

In the event that a Security Breach, Security Incident, or Security Incident is found to have taken place, the notification requirements contained in this policy will be initiated to at least meet the required timeframes contained herein. Where possible, notifications will be made as quickly as possible.

d) Procedure:

Breach Notification requirements vary amongst laws and compliance frameworks. In the event that data is compromised, notification as outlined in this policy will be

initiated using existing SCG personnel. In the event that the breach is sufficient in size, third party support will be engaged to ensure the required notifications are met.

Should multiple laws or compliance frameworks be affected by a data breach, all requirements for each data type will be met. SCG ITS, as the information holder and service provider, will notify the County data owners whose data may have been affected by a possible data breach as soon as a breach is reasonably suspected. SCG initiates and conducts breach notification strategies based upon the type of data compromised, as listed below:

(1) **HIPAA/HITECH Act/ePHI/PHI**

(i) Risk Assessment – In the event of an incident involving electronic Protected Health Information (ePHI), the SCG ITS Security Office will perform an investigation of the event and will complete a risk assessment, as defined under the HHS Breach Notification Guidance. This assessment will include, at a minimum, review of the following:

- The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification;
- The unauthorized person who used the protected health information or to whom the disclosure was made;
- Whether the protected health information was actually acquired or viewed; and,
- The extent to which the risk to the protected health information has been mitigated.

The following exceptions must also be considered as they may assist in informing whether the incident rises to the level of a breach:

- Was this an unintentional acquisition, access, or use of protected health information by a workforce member or person acting under the authority of a covered entity or business associate, if such acquisition, access, or use was made in good faith and within the scope of authority.
- Was this an inadvertent disclosure of protected health information by a person authorized to access protected health information at a covered entity or business associate to another person authorized to access protected health information at the covered entity or business associate, or organized health care arrangement in which the covered entity participates.
- Does the covered entity or business associate have a good faith belief that the unauthorized person to whom the impermissible disclosure was made, would not have been able to retain the information.

(ii) Breach Notification - In the event that the risk assessment has determined that a breach of electronic Protected Health Information (ePHI) has occurred, SCG will provide notification of the breach of unsecured PHI to

affected individuals, the Secretary, and, in certain circumstances, to the media. These notifications will be conducted according to the current "Breach Notification Requirements" located on the HHS.GOV website which currently consist of;

- Third Party Breach or Business Associate Breaches - Breaches of unsecured PHI occurs at or by a BA, the BA must notify the covered entity within 60 days following the discovery of the breach. The business associate should provide the covered entity (CE) with the following information;
  - The identification of each individual affected by the breach
  - Any other available information required to be provided by the covered entity in its notification to affected individuals.
  - While the CE is ultimately responsible for ensuring individuals are notified, SCG will delegate the responsibility of providing individual notices to the business associate experiencing the breach.

- Notice to Individuals - In the event of data breach affecting an individual, the SCG (the CE) will provide notification as follows;
  - Notification must occur within 60 days of the breach discovery.
  - Affected individuals must be notified in written form by first-class mail or by e-mail if the affected individual has agreed to receive such notices electronically.
  - If contact information for 10 or more individuals is out of date, the CE must either post the notice on the home page of its web site for at least 90 days or provide the notice in major print or broadcast media where the affected individuals likely reside.
  - If contact information for fewer than 10 individuals is insufficient or out-of-date, the covered entity may provide substitute notice by an alternative form of written notice, by telephone, or by other means.
  - The CE must include a toll-free phone number that remains active for at least 90 days where individuals can learn if their information was involved in the breach.
  - Notifications must include a brief description of the breach, a description of the types of information that were involved in the breach, the steps affected individuals should take to protect themselves from potential harm, a brief description of what the covered entity is doing to investigate the breach, mitigate the harm, and prevent further breaches, and contact information for the covered entity (or business associate, as applicable).
- Notice to the Public/Media - Within 60 days of the discovery of a breach affecting more than 500 residents of a State or jurisdiction, the CE is, in addition to notifying the affected individuals, required to provide notice to prominent media outlets serving the State or jurisdiction.
- Notice to the Secretary
  - CEs must notify the Secretary of breaches of unsecured protected health information by;

- Completing and electronically submitting the breach report form at the HHS web site, (http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brinstruction.html).
- Notification of breaches above 500 individuals must occur within 60 days of the breach discovery.
- Notification of breaches affecting fewer than 500 individuals may be reported annually no later than 60 days after the end of the calendar year in which the breaches are discovered.

(2) **Personally Identifiable Information (PII)** - In the event of a breach of PII, SCG, as the information holder, will provide notification of the breach according to the requirements of the Tennessee Code Annotated §47-18-2107 which currently consists of;

(i) Tennessee Residents - Information holders shall disclose any breach of the security of the system, following discovery or notification of the breach in the security of the data, to any resident of Tennessee whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subsection (d), or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

(ii) Non-Owner - Any information holder that maintains computerized data that includes personal information that the information holder does not own shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

(iii) Notification - Notice may be provided by one (1) of the following methods:

- Written notice;
- Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in 15 U.S.C. § 7001; or
- Substitute notice, if the information holder demonstrates that the cost of providing notice would exceed two hundred fifty thousand dollars ($250,000), or that the affected class of subject persons to be notified exceeds five hundred thousand (500,000), or the information holder does not have sufficient contact information. Substitute notice shall consist of all of the following:

- E-mail notice, when the information holder has an e-mail address for the subject persons;
- Conspicuous posting of the notice on the information holder's internet website page, if the information holder maintains such website page; and
- Notification to major statewide media.

In the event that more than one thousand (1,000) persons at one time are affected by a data breach of PII, notification, without unreasonable delay, will be made to all consumer reporting agencies and credit bureaus that compile and maintain files on consumers on a nationwide basis, as defined by 15 U.S.C. § 1681a, of the timing, distribution and content of the notices.

Notification required by these sections may be delayed, if a law enforcement agency determines that the notification will impede a criminal investigation. The notification required by this section shall be made after the law enforcement agency determines that it will not compromise the investigation.

(3) **Card Holder Data (CHD)** - In the event of a breach of CHD, SCG, as the information holder and service provider, will provide notification of the breach according to the most stringent requirements of the MasterCard and Visa card brands and will begin with notification to the County's credit card processor for the CC processing channel breached. [PCI DSS 12.10.1.a]

(iv) Notification – Elavon

Notice of breaches involving all credit card data must be provided to Elavon (the County payment processor) as soon as reasonably suspected. This report must be submitted on the ADC Client Questionnaire which is located in Appendix A. This questionnaire should be reported to Information Technology Service's current Elavon client representative who is Tim Smith (1-513-234-0368)

(v) Notification - Mastercard

Notice of breaches involving MasterCard credit card data must follow the current requirements of the MasterCard Security Rules and Procedures Merchant Edition sections 10.2.2.1and 10.2.2.2. The current revision of this document is located at http://www.mastercard.com/us/merchant/pdf/SPME-Entire_Manual_public.pdf. These include immediate initiation of the following steps upon identification of an Account Data Compromise (ADC) event or Potential ADC, unless otherwise directed in writing by MasterCard.

- Immediately commence a thorough investigation into the ADC Event or Potential ADC Event.
- Within twenty-four (24) hours, identify, contain, and mitigate the ADC Event or Potential ADC Event, secure Account data and preserve all

information, in all media, concerning the ADC Event or Potential ADC Event (pg.78)

- Within twenty-four (24) hours, and on an ongoing basis thereafter, submit to MasterCard all known or suspected facts concerning the ADC Event or Potential ADC Event, including, by way of example and not limitation, known or suspected facts as to the cause and source of the ADC Event or Potential ADC Event.
- Within twenty-four (24) hours and continuing throughout the investigation and thereafter, provide to MasterCard, in the required format, all PANs and expiration dates associated with Account data that were actually or potentially accessed or disclosed in connection with the ADC Event or Potential ADC Event and any additional information requested by MasterCard (pg.78).
- Within seventy-two (72) hours, engage the services of a PCI SSC Forensic Investigator (PFI) to conduct an independent forensic investigation to assess the cause, scope, magnitude, duration, and effects of the ADC Event or Potential ADC Event (pg.78).
  - Within two (2) business days from the date on which the PFI was engaged, identify to MasterCard the engaged PFI and confirm that such PFI has commenced its investigation (pg.78).
  - Within three (3) business days from the commencement of the forensic investigation, ensure that the PFI submits to MasterCard a preliminary forensic report detailing all investigative findings to date (pg.78).
- Within twenty (20) business days from the commencement of the forensic investigation, provide to MasterCard a final forensic report detailing all findings, conclusions, and recommendations of the PFI and continue to address any outstanding exposure, and implement all recommendations until the ADC Event or Potential ADC Event is resolved to the satisfaction of MasterCard (pg.79).
- Notwithstanding the foregoing, MasterCard may engage a PFI on behalf of the Customer in order to expedite the investigation. The Customer on whose behalf the PFI is so engaged will be responsible for all costs associated with the investigation.
- Provide weekly written status reports containing current, accurate, and updated information concerning the ADC Event or Potential ADC Event, the steps being taken to investigate and remediate same, and such other information as MasterCard may request (pg.79).

(vi) Notification – Visa - Notice of breaches involving Visa credit card data must follow the current requirements of the Visa "What To Do If Compromised Visa Inc. Fraud Investigation Procedures Version 4.0 (Global)" sections :Notification". For each step listed below, reference this document which is located at https://usa.visa.com/dam/VCOM/download/merchants/cisp-what-to-do-if-compromised.pdf for additional information and sub steps. For the purpose of notification SCG merchants are "entities" to Visa.

- Immediately conduct an initial investigation and complete the "Initial Investigation Request" for submission to Visa (pg.18).
- Alert all necessary parties immediately (pg.7).
- In the event of PCI SSC PTS Approved PINEntry device (PED) compromise, report the event to the PED (pg.8).
- Consult the SCG legal department to determine if laws mandating customer notification are applicable (pg. 9).
- Engage a Payment Card Industry Forensic Investigator (PFI) to perform a forensic investigation of the event (pg.25). The current list of approved PFIs is located at https://www.pcisecuritystandards.org/approved_companies_providers/pci_forensic_investigator.php.
- Provide all compromised Visa, Interlink, and Plus accounts to the Visa acquiring bank or to Visa within ten (10) business days (pg. 9).
- Within three (3) business days of the reported compromise, provide a written documentation to the Visa client or to Visa. See Appendix A (pg. 9).

(4) **Unclassified Data** – In the event of data breaches unrelated to the explicitly addressed data types within this document, the County will initiate investigative activities immediately upon suspicion of the breach and will notify the County data owners whose data may have been affected by the breach as soon as is reasonably possible.

e) Applicability of Other Policies

This document is part of the Shelby County Government Information Technology Services cohesive set of security policies. Other policies may apply to the topics covered in this document and as such the applicable policies should be reviewed as needed.

Specific documents related to this cohesive incident response process include the Shelby County Security Incident Management and Response Policy and the Incident Response Plan.

f) Enforcement:

The Security Officer will enforce this policy. Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities are suspected, the county will report such activities to the applicable authorities.

g) Policy Owner

Shelby County Government

h) Policy Administrator:

Chief Information Officer, Department of Information Technology Services

i) Policy Approval Date:

Current Revision Review Date:			08/01/2016
Current Revision	1.1	Approval date:	12/15/2015
Original Version	1.0	Approval date:	12/15/2015

j) Policy Effective Date:

Current Revision	1.1	Effective Date:	08/01/2016
Original Version	1.0	Effective Date:	12/15/2015

k) Compliance:

The Health Insurance Portability and Accountability Act (HIPAA) Final Omnibus Rule
The Health Information Technology for Economic and Clinical Health (HITECH) Act
Tennessee Code Annotated (TCA) § 47-18-2107
Payment Card Industry Data Security Standard (PCI DSS)
Privacy Act of 1974, 5 U.S.C. § 552a

l) Supporting Form(s):

Elavon ADC Client Questionnaire

m) Definitions

(1) Breach - The acquisition, access, use, or disclosure of sensitive data in a manner not permitted by the controlling legislation or compliance framework which compromises the security or privacy of the data. Good faith acquisition of personal information by an employee or agent of the information holder for the purposes of the information holder is not a breach of the security of the system; provided, that the personal information is not used or subject to further unauthorized disclosure.

(2) Electronic Protected Health Information (ePHI) - Individually identifiable health information that is transmitted by electronic media, maintained in electronic media, or transmitted or maintained in any other form or medium.

(3) Information Holder - Any person or business that conducts business in the State of Tennessee, or any agency of the Shelby County or any of its political subdivisions, that owns or licenses computerized data that includes personal information.

(4) PCI SSC Forensic Investigator (PFI) – Companies certified as PFIs by the PCI DSS council who are;

a. A recognized QSA Company,
b. Have a dedicated forensic investigation practice within their company,
c. Have staff with the necessary backgrounds and skills,
d. Have experience performing investigations within the financial industry using proven investigative methodologies & tools, and have relationships with law enforcement to ensure they can support any resulting criminal investigations.

(5) Personally Identifiable Information - An individual's first name or first initial and last name, in combination with any one (1) or more of the following data elements, when either the name or the data elements are not encrypted:

a. Social security number;
b. Driver license number; or
c. Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account; and

"Personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

(6) Protected Health Information (PHI) - Includes individually identifiable health information that is transmitted by electronic media, maintained in electronic format, or transmitted or maintained in any other form or medium.

(7) Sensitive Information - Privileged or proprietary information which, if compromised through alteration, corruption, loss, misuse, or unauthorized disclosure, could cause serious harm to the organization owning it. This information includes but is not limited to Social Security Numbers (SSN), Electronic Protected Health Information (EPHI), Credit Cardholder Data (CHD) and personally identifiable information (PII).

(8) Unsecured Protected Health Information (unsecured PHI) - *A*ny PHI which is not unusable, unreadable, or indecipherable to unauthorized persons through the use of technology or methodology, such as encryption or destruction, as specified by the HSS Secretary.

(9) Workforce - Employees, volunteers, trainees, and other persons under the direct control of SCG, whether or not they are paid by SCG.

(10) Non-Serious Incidents - Have both of the following characteristics:

a. It is determined that there was no malicious intent (or the attack was not directed specifically at SCG networks or systems).
b. It is determined that no sensitive information, (especially cardholder and protected health data), was used, disclosed, or damaged in an unauthorized manner.

(11) Private Data - Data about individuals that is classified by law as private or confidential and is maintained by the SCG in electronic format or medium. "Private data" means data classified as not public and available to the subject of the data, and "confidential data" means data classified as not public but not available to the subject of the data.

(12) SCG ITS Resources or Systems - Includes all SCG-owned computers, peripherals, networks and related equipment and software, and the voice and data communications infrastructure.

(13) Security Breach – A confirmed, unauthorized acquisition, modification or destruction of SCG or private data has taken place. At this point, a breach has been forensically determined and evidence supports that data was compromised.

(14) Security Incident – A security incident is a computer, network, telecommunication, or paper based activity which results (or may result) in misuse, violation of need-to-know, damage, denial of service, compromise of integrity, or loss of confidentiality or availability of a network, computer, application, telecommunication resource or data; and threats, misrepresentations of identity, or harassment of or by individuals using these resources.

(15) Serious Incidents - Have either of the following characteristics:
a. It is determined that there was malicious intent and/or an attack was directed specifically at SCG.
b. It is determined that sensitive information, especially cardholder and/or protected health data, may have been used, disclosed, or damaged in an unauthorized manner.

(16) Systematic Unsuccessful Attempts -- continual probes, scans, or login attempts, where the perpetrators obvious intent is to discover a vulnerability and inappropriately access and compromise that device.

(17) Unauthorized acquisition - For the purposes of this plan, this means that a person has obtained SCG data without statutory authority or the consent of the individual who is the subject of the data, and with the intent to use the data for non-SCG purposes.

n) Appendix A – Elavon ADC Client Questionnaire

Merchant Information	Response

Merchant contact name:	
Phone:	
Fax:	
Email Address:	
Street:	
City:	
State:	
Zip Code:	
Business type:	
MCC:	
Has the location validated PCI DSS Compliance?	
• Date validated:	
• Scanning vendor and date of last passing scan • (Please attach a copy of your most recent passing scan)	
• If no, timeframe to validate full compliance:	
The following card payment methods are accepted (Y/N)	
• Signature	
• PIN	
• E-Commerce	
• Phone/Mail order	

POS/Terminal Information	Response
Location of terminals:	
Hours of usage:	
Terminal ID	
Terminal type:	
Software application name:	
Software application version:	
Is this a recent software update?	
Please explain	
Is track data stored?	
Is two factor authentication implemented? (Y/N)	
Are the terminals visible to the customers?	
Are they in a secure location?	
Is each employee required to log in when using the terminal?	
What is the type and version of antivirus protection that the POS	

Payment terminals have installed? (Product, Version and date of last update)	
Do you have Remote Access software? If Yes (e.g. PC-Anywhere, Log Me In, Windows Remote Desktop, SSH, FTP…etc)	
• Product and Version	
• Is your remote access software is disabled by default and is only enabled when needed?	
• Is logging enabled to properly audit connections?	
Do you have a back of house (BOH) sever? If yes,	
• Is antivirus protection installed on the BOH server? (Product, Version and date of last update)	
• Does BOH server have a public IP address?	
• Firewall installed between itself and the Internet?	
• Unique Windows accounts are established for each user of the Back of House server?	
• BOH server is configured for business functions only and that no personal functions such as Internet surfing or email is completed.	

Card Present Merchants Only	Response
Were there any commonalities with the accounts used at this merchant, such as a common clerk or shift time? If Yes	
• What are the employment dates for any employee who is suspected of skimming?	
• Was the employee a temporary or seasonal hire at the location?	
• Did the employee ask a lot of questions about credit cards?	
• Was there an unusual interest in running the credit card transactions?	
• Is the employee or employees suspected of skimming still employed at the merchant?	
• What has the management put in place to prevent future fraud from occurring?	
• Was the terminal inspected to determine if it has been tampered or manipulated?	
• Were tamper proof seals affixed?	
• Has a skimming device been seen or found at the location?	

Web Merchants Only	Response
Shopping Cart Software (Company, software and Version)	
Web Hosting Provider	
How long are web server logs archived?	
Were new SSH certificates reissued?	
Did the merchant make changes to web server or begin using a new server?	

Incident Summary	Response
Was there evidence of a breach?	
When was the breach identified?	
Has the breach been contained?	
• If so what date?	
Explain what type breach was found? (e.g. Malware, Virus, SQL Injection, employee theft, etc.)	
What is the date range of the exposure?	From: To:
Was a forensic investigation completed?	
If Yes	
• Forensic Company Name	
• Forensic Company Contact	
• Date forensic initiated	
• Date forensic company onsite	
• Date forensic completed	

Law Enforcement	Response
Has the merchant been contacted by law enforcement?	
Name:	
Department:	
Phone:	
Fax:	
E-mail:	

Containment and Remediation Steps Taken Card Present Merchants	Response (Yes with date completed or No)
Isolated compromised systems(s) from the network by unplugging the network cable. Do not turn the unit off or remove/interrupt power supply.	
Merchant began processing transactions using an alternate method to limit exposure to cardholder data.	
Implemented a firewall with strict inbound/outbound filtering. Prohibit direct public access between the Internet and the cardholder data environment.	
Changed all passwords used to connect to the network	
Assigned a unique user name to all users accessing the system	
Disabled remote access ports from the network	
Implemented two-factor authentication for remote access to the system	
Installed anti-virus software on all systems and enable logging	

Use of a PA-DSS compliant payment application	
Rebuilt any potentially compromised system prior to reuse by the merchant	
Engaged an Approved Scanning Vendor and schedule a vulnerability scan.	

Containment and Remediation Steps Taken Card Not Present Merchants	Response (Yes with date completed or No)
Examined firewall settings	
Reviewed web applications for unauthorized modification	
Checked environment for storage of cardholder data	
Merchant begin processing transactions on a new server	
Implemented a firewall with strict inbound/outbound filtering. Install a Web application firewall in front of public-facing Web applications.	
Changed all passwords used to connect or administer the website	
Assigned a unique user name to all users accessing the system	
Disabled remote access ports from the network	
Implemented two-factor authentication for remote access to the system	
Removed and disable storage of sensitive authorization data	
Installed anti-virus software on all systems and enable logging	
Developed Web applications based on secure coding guidelines	
Rebuilt any potentially compromised system prior to reuse	
Ensured logs (firewall, anti-virus, weblogs, etc.) are retained for 90 days on the system and one year offline	
Engaged an Approved Scanning Vendor and schedule a vulnerability scan. A list of ASVs is available at www.pcisecuritystandards.org/approved_companies_providers/approved_scanning_vendors.php	

PCI/DSS

All merchants need to achieve full compliance with achieve full compliance with the Payment Card Industry Data Security Standard (PCI/DSS) after any and all data security issues have been investigation and remediated. To do this they must complete the following steps:

- A completed and fully compliant PCI SSC Self-Assessment Questionnaire (A,B,C or D) which can be found at https://www.pcisecuritystandards.org/security_standards/documents.php.
- A completed and signed Attestation of Compliance (A,B,C or D)
- A passing quarterly network scans and an ASV Scan Report Attestation of Scan Compliance. The quarterly network scan can be completed by any of the approved scanning vendors located at https://www.pcisecuritystandards.org/approved_companies_providers/approved_scanning_vendors.php
- Verification the Merchant is using a PABP compliant payment application.

14. Video Surveillance Policy

a) Policy Intent:

This policy establishes guidelines and responsibilities for the use and maintenance of electronic surveillance systems monitoring Shelby County Government – Information Technology Services (SCG-ITS) managed resources whether for SCG-ITS purposes or in support of SCG-ITS clients.

b) Scope:

This policy applies to both SCG-ITS and SCG-ITS SLA clients (henceforth known as Clients) who have included video surveillance services through their SLA contracts. This policy addresses all electronic surveillance systems and related technology.

c) Policy:

It is the policy of Shelby County Government (SCG) to ensure the safety and security of SCG and Client employees, users, visitors, and property through the use of video surveillance systems where deemed necessary. Video surveillance has been found to be a highly effective means of assuring SCG facilities and properties operate in a safe and secure manner.

SCG recognizes the need to balance this increased safety and security with the individual's right to privacy. For this reason, SCG video surveillance cameras are installed in a manner that maximizes the safety and security of SCG sites and property while also minimizing privacy intrusion.

d) Procedure:

(1) Camera Location, Operation and Control

(i) SCG-ITS and Client's buildings and grounds may be equipped with video monitoring devices.

(ii) Video cameras may be placed in areas where surveillance has been deemed necessary as a result of threats to personal safety, loss of assets (work areas, equipment rooms, etc.) prior property damages, security incidents, or as required for compliance.

(iii) Cameras placed outside shall be positioned only where it is necessary to protect external assets or to provide for the personal safety of individuals on SCG-ITS or Client grounds or premises.

(iv) Cameras shall not be used in staff break areas, nor in areas where there is an expectation of privacy, e.g., washrooms, change rooms, etc.

(v) The SCG-ITS Security Officer, and/or their designee, shall manage, control, and audit the use and security of monitoring cameras, monitors, tapes, computers used to store images, computer diskettes, and all other video records.

(vi) SCG-ITS designated staff members will be authorized to view videos only in "real-time".

(vii) Video surveillance cameras shall not have audio recording capabilities; or any such audio capabilities will not be enabled if they are available.

(viii) "Dummy" (intentionally non-operational) cameras shall NOT employ signage indicating surveillance is taking place.

(ix) All SCG-ITS and Client entryways will be posted by way of signage that indicates video surveillance is taking place. See d.7 Video Surveillance Signage for recommended wording.

(2) Use of Video Recordings

(i) Video recordings of SCG-ITS and the Client's customers, staff, or others may be reviewed or audited for the purpose of determining adherence to official SCG-ITS or Client policies.

(ii) SCG-ITS and the Client may use video surveillance to detect or deter criminal offenses that occur in view of the camera.

(iii) Video recordings may be released to third parties in conformance with the requirements of a local, state, or federal law enforcement agency.

(iv) SCG-ITS and the Client may use video surveillance and the resulting recordings for inquiries and proceedings related to law enforcement, deterrence, and associated discipline.

(v) Neither SCG-ITS nor the Client shall use video monitoring for other purposes unless expressly authorized by the SCG-ITS C.I.O., the Client's elected official or appointed director, or their designee/s.

(3) Protection of Information and Disclosure/Security and Retention of Recordings (Safeguards)

(i) Videos are initially recorded on a computer hard disk. Information on the hard disk is retained until such time that the hard disk becomes full and then the newest segments overwrite the oldest video segments.

(ii) No attempt shall be made to alter any part of a video recording.

(iii) Video recordings that may be relevant to the investigation of an incident will be transferred from the computer hard disk onto removable media such as a CD, removable drive, and/or DVD.

(iv) Any records (videotapes, still photographs, digital images, etc) produced by surveillance systems shall be kept in a secure, locked facility or manner and managed appropriately by SCG-ITS management staff to protect legal obligations and evidentiary values.

(v) All video records that have been saved pending the final outcome of an incident investigation shall be numbered, dated, and retained by SCG-ITS.

(vi) Users desiring access to video monitoring must request this access via the access request process. Requests must include the areas and cameras for which monitoring is required.

(vii) Access to historical footage (not live) must be requested through the SCG-ITS service desk Work Order system and will only be granted, as needed and for specific dates, to users already having real-time monitoring rights.

Work Orders opened for these requests will contain the following and will be reported to the SCG-ITS Security Officer for logging purposes:

- the video number and date of recording,
- the name of the individual or department that was given access to the recording,
- the date that access was given,
- the reason that access was given, and
- the date when access was removed.

(viii) Both SCG-ITS and the Client will provide reasonable security measures to prevent unauthorized access to the electronic surveillance network; however, access to the network through illegal methods cannot be guaranteed.

(4) Disposal or Destruction of Recordings

(i) All saved recordings shall be disposed of in a secure manner unless they are archived as part of a permanent record as stated above. Removable media shall be shredded, burned, degaussed, DOD wiped, or otherwise made permanently unreadable.

(5) Video Monitors and Viewing

(i) Video monitoring for security purposes will be conducted in a professional, confidential, ethical, and legal manner.

(ii) SCG-ITS Management team or individuals authorized by SCG-ITS as defined above, and members of law enforcement agencies shall have access to video monitors while they are in operation.

(iii) Video monitors will be accessed through a secure login and password.

(iv) Video records should be viewed on a need to know basis only, in such a manner as to avoid public viewing.

(v) All authorized individuals who have access to camera controls (such as pan, tilt, and zoom) will not monitor individuals based on characteristics of race, creed, color, sex, national origin, sexual orientation, marital status, disability, public assistance status, age, or inclusion in any group or class protected by state or federal law. Camera control operators will monitor activity based on suspicious behavior, not individual characteristics.

(6) Internal Audit

(i) The SCG-ITS Management team or designee may ensure that periodic audits are conducted to ensure compliance with this policy.

(ii) In special situations where an allegation has been made and a confidential investigation is underway, the goal will be to limit information to only those involved in the investigation. Consequently, not all SCG-ITS staff who are involved in the development and administration of these policies may be aware of a particular investigation.

(7) Video Surveillance Signage

(i) Clearly visible signage, identifying the use of video surveillance cameras, must be installed in the building entrances, and wherever else there are cameras.

(ii) Suggested Wording:
This area is monitored by video camera.

e) Applicability of Other Policies:

This document is part of the County's cohesive set of security policies. Other policies may apply to the topics covered in this document and as such the applicable policies should be reviewed as needed.

f) Enforcement:

The Security Officer will enforce this policy. Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities are suspected, the county will report such activities to the applicable authorities.

g) Policy Owner:

Shelby County Government

h) Policy Administrator:

Chief Information Officer, Department of Information Technology Services

i) Policy Approval Date:

Current Revision Review Date:			08/01/2016
Current Revision	1.1	Approval date:	07/24/2014
Original Version	1.0	Approval date:	08/30/2013

j) Policy Effective Date:

Current Revision	1.1	Effective Date:	07/24/2014
Original Version	1.0	Effective Date:	11/30/2012

k) Compliance:

PCI DSS Requirement 9
PCI DSS Requirement 11

l) Supporting Form(s):

m) Definitions:

n) Appendices:

15. Physical Access Procedures

a) Purpose:

This document outlines the current practices when providing physical building access to facilities in the Shelby County Government organization.

b) Scope:

This policy applies to all Shelby County organizations, employees, and contractors, and any other individuals or organizations that require physical entree to Shelby County Technology facilities.

c) Procedures:

(1) 160 North Main North Elevator Access Procedure

a. Note, the Manager of Customer Support authorizes access to the Mayoral elevator. In his absence, The CAO will provide authorization.

b. The requestor sends an email requesting access to the service desk. The request is assigned to a Senior Staff Member who notifies the Manager of Customer Support requesting authorization to grant the access.

c. The Senior Staff Member gathers the details of the requested access including the users name, their employment status (permanent, temporary, contractor, State of Tennessee, etc.), the floors to be accessed, the hours of access, and the department to be accessed and adds this information to the work order.

d. The Senior Staff Member requests approval from the Manager of Customer support to grant the requested access.

e. The Manager of Customer Support will notify the Senior Staff Member of the approval or declination of the access via verbal or written communication.

f. If the request is declined, the Senior Staff member will notify the requestor and close the work order.

g. If the request is approved, the content of the approval shall be included in the work order and the work order will be assigned to a member of the Customer Support senior staff for processing.

h. Customer Support senior staff will engage the requestor to setup an appointment to register their fingerprints into the database.

i. After access has been verified, it is documented with the person's name and area of access in the Elevator List spreadsheet.

(2) Proxy Card Access Procedure

a. Requests for proxy card physical access to Shelby County Government (SCG) facilities not specifically listed in this procedure must be submitted by an approver (supervisor, higher –level authority, or other designated approver from the Office or Department residing in the location).

b. Note, all third-party personnel (vendor, volunteer, etc.) physical access to proxy card controlled doors in the Shelby County Administration building located at 160 North Main must be approved by the Director of Support Services, the Director of Homeland Security, or the Director of Public Works.

c. Proxy Card Configuration Process

(i) For SCG Employees, the Human Resources Department assigns the card recipient a proxy card and sends the Service Desk an email informing staff that there is a need to assign access to that card [PCI DSS 9.2.a / 9.2.b].

(ii) For SCG contractors or vendors, the Customer Support Department assigns the card recipient a proxy card and informs the Service Desk that there is a need to assign access to that card.

(iii) The Service Desk opens a work order and contacts the approver or the SCG sponsor of the contractor to verify the area(s) the person needs access to. Note, any changes to locations previously approved require reauthorization by the appropriate approver.

(iv) Upon completion of configuration, the new employee or contractor is contacted and advised to verify function of the card. Once function is verified, the work order is closed.

d. Proxy Access Modification Procedure

(i) The approver or SCG Sponsor of the third-party personnel submits a request to the Service Desk for proxy card access modification and the Service Desk opens a work order.

(ii) Access changes for third-party personnel may be subject to an additional approval process. For these requests, the Service Desk will verify the validity of the request by;

- Contacting the appropriate specific location approver (see section 2.b).
- If the request is not approved by the approver, the sponsor is informed and the work order is closed.
- If the request is approved it will be processed accordingly.

(iii) The Service Desk configures the requested access.

(iv) The access recipient is contacted and advised to verify function of the card. Once function is verified, the work order is closed.

(3) Proxy Access Removal Procedure –

(i) Access deletion requests for employees must originate from the employee's access approver or SCG Human Resources Department while access deletion requests for third-party personnel must originate from their sponsor.

(ii) The request for access removal is submitted to the Service Desk.

(iii) The Service Desk opens a work order, removes the access, and contacts the access removal requestor to inform them the request is complete.

(iv) The requestor returns any cards collected to Human Resources.

(4) Proxy-Controlled Door Lock and Unlock Schedule Changes –

(i) Proxy Lock Doors at 160 N. Main - Changes to the schedule for doors that have proxy locks on them for this location , with the exception of offices mentioned below, must be requested by the following individuals with unauthorized requestors being directed to Mr. Needham, Mr. Moss, or Lieutenant Crowder:
- Tom Needham
- Tom Moss
- Lieutenant Crowder
- Harvey Kennedy

(ii) Proxy Lock Doors into the Mayor's Suite at 160 N. Main - Changes to the schedule for doors that have proxy locks on them for this location must be requested by:
- Mattie James or
- Jackie Taylor

(iii) Proxy Lock Doors into the Committee Room on the 6th floor - Changes to the schedule for doors that have proxy locks on them for this location must be requested by:

- Qur'an Folsom
- Rosalind Nichols
- Evelyn Guy
- Lakeetha Barnes
- Clay Perry

(5) Punch Codes –

a. Punch codes will be issued according to the Proxy process outlined above for SCG Offices and Departments.

b. Note, requests for Punch Code access to 157 Poplar require the submission of the Access Card Request Form.

(6) Physical Key Distribution Procedure -

a. Support Services is responsible for the management of all SCG location physical keys.

b. New Keys and Duplicates: An email request is sent from the requestor's department manager to the Support Services Manager. The key(s) is then distributed to the requesting department manager.

d) Applicability of Other Policies:

This document is part of the Shelby County Government Information Technology Services cohesive set of security policies. Other policies may apply to the topics covered in this document and as such the applicable policies should be reviewed as needed.

e) Enforcement:

The Security Officer will enforce this policy. Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities are suspected, the county will report such activities to the applicable authorities.

f) Policy Owner:

Shelby County Government

g) Policy Administrator:

Chief Information Officer, Department of Information Technology Services

h) Policy Approval Date:

Current Revision Review Date:			08/01/2016
Current Revision	1.0	Approval date:	10/03/2014
Original Version	1.0	Approval date:	10/03/2013

i) Policy Effective Date:

Current Revision	1.0	Effective Date:	10/03/2014
Original Version	1.0	Effective Date:	10/03/2013

j) Compliance:

k) Supporting Forms:

l) Definitions:

m) Appendices:

Prior Policy and Procedure Update Listing

The policies listed in this table were modified in prior publication dates.

Policy Name	Modified Date	Modifier	Notes
Mobile System Use Policy	06/10/2015	Shawn McClure	Increased PSK timeframes.
Acceptable Use Policy	08-28-15	Shawn McClure	Restriction on use of County email accounts.
Network Security Policy	09-17-15	Shawn McClure	Updated the password reset requirement to "at least every 90 days".
Network Security Policy	09-17-15	Shawn McClure	Updated the password version requirement to "…where technically feasible.
Firewall and Router Configuration Standard	10-06-15	Shawn McClure	Updated the Firewall Application Traffic Ruleset Form
Firewall and Router Configuration Standard	10-15-15	Shawn McClure	Updated Changes to routers and firewalls follow this process: Pg104
Information Security Policy	10-19-15	Shawn McClure	Assigned responsibility for information security management to the current Shawn T. McClure as of April 2014
Information Security Policy	10-29-15	Shawn McClure	Documented due diligence process currently in use and added the contract language currently being placed in ITS contracts in appendix for PCI DSS 12.8.3.
Incident Response Policy	11-25-15	Shawn McClure	Updated applicability of other policies and referenced the breach notification policy in the policy statement.
Breach Notification Policy	12-11-15	Shawn McClure	Added this policy to the manual.
Firewall and Router Configuration Standard	12/14/2015	Leonard Tan	Added BOOTP as unnecessary service and MOP(DECNET) as protocol that needs to be disabled.
Network Security - Policy Card Reader Device Security	04-06-16	Shawn McClure	Updated the section to reference the PCI requirements. Added reference to the ITS inspection policy.
Network Security Policy	04-19-16	Shawn McClure	Included 8.2.6 requirement that reset passwords have

			unique values.
Information Security Policy	08-01-16	Shawn McClure	Updated legacy portion of the security contract verbiage.
PKI Certificate Policy Statement	08-01-16	Shawn McClure	Added this policy statement.
Shelby County Breach Notification Policy	08-01-16	Shawn McClure	Added specific HHS risk assessment requirements under the ePHI section.