

South Carolina

Enterprise Architecture

Security Domain

Information Security Policy

v1.8 - November 14, 2007



TABLE OF CONTENTS

TABLE OF CONTENTS 2

INTRODUCTION 4

PURPOSE 4

SCOPE..... 4

POLICY 6

 PART 1. PREFACE 6

 PART 2. ORGANIZATIONAL AND FUNCTIONAL RESPONSIBILITIES 6

 PART 3. INFORMATION POLICY 9

Individual Accountability..... 9

Confidentiality / Integrity / Availability..... 10

Policy and Standards Relationship..... 10

 PART 4. ORGANIZATIONAL SECURITY POLICY 10

Role and Responsibilities of the State Entity Information Security Officer 11

 PART 5. ASSET CLASSIFICATION AND CONTROL POLICY 12

 PART 6. PERSONNEL SECURITY POLICY 12

Including Security in Job Responsibilities..... 12

User Training 13

Security Incidents or Malfunctions Management Process..... 13

 PART 7. PHYSICAL AND ENVIRONMENTAL SECURITY POLICY 14

Physical Security Perimeter..... 14

Equipment Security..... 14

Secure Disposal or Re-use of Storage Media and Equipment 15

Clear Screen 15

 PART 8. COMMUNICATIONS AND NETWORK MANAGEMENT POLICY 15

Sharing Information Outside State Entity..... 15

Network Management..... 16

Vulnerability Scanning 16

Penetration & Intrusion Testing 17

Internet and Electronic Mail Acceptable Use..... 17

External Connections..... 18

Security of Electronic Mail..... 19

Portable Devices..... 19

Telephones and Fax Equipment..... 20

Wireless Networks 20

Modem Usage 21

Public Websites Content Approval Process..... 21

Electronic Signatures..... 22

Public Key Infrastructure 23

 PART 9. OPERATIONAL MANAGEMENT POLICY 23

Segregation of Security Duties 23

Separation of Development, Test and Production Environments 24

System Planning and Acceptance 24

Protection against Malicious Code 25

Software Maintenance 25

Information Back-up..... 25

Assessment..... 25

System Security Checking..... 25

 PART 10. ACCESS CONTROL POLICY 26

User Registration and Management 26

Logon Banner 27
Privileged Accounts Management 27
User Password Management..... 27
Network Access Control 27
User Authentication for External Connections (Remote Access Control) 28
Segregation of Networks..... 29
Operating System Access Control..... 30
Application Access Control 30
Monitoring System Access and Use 30
PART 11. SYSTEMS DEVELOPMENT AND MAINTENANCE POLICY 30
Input Data Validation..... 31
Control of Internal Processing 31
Message Integrity..... 32
Cryptographic Controls..... 32
Key Management 32
Protection of System Test Data..... 32
Change Control Procedures..... 33
PART 12. CYBER SECURITY CITIZENS' NOTIFICATION POLICY 33
PART 13. COMPLIANCE POLICY 35
Monitoring..... 35
Compliance..... 35
Enforcement and Violation Handling 35
DOCUMENT CHANGE MANAGEMENT 36
DEFINITIONS..... 37

INTRODUCTION

The South Carolina Information Security Policy was developed by the South Carolina Enterprise Architecture Oversight Committee as a set of guidelines to be followed by South Carolina state entities in order to ensure the State's assets are maintained in a secure, reliable, and sustainable environment. As these guidelines are based on best practices, the prescriptive nature of the recommendations are designed to represent the level of compliance required for optimal informational security in relation to each entities' strategic business and IT plans. The goal is for all state entities to strive to achieve or exceed the levels set forth within this document as soon as feasible with the understanding that it will take a phased approach over several years in an on-going process to complete the arduous task of fully implementing the included recommendations. There is currently no clear time-frame set forth in which agencies are required to be compliant and it is understood that going forward attention will need to be paid to both funding and support internal to each agency as well as at the top levels of government within South Carolina to support the work towards the common goal of securing the State's digital assets.

PURPOSE

The purpose of this policy is to define a set of minimum security requirements to be met by all *state entities (SE)*, except for those SE not bound by the authority of the AOC, for whom the policy shall define best practices. A SC *SE* may, based on its individual business needs and specific legal requirements such as Health Insurance Portability and Accountability Act (HIPAA), exceed the security requirements put forth in this document, but must, at a minimum, achieve the security levels required by this policy.

The primary objectives of this Information Security Policy and security program are to:

- effectively manage the *risk* of security exposure or compromise within *SE systems*;
- communicate the responsibilities for the protection of *SE information*;
- establish a secure processing base and a stable processing environment;
- reduce to the extent reasonably possible the opportunity for errors to be entered into an electronic *system* supporting *SE* business processes;
- preserve management's options in the event of an *information asset* misuse, loss or unauthorized disclosure;
- promote and increase the awareness of *information security* in all *SEs*.

SCOPE

This policy applies to all *state entities*. This policy is not intended to unilaterally change the terms and conditions of employment. All *SEs*, when coming into compliance with this policy, must consider all terms and conditions of employment.

This policy is applicable to *state entities*, staff and all others, including outsourced third parties, which have access to or manage *SE information*. Where conflicts exist between this policy and a *SE's* policy, the more restrictive policy will take precedence. The Information Security Policy for *state entities* encompasses all *systems*, automated and manual, for which the *state* has administrative responsibility, including *systems* managed or hosted by third parties on behalf of the *SE*. It addresses all *information*, regardless of the form or format, which is created or used in support of business activities of *state entities*. This policy must be communicated to all staff and all others who have access to or manage *SE information*.

POLICY

Part 1. Preface

This Information Security Policy is a statement of the minimum requirements, ethics, responsibilities, and accepted behaviors required to establish and maintain a secure environment, and achieve the *state's information security* objectives. Compliance with this policy should be required within each organization within the state of South Carolina. This Information Security Policy sets the direction, gives broad guidance and defines requirements for *information security* related processes and actions across *state entities* (*SE*'s). This policy documents many of the security practices already in place in some *SE*'s. The leadership of the State of South Carolina is fully committed to *information security* and agrees that every person employed by or on behalf of South Carolina State government has important responsibilities to continuously maintain security and *privacy* of *SE data*.

Part 2. Organizational and Functional Responsibilities

A. **State Entity (*SE*):** Each *SE* will establish a framework to initiate and control the implementation of *information security* within the *SE*. An Information Security Officer (*ISO*) role must be assigned to an individual with the preference to a role being appointed as a wholly separate position within the organization. A process will be established to determine *information sensitivity*, based on best practices, *state* and federal directives, legal and regulatory requirements to determine the appropriate levels of protection for that *information*. Each *SE* should ensure, through its appropriate chain of command, that an organization structure is in place for:

- the implementation of *information security* policies and *standards*;
- assigning *information security* responsibilities;
- the implementation of a security awareness program;
- monitoring significant changes in the exposure of *information assets* to major *threats*, legal or regulatory requirements;
- responding to security *incidents*;
- the approval of major initiatives to enhance *information security*;
- the development of a process to measure compliance with this policy;
- the approval of new applications and services.

- B. **The State of South Carolina Architectural Oversight Committee (AOC):** The AOC and its Security Domain Sub-Committee is the owner of this policy and all associated security sub-policies and procedures. Periodic review of this policy shall be at no less than once a year with more frequent updates possible if situations warrant. At any point, the AOC and SEs may bring up concerns as it relates to this policy. Those concerns will be referred to the Security Sub-Committee and addressed within the next two AOC monthly meetings or by way of documented electronic correspondence.
- C. **SE Designated Staff:** SE designated staff will be responsible for the implementation of this and other *information security* policies and the compliance of SE employees to this policy. The designated staff must educate SE employees with regard to *information security* issues. Staff must explain the issues, why the policies have been established, and what role(s) individuals have in safeguarding *information*. Consequences of non-compliance will also be explained.
- D. **Information Owners:** An individual or a group of individuals designated by the SE will serve as or represent *information owners* for the *data* and tools they use. *Information owners* are responsible for determining who should have access to protected resources within their jurisdiction, and what those access privileges should be (read, update, etc.). These access privileges must be in accordance with the *user's* job responsibilities. *Information owners* also communicate to the SE ISO the legal requirements for access and disclosure of their *data*. *Information owners* must be identified for all SE *information assets* and assigned responsibility for the maintenance of appropriate security measures such as assigning and maintaining asset *classification* and *controls*, managing *user* access to their resources, etc. Responsibility for implementing security measures may be delegated, though accountability remains with the identified owner of the asset.
- E. **SE Chief Information Officer or Manager/Director of Information Technology (SE CIO):** The SE CIO is directly responsible to the SE's Executive Management Team (EMT). The SE ISO reports to the CIO in most organizations within South Carolina and as such the CIO/IT Manager bears responsibility for integration of this and all security related policies and procedures into the accepted IT Management Framework within each SE.
- F. **The State CIO Information Security Officer (CIO ISO):** The State CIO's ISO and his staff perform as security consultants to their own organization as well as potential security resources to SE CIO's and ISOs. This role differs from SE ISO's in that the responsibility for shared critical infrastructure falls directly on this individual and his/her staff. The CIO ISO may also perform, at the request of the SE's EMT, CIO, or ISO, periodic reviews of SE security programs for compliance with this and other security policies and *standards*. The CIO ISO establishes and monitors effectiveness of *information security policy, standards* and *controls* within the the CIO's Organization while providing an open transparent communications conduit to local, state, and national security organizations. This individual and organization also seeks to provide guidance on grant and other funding opportunities as well as other cost-effective strategic means of raising the level of security in SE's and across the state as a whole.

- G. **SE Information Security Officer (SE ISO):** The *SE* Information Security Officer, or person appointed to that role, has overall responsibility for ensuring the implementation, enhancement, monitoring and enforcement of the *information security* policies and *standards*. The *SE* Information Security Officer is responsible for providing direction and leadership to his or her CIO and *SE* through the recommendation of security policies, *standards*, processes and education and awareness programs to ensure that appropriate safeguards are implemented, and to facilitate compliance with those policies, *standards* and processes. The *SE* Information Security Officer is responsible for investigating all alleged *information* security violations. In this role, the *SE* Information Security Officer will follow *SE procedures* for referring the investigation to other investigatory entities, including law enforcement. The *SE* Information Security Officer will coordinate and oversee security program activities and reporting processes in support of this policy and other security initiatives. For more detail, see Part 4, Organizational Security Policy, Role and Responsibilities of the *SE* Information Security Officer.
- H. **Security Administrators:** When such an individual or individuals exist, the individual or individuals will work closely with the *SE* Information Security Officer and support staff. Security Administrators are the staff normally responsible for administering security tools, reviewing security practices, identifying and analyzing security *threats* and solutions, and responding to security violations. This individual or individuals has administrative responsibility over all user-IDs and passwords and the associated processes for reviewing, logging, implementing access rights, emergency privileges, exception handling, and reporting requirements. Where a formal *Security Administration* function does not exist, the organization or staff responsible for the *security administration* functions described above will adhere to this policy.
- I. **Information Technology (IT):** IT management has responsibility for the *data* processing infrastructure and computing network which support the *information owners*. It is the responsibility of IT management to support the Information Security Policy and provide resources needed to enhance and maintain a level of *information security* control consistent with their *SE*'s Information Security Policy.

IT management has the following responsibilities in relation to the security of *information*:

- ensuring processes, policies and requirements are identified and implemented relative to security requirements defined by the *SE*'s business;
- ensuring the proper *controls* of *information* are implemented for which the *SE*'s business have assigned ownership responsibility, based on the *SE*'s *classification* designations;
- ensuring the participation of the *SE* Information Security Officer and technical staff in identifying and selecting appropriate and cost-effective security *controls* and *procedures*, and in protecting *information assets*;
- ensuring that appropriate security requirements for *user* access to automated *information* are defined for files, databases, and physical devices assigned to their areas of responsibility;

- ensuring that *critical data* and recovery plans are backed up and kept at a secured off-site storage facility and that recovery of backed-up media will work if and when needed.
- J. **SE Employees:** It is the responsibility of all employees to protect *SE information* and resources, including passwords, and to report suspected security *incidents* to the appropriate manager and the *SE* Information Security Officer.
- K. **Non-SE Employees:** Individuals who work under agreements with the *SE* such as Contractors, Consultants, Vendors, volunteers and other persons in similar positions, to the extent of their present or past access to *SE information*, are also covered by this Information Security Policy.

Part 3. Information Policy

- A. All *information*, regardless of the form or format, which is created, acquired or used in support of *SE*'s business activities, must only, be used for *SE* business. *SE information* is an asset and must be protected from its creation, through its useful life, and to its authorized disposal. It must be maintained in a secure, accurate, and reliable manner and be readily available for authorized use. *Information* must be classified and protected based on its importance to business activities, *risks*, and security best practices.
- B. *Information* is among *SEs*' most valuable assets and *SEs* rely upon that *information* to support their business activities. The quality and *availability* of that *information* is key to *SE*'s ability to carry out their missions. Therefore, the security of *SE*'s *information*, and of the technologies and *systems* that support it, is the responsibility of everyone concerned. Each authorized *user* of *SE information* has an obligation to preserve and protect *SE information* in a consistent and reliable manner. Security *controls* provide the necessary physical, logical and procedural safeguards to accomplish those goals.
- C. *Information security management* enables *information* to be shared while ensuring protection of that *information* and its associated *computer* assets including the network over which the *information* travels. *SE* designated staff is responsible for ensuring that appropriate physical, logical and procedural *controls* are in place on these assets to preserve the security properties of *confidentiality*, *integrity*, *availability* and *privacy* of *SE information*.

Individual Accountability

Individual accountability is the cornerstone of any security program. Without it, there can be no security.

- Access to *SE computer*, *computer systems* and networks where the information owner has identified the business need for limited user access or information integrity and accountability, must be provided through the use of

individually assigned unique *computer* identifiers, known as user-IDs, or other technologies including biometrics, token cards, etc.

- Individuals who use *SE computers* must only access *information assets* to which they are authorized.
- Associated with each user-ID is an *authentication* token, such as a password, which must be used to authenticate the person accessing the *data, system* or network. Passwords, tokens or similar technology must be treated as confidential *information*, and must not be disclosed. Where technically feasible, transmission of such *authentication information* must use secure mechanisms.
- Each individual is responsible to reasonably protect against *unauthorized activities* performed under their user-ID.
- For the *user's* protection, and for the protection of *SE* resources, user-IDs and passwords (or other tokens or mechanisms used to uniquely identify an individual) must not be shared (refer to Part 10. Access Control Policy, Operating System Access Control, B.).

Confidentiality / Integrity / Availability

- A. All *SE information* must be protected from *unauthorized access* to help ensure the *information's confidentiality* and maintain its *integrity*. The *information owner* will classify and secure *information* within their jurisdiction based on the *information's* value, *sensitivity* to disclosure, consequences of loss or compromise, and ease of recovery.
- B. Appropriate processes will be defined in the *SE* recovery plan and implemented to ensure the reasonable and timely recovery of all *SE information*, applications, *systems* and security regardless of computing platform, should that *information* become corrupted, destroyed, or unavailable for a defined period (refer to Part 9. Operational Management Policy, Information Backup).

Policy and Standards Relationship

SEs will develop *standards* and *procedures* that support the implementation of this policy for *systems* and technologies being used within their domains. These security *standards* will be produced and implemented to ensure uniformity of *information* protection and *security management* across the different technologies deployed within an *SE*. The *standards* can be used as a basis for policy compliance measurement.

Part 4. Organizational Security Policy

Each *SE* must have an Information Security Function led by an Information Security Officer (*ISO*) or someone assigned to the aforementioned role. The *SE ISO* should report at a level no less than directly to the SE Chief Information Officer or the Director/Manager of Information Technology serving in that capacity. The function must be auditable to balance security with technological and programmatic issues.

Mission of the Information Security Function

- develop, deploy and maintain an *information security architecture* that will provide security policies, mechanisms, processes, *standards* and *procedures* that meet current and future business needs of the *SE*;
- provide *information security* consulting to the *SE* regarding security *threats* that could affect the *SE* computing and business operations, and make recommendations to mitigate the *risks* associated with these *threats*;
- assist management in the implementation of security measures that meet the business needs of the individual *SE*;
- develop and implement security training and awareness programs that educate *SE* employees, contractors and vendors with regard to the *SE*'s *information security* requirements;
- investigate and report to management breaches of security *controls*, and implement additional compensating *controls* when necessary to help ensure security safeguards are maintained;
- participate in the development, implementation and maintenance of *disaster* recovery processes and techniques to ensure the continuity of the *SE*'s business and the security controls, in the event of an extended period of computing resource unavailability;
- although *information security* roles & responsibilities may be outsourced to third parties, it is the overall responsibility of each *SE* to maintain control of the security of the *information* that it owns.

Role and Responsibilities of the CIO and SE Information Security Officer

Both CIO and SE ISO's are responsible for performing, at a minimum, the following tasks:

- coordinate the development and implementation of *information security* policies, *standards*, *procedures*, and other control processes that meet the business needs of the *SE*;
- provide consultation for the various *SE* computing platforms;
- work closely with *security administration* or those serving in that function to ensure security measures are implemented to meet policy requirements;
- evaluate new security *threats* and counter measures that could affect the *SE* and make appropriate recommendations to the *SE*'s *CIO* and other management to mitigate the *risks*;
- review and approve all external network connections to the *SE*'s network;
- provide consultation to the *SE* management with regard to all *information security*;
- investigate and report incidents to appropriate internal management while following the *SE* or AOC approved Incident Reporting Policy (IRP);
- ensure that appropriate follow-up to security violations is conducted;
- ensure appropriate *information security* awareness and education to all *SE* employees, and where appropriate *third party* individuals;

- be aware of laws and regulations that could affect the security *controls* and *classification* requirements of the *SE's information*;
- due to the dynamic nature of the *information* technology and the critical role of the CIO and SE Security Officers as well as the need to maintain an adequate level of current knowledge appropriate security certifications such as the CISSP or CISA are strongly recommended. Proficiency in *information security* requires a minimum of forty (40) hours of Continuing Professional Education (CPE) credits completed annually. The CPEs must be directly related to *information systems* security and can be used to partially satisfy certification requirements. The *SE* should provide the opportunity for the *ISO* to earn the required CPEs annually.

Part 5. Asset Classification and Control Policy

- A. *Information*, like other assets, must be properly managed from its creation, through authorized use, to proper disposal. As with other assets, not all *information* has the same use or value, and therefore *information* requires different levels of protection. All *information* will be classified and managed based on its *confidentiality, integrity and availability* characteristics.
- B. All *information* will have an *information owner* established within the *SE's* lines of business who will be responsible for assigning the initial *information classification*, and make all decisions regarding *controls*, access privileges of *users*, and daily decisions regarding *information* management. Periodic high-level business impact analyses will be performed on the *information* to determine its relative value, *risk* of compromise, etc. Based on the results of the assessment, *information* will be classified or reclassified into one of the *SE's information classifications*.
- C. Each *classification* will have a set or range of *controls*, designed to provide the appropriate level of protection of the *information* and its associated application software commensurate with the value of the *information* in that *classification*. If this *information* is stored by a third-party, the third-party must contractually abide by these rules.

Part 6. Personnel Security Policy

The intent of the Personnel Security Policy is to reduce the *risk* of human error and misuse of *SE information* and facilities to an acceptable level.

Including Security in Job Responsibilities

Security roles and responsibilities must be documented. These roles and responsibilities will include general responsibilities for all *SE* employees, as well as specific responsibilities for protecting specific *information* and performing tasks related to security *procedures* or processes. Additional security roles and responsibilities for those individuals responsible for *information* security are defined in this document, Part 4 Organizational Security Policy.

User Training

- A. All individuals with access to private *SE information* must receive security awareness training to ensure they are knowledgeable of security *procedures*, their role and responsibilities regarding the protection of *SE information*, and the proper use of *information* processing facilities to minimize security *risks*.
- B. An *information security* awareness program must be developed, implemented and maintained that addresses the security education needs of all *SE* employees. A *SE* security awareness program will be developed by the *SE*'s Information Security Officer to supplement the *SE*'s new employee orientation program, and must be reinforced at least annually.

Security Incidents or Malfunctions Management Process

- A. Formal *incident* or malfunction reporting and *response procedures* must be established, that define the actions to be taken when an *incident* occurs. The following must be included:
 - the symptoms of the problem and any messages displayed should be documented;
 - where appropriate, the *computer* should be isolated, if possible, and use of it stopped until the problem has been identified and resolved;
 - the *incident* must be reported immediately to the appropriate *SE* manager and the *SE ISO*.
- B. Feedback mechanisms must be implemented to ensure that individuals reporting *incidents* are notified of the results after the *incident* has been resolved and closed.
- C. An *incident* management process must be established to track the types and volumes of security *incidents* and malfunctions. This *information* will be used by the *SE* to identify recurring or high impact *incidents* and to record lessons learned. This may indicate the need for additional *controls* to limit the frequency, damage and cost of future *incidents*, or to be taken into account in the policy review process.
- D. ***State* employees and contractors must not attempt to prove a suspected weakness unless authorized by the *SE ISO* to do so.** Testing weaknesses could have unintended consequences.
- E. All *users* of *SE systems* must be made aware of the procedure for reporting security *incidents*, *threats* or malfunctions that may have an impact on the security of *SE information*. All *SE* staff and contractors are required to report any observed or suspected *incidents* to the appropriate manager and the *SE ISO* as quickly as possible.
- F. Approaches to *incident* management must be documented and *procedures* must be clearly identified to ensure responsibilities are defined, resulting in a prompt and organized response to security *incidents*.
- G. Incident response procedures must be clearly identified to promote effective response to security incidents. Include procedures for *information system* failure, *denial of*

service, disclosure of confidential information and compromised systems of software. Once an incident has been identified, the following procedures must be followed:

- report the action to SE ISO according to the SE's IRP
- identify the underlying cause of the *incident* ;
- identify procedures the *SE* will employ to resolve the problem
- identify procedures the *SE* will employ to prevent the same or similar *incident* from occurring;
- track the response procedure from initial report through follow-up for review and audit purposes; and,
- provide adequate follow-up to ensure that individuals involved or affected by the *incident* understand what took place and how the *incident* was resolved

Part 7. Physical and Environmental Security Policy

- A. *Critical* or sensitive *SE* business *information* processing and storage facilities must be contained in secure areas protected by a defined security perimeter, with appropriate security barriers and some form of access *controls*. Physical protection measures will be implemented to protect the facility from *unauthorized access*, damage and interference.
- B. The *SE* may include *physical security*, such as controlling access to the building, etc. The *SE* will perform periodic *threat* and *risk* analysis to determine where additional *physical security* measures are necessary, and implement these measures to mitigate the *risks*.

Physical Security Perimeter

- A. Breaching *physical security* can cause a loss of or damage to *SE information*. *Physical security* can be achieved by creating physical barriers around the assets being protected. Each barrier establishes a security perimeter that would require a method of access control to gain entry. This perimeter could be in the form of an entry point with card key access, a staffed reception area, a locked cabinet or office or other physical barrier.
- B. The *SE* will perform a *threat* and *risk assessment* to determine the extent of the perimeter, and types of *controls* necessary to mitigate the *risk*. Based on the *threat* and *risk assessment*, a *physical security* perimeter must be established in *SE* environments where *information* or *information assets* are stored or operational, *SE data* centers, wiring closets for network and telephonic connections, printers where confidential or sensitive *information* may be printed, and any other location where *information* may be in use or stored. The purpose of the security perimeter is to prevent *unauthorized access* or theft of *information* or *information assets*.

Equipment Security

Computer equipment must be physically protected from security *threats* and environmental hazards. Protection of *computer* equipment is necessary to reduce the *risk* of *unauthorized access* to *information* and to protect against loss or damage. Special *controls* may also be necessary to protect supporting facilities such as electrical supply and cabling infrastructure. This protection will include but is not limited to *data* centers, wiring closets, server rooms, and storage facilities where *computers* and *computer* peripherals are stored.

Secure Disposal or Re-use of Storage Media and Equipment

There is *risk* of disclosure of sensitive *information* through careless disposal or re-use of equipment. Formal processes must be established to minimize this *risk*. Storage devices such as hard disk drives and other media (e.g. USB devices, tape, diskette, CDs, DVDs, cell phones, digital copiers or other devices that store *information*) or paper containing sensitive *information* must be physically destroyed or securely overwritten to prevent the unauthorized disclosure of sensitive *SE information*.

Clear Screen

To prevent *unauthorized access* to *information*, automated techniques and *controls* will be implemented to require *authentication* or re-*authentication* after a predetermined period of inactivity for desktops, laptops, PDA's and any other *computer systems* where *authentication* is required. These *controls* may include such techniques as password protected screen savers, automated logoff processes, or re-*authentication* after a set time out period.

Part 8. Communications and Network Management Policy

- A. All *SE* networks will implement appropriate security *controls* to ensure the *integrity* of the *data* flowing across these networks. If there is a business need, additional measures to ensure the *confidentiality* of the *data* will also be implemented.
- B. The *SE ISO* will ensure that measures are in place to mitigate any new security *risks* created by connecting the *SE* networks to a *third party* network.
- C. Where a *SE* has outsourced a server or application to a *third party* service (such as web applications), the *SE ISO* must perform or have performed periodic security reviews of the outsourced environment to ensure the security and *availability* of the *SE's information* and application.
- D. All connections to the *SE* networks must be authorized by the appropriate Network Manager, and reviewed by the *SE ISO*. Additions or changes to network configurations must also be reviewed and approved through the *SE* Change Management process.

Sharing Information Outside State Entity

- A. To facilitate the secure sharing of *information*, appropriate security measures must be in place commensurate with the *sensitivity* and *confidentiality* of the *information*

being shared. In most cases, the security *confidentiality* requirements of the *data* being shared will determine the level of security required when sharing *data*.

B. For *information* to be released outside an *SE* or shared between *SEs*, a process must be established that, at a minimum:

- evaluates and documents the *sensitivity* of the *information* to be released or shared;
- identifies the responsibilities of each party for protecting the *information*;
- defines the minimum *controls* required to transmit and use the *information*;
- records the measures that each party has in place to protect the *information*;
- defines a method for compliance measurement;
- provides a signoff procedure for each party to accept responsibilities;
- establishes a schedule and procedure for reviewing the *controls*.

Network Management

All *SEs* must implement a range of network *controls* to maintain security in its trusted, internal network, and ensure the protection of connected services and networks. These *controls* help prevent *unauthorized access* and use of the *SE* private network. The following *controls*, at a minimum must be implemented:

- Operational responsibility for networks will be separate from *computer* operations when possible;
- Responsibilities and *procedures* for remote use must be established (refer to Part 10. Access Control Policy section of this document);
- When necessary, special *controls* will be implemented to safeguard *data integrity* and *confidentiality* of *data* passing over public networks (*Internet*).

Vulnerability Scanning

A. All *SE* owned *hosts* that are or will be accessible from outside the *SE* network must be scanned for *vulnerabilities* and weaknesses before being installed on the network, and after software, operating *system* or configuration changes are made. For both internal and external *systems*, scans will be performed at least annually to ensure that no major *vulnerabilities* have been introduced into the environment. The frequency of additional scans will be determined by the *SE ISO* and the *information* owner(s), depending on the criticality and *sensitivity* of the *information* on the *system*.

B. Network *vulnerability scanning* will be conducted after new network software or major configuration changes have been made on *systems* that are essential to supporting a process that is *critical* to a *SE* business, and annually on all other *systems*. The output of the scans will be reviewed in a timely manner by the *SE ISO*, and any *vulnerability* detected will be evaluated for *risk* and mitigated. The tools used to scan for *vulnerabilities* will be updated periodically to ensure that recently discovered *vulnerabilities* are included in any scans.

- C. Where a *SE* has outsourced a server, application or network services to another *SE*, responsibility for *vulnerability scanning* must be coordinated by both *SEs*.
- D. Anyone authorized to perform *vulnerability scanning* must have a process defined, tested and followed at all times to minimize the possibility of disruption. Reports of exposures to vulnerabilities will be forwarded to the *SE ISO* and other defined staff.
- E. Any *vulnerability scanning* must be conducted by individuals who are authorized by the *SE CIO and ISO*. Any scanning without prior authorization by entities outside of their own approval process will be considered a violation of this policy.

Penetration & Intrusion Testing

- A. All *SE* computing *systems* that provide *information* through a public network, either directly or through another service that provides *information* externally (such as the *World Wide Web*), will be subjected to *SE* penetration analysis and intrusion testing. Such analysis and testing will be used to determine if:
 - an individual can make an unauthorized change to an application;
 - a *user* may access the application and cause it to perform unauthorized tasks;
 - an unauthorized individual may access, destroy or change any *data*; or
 - an unauthorized individual may access the application and cause it to take actions unintended by the application designer(s).
- B. The output of the *penetration testing* and intrusion testing will be reviewed in a timely manner by the *SE ISO*, and any *vulnerability* detected will be evaluated for *risk* and mitigated as appropriate.
- C. The tools used to perform the *penetration testing* will be updated to ensure that recently discovered *vulnerabilities* are included in any testing.
- D. Where a *SE* has outsourced a server, application or network services to another *SE*, *penetration testing* must be coordinated by both *SEs*.
- E. Only individuals authorized by the *SE* will perform *penetration testing*. The *SE CIO and ISO* must approve individually of each test and any entity where impact is deemed possible must be notified 24 hours prior to each *penetration test*. Any other attempts to perform such *penetration testing* without approvals from the *SE* will be deemed an *unauthorized access* attempt.

Internet and Electronic Mail Acceptable Use

When *SE* employees connect to the *Internet* using any *SE Internet* address designation or send electronic mail using the *SE* designation, it should be for purposes authorized by *SE* management. The following is not an all-inclusive list, and provides only examples of behavior that could result in security breaches. Specifically, the *Internet* and electronic mail will not be used:

- to represent yourself as someone else (i.e., “*spoofing*”);
- for spamming;

- for unauthorized attempts to break into any computing *system* whether *SE*'s or another organization's (i.e., *cracking* or *hacking*);
- for theft or unauthorized copying of electronic files;
- for posting sensitive *SE information* without *authorization* from *SE*;
- for any activity which create a *denial of service*, such as "chain letters";
- for "*sniffing*" (i.e., monitoring network traffic), except for those authorized to do so as part of their job responsibilities.

External Connections

(Also see Part 10. Access Control Policy, User Authentication for External Connections (Remote Access Control))

- A. Because the *Internet* is inherently insecure, access to the *Internet* is prohibited from any device that is connected, wired or wireless to any part of a *SE* network unless specifically authorized by *SE ISO*. This includes accounts with *third party Internet* service providers. *Users* will not use the *SE*'s *Internet* accounts to establish connections to these *third party* services, unless authorized to do so by *SE* management and the security of the connection is reviewed and approved by the *SE ISO*.
- B. All connections from the *SE* network to external networks must be approved by the *SE ISO*. Connections will be allowed only with external networks that have been reviewed and found to have acceptable security *controls* and *procedures*, or appropriate security measures have been implemented by the *SE* to protect *SE* network resources. A *risk* analysis will be performed to ensure that the connection to the external network will not compromise the *SE*'s private network. Additional *controls*, such as the establishment of *firewalls* and a *DMZ* (demilitarized zone) may be implemented between the *third party* and the *SE*. These connections will be periodically reviewed by the *SE* to ensure:
 - the business case for the connection is still valid and the connection is still required;
 - the security *controls* in place (filters, rules, access control lists, etc.) are current and functioning correctly.
- C. This policy requires that connection to the *SE* network be done in a secure manner to preserve the *integrity* of the *SE* network, *data* transmitted over that network, and the *availability* of the network. The security requirements for each connection will be assessed individually, and be driven by the business needs of the parties involved. Only *SE* authorized and qualified staff or qualified *third party* will be permitted to use sniffers or similar technology on the network to monitor operational *data* and security events
- D. The *SE ISO* or designee will regularly review audit trails and *system* logs of external network connections for abuses and anomalies.
- E. *Third party* network and/or workstation connection to a *SE* network must have an internal *SE* sponsor develop a business case for the network connection. A *SE* non-

disclosure agreement must be signed by a duly appointed representative from the *third party* organization who is legally authorized to sign such an agreement. In addition to the agreement, the *third party's* equipment must also conform to the *state's* security policies and *standards*, and be approved for connection by the *SE ISO*.

- F. Any connection between *SE firewalls* over external networks that involves sensitive *information* must use *encryption* to ensure the *confidentiality* and *integrity* of the *data* passing over the external network.

Security of Electronic Mail

Electronic mail provides an expedient method of creating and distributing messages both within the organization and outside of the organization. *Users* of the *SE E-mail system* are a visible representative of the *state* and must use the *systems* in a legal, professional and responsible manner. Unless approved by management or specifically allowed by the SE Internet Acceptable Use Policy, *SE users* must not connect to commercial E-mail *systems* (i.e., AOL, Yahoo, etc.) from any *SE system*, workstation, or internal email account. If connections to commercial email systems are allowed, no data associated with the SE is to be sent unless specifically authorized by policy or the SE ISO. *Users* of *SE E-mail systems* must comply with this policy and be knowledgeable of their responsibilities as defined in the Communications and Network Management Policy, Internet and Electronic Mail Acceptable Use.

Portable Devices

- A. All portable computing resources and *information* media must be secured to prevent compromise of *confidentiality* or *integrity*. No *computer* device may store or transmit *non-public information* without suitable protective measures that are approved by the *SE ISO*.
- B. When using mobile computing facilities such as notebooks, palmtops, laptops and mobile phones, special care must be taken to ensure that *information* is not compromised. Approval is contingent on satisfaction of the requirements for physical protection, access *controls*, cryptographic techniques, back-ups, *virus* protection and the rules associated with connecting mobile facilities to networks and guidance on the use of these facilities in public places.
- Care must be taken when using mobile computing facilities in public places, meeting rooms and other unprotected areas outside of the *SE's* premises. Protection must be in place to avoid the *unauthorized access* or disclosure of the *information* stored and processed by these facilities, e.g. using cryptographic techniques.
 - It is important that when such facilities are used in public places care must be taken to avoid the *risk* of unauthorized persons viewing *information* on-screen.
 - *Procedures* against malicious software shall be developed and implemented and be kept up to date. Equipment will be available to enable the quick and easy back up of *information*. These back-ups must be given adequate protection against theft or loss of *information*.

- Equipment carrying important, sensitive and/or *critical* business *information* must not be left unattended and, where possible, must be physically locked away, or special locks must be used to secure the equipment.
- Training must be provided to staff using mobile computing resources to raise their awareness on the additional *risks* resulting from this way of working and the *controls* that will be implemented.
- Employees in the possession of portable, laptop, notebook, palmtop, and other transportable *computers* must not check these *computers* in airline luggage *systems*. These *computers* must remain in the possession of the traveler as hand luggage unless other arrangements are required by Federal or *State* authorities. The exception to this is a device with full disk encryption and adequate password controls enabled.

Telephones and Fax Equipment

The use of telephones outside the *SE* for business reasons is sometimes necessary, but it can create security exposures. Employees should:

- take care that they are not overheard when discussing sensitive or confidential matters;
- avoid use of any wireless or cellular phones when discussing sensitive or confidential *information*;
- avoid leaving sensitive or confidential messages on voicemail *systems*;
- if sending sensitive or confidential documents via fax, verify the phone number of the destination fax. Contact the recipient to ensure protection of the fax, either by having it picked up quickly or by ensuring that the fax output is in a secure area;
- avoid using *Internet* fax services to send or receive sensitive or confidential *information*;
- not use *third party* fax services to send or receive sensitive or confidential *information*;
- not send sensitive or confidential documents via wireless fax devices;
- not send teleconference call-in numbers and passcodes to a pager, if sensitive or confidential *information* will be discussed during the conference;
- when chairing a sensitive or confidential teleconference, confirm that all participants are authorized to participate, before starting any discussion.

Wireless Networks

- A. Advances in wireless technology and pervasive devices create opportunities for new and innovative business solutions. However security *risks*, if not addressed correctly, could expose *SE information systems* to a loss of service or compromise of sensitive *information*.
- B. Wireless is a shared medium. Everything that is transmitted over the radio waves can be intercepted if the interceptor is within the coverage area of the radio transmitters. This represents a potential security issue in the wireless Local Area Networks

(LANs). The security exposure is more evident if the wireless LANs are deployed or used in public areas, such as airports, hotels or conference centers.

- C. No wireless network or wireless access point will be installed without a *risk assessment* being performed and the approval of the *SE ISO*.
- D. Suitable *controls*, such as *Media Access Control (MAC) address* restriction, *authentication*, and *encryption* must be implemented to ensure that a wireless network or access point can not be exploited to disrupt *SE information* services or to gain *unauthorized access* to *SE information*. When selecting wireless technologies, 802.11x wireless network security features on the equipment must be available and implemented from the beginning of the deployment. Network Access Control technologies are strongly recommended for new deployments.
- E. Access to *systems* that hold *non-public information* or the transmission of *non-public* or sensitive *information* via a wireless network is not permitted unless appropriate and adequate measures have been implemented and approved by the *SE ISO*. Such measures must include *authentication*, *authorization*, access *controls* and logging (refer to Part 10 Access Control Policy, Monitoring System Access and Use).

Modem Usage

Connecting dial-up modems to *computer systems* which are also connected to *SE*'s local area network or to another internal communication network is prohibited unless the *SE ISO* approves the request, a *risk assessment* is performed and risks are appropriately mitigated.

Public Websites Content Approval Process

- A. The *World Wide Web* provides an opportunity for *SEs* both to disseminate *information* and to provide interactive government services quickly and cost effectively. Because anything posted on a public web server is globally available and each web presence is a potential connection path to *SE* networks, care must be exercised in the deployment of publicly accessible servers. There is also potential for an insecure server to be used or exploited to assist in an unauthorized or illegal activity, such as an attack on another web site.
- B. The content of each public site must be reviewed according to a process that will be defined and approved by the *SE*. A process must be established for reviewing and approving updates to publicly available content. These reviews must include consideration of *copyright* issues (both the potential publication of *copyright* material and the appropriate protection of *SE copyright* materials), the type of *information* being made available (*confidentiality*, *privacy* and *sensitivity* of the *information*), the accuracy of the *information* and potential legal implications of providing the *information*.
- C. Sensitive or confidential *State information* must not be made available through a server that is available to a public network without appropriate safeguards approved by the *SE ISO*. The *SE ISO* will implement safeguards to ensure *user authentication*, *data confidentiality* and *integrity*, access control, *data* protection and logging

mechanisms. Definition of sensitive *information* includes, but is not limited to the following related *information*:

- structures, individuals and services essential to the security, government, or economy of the *State*, including telecommunications (including voice and *data* transmission and the *Internet*);
- electrical power, gas and oil storage and transportation;
- banking and finance;
- transportation;
- water supply;
- emergency services (including medical, fire, and police services);
- and the continuity of government operations.

Sensitive *information* includes, but is not limited to:

- *Critical* Infrastructure Assets which are so vital that their infiltration, incapacitation, destruction or misuse would have a debilitating impact on health, welfare or economic security of the citizens and businesses of South Carolina.
- *data* that identifies specific structural, operational, or technical *information*, such as: maps, mechanical or architectural drawings, floor plans, operational plans or *procedures*, or other detailed *information* relating to electric, natural gas, steam, water supplies, nuclear or telecommunications *systems* or infrastructure, including associated facilities;
- training and security *procedures* at sensitive facilities and locations;
- descriptions of technical processes and technical architecture;
- plans for *disaster* recovery and business continuity;
- inventory/depictions/photographs/locations of physical equipment, assets and infrastructure;
- reports, surveys, or audits that contain sensitive *information*; and
- other subjects and areas of relevant concern as determined by the *SE*.

- D. The design of a hosting service must be reviewed and approved in writing by the *SE ISO* to ensure that the security of the web server, protection of *SE* networks, performance of the site, *integrity* and *availability* considerations are adequately addressed.
- E. The implementation of any web site or software is subject to all requirements set forth in Part 11, Systems Development and Maintenance Policy. The service must be reviewed and approved by the *SE ISO* to ensure that the collection and processing of sensitive *information* meets *SE* security and *privacy* requirements. The review must ensure that sensitive *information* is adequately protected in transit over public and *SE* networks, in storage and while being processed.

Electronic Signatures

South Carolina Uniform Electronic Transactions Act (UETA) (Code of Law of South Carolina, 1976, Section 26-6-10 through 25-6-210) provides that the use of an electronic signature that meets the requirements established by UETA shall have the same validity and affect as a signature affixed by hand. *SEs* must comply with UETA and any associated rules and regulations.

Public Key Infrastructure

The establishment of Public Key Infrastructure (PKI) based security architecture is a significant undertaking that requires the establishment of the required business processes to support the PKI and the implementation of technology to support the resulting business processes. In order for the *SE* to operate with a PKI based Security Architecture, the following requirements must be satisfied.

- An appropriate trust model must be defined to include all of the stakeholders. The resulting trust domain or multiple trust domains must be supported by the appropriate certificate policies and certification practice statements. These apply to the stakeholders and *users* of *SE systems* and *data*.
- Where PKI is used for digital signatures or *encryption*, it must operate under and comply with the *State* Certificate Policy for Digital Signatures and *Encryption* issued by the Office for Technology and any associated rules and regulations.

Part 9. Operational Management Policy

- A. All *SE information* processing facilities must have documented operating instructions, management processes and formal *incident* management *procedures* related to *information* security matters, that define roles and responsibilities of affected individuals who operate or use *SE information* processing facilities.
- B. Computing hardware, software or *system* configurations provided by *SE* must not be altered or added to in any way unless exempted by documented written policy, *procedures* or specific written approval of *SE* management.
- C. Where a *SE* provides a server, application or network services to another *SE*, operational and management responsibilities must be coordinated by both *SEs*.

Segregation of Security Duties

- A. To reduce the *risk* of accidental or deliberate *system* misuse, separation of duties or areas of responsibility should be implemented where practical.
- B. Whenever separation of duties is difficult to achieve, other compensatory *controls* such as monitoring of activities, audit trails and management supervision must be implemented. At a minimum the audit of security must remain independent and segregated from the security function.

Separation of Development, Test and Production Environments

- A. Separation of the development, test and production environments is required, either logically or physically. Processes must be documented and implemented to govern the transfer of software from the development environment to the production platform. The following *controls* must be considered:
- development software and tools must be maintained on computer systems isolated from the production environment. Isolate development software on physically separate machines or separate them by access controlled domains or directories;
 - access to compilers, editors and other *system* utilities must be removed from production systems when not required;
 - logon procedures and environmental identification must be sufficiently unique for production testing and development;
 - Controls must be in place to issue short-term access to development staff to correct problems with production systems allowing only necessary access.
- B. Development and testing can cause serious problems to the production environment if separation of these environments does not exist. The degree of separation between the production and test environments must be considered by each *SE* to ensure adequate protection of the production environment.
- C. Separation must also be implemented between development and test functions. Each *SE* must consider the use of a stable quality assurance environment where *user* acceptance testing can be conducted and changes cannot be made to the programs being tested.

System Planning and Acceptance

- A. Because *system* and *data availability* is a security concern, advance planning and preparation must be performed to ensure the *availability* of adequate capacity and resources. The security requirements of new *systems* must be established, documented and tested prior to their acceptance and use.
- B. Storage and memory capacity demands must be monitored and future capacity requirements projected to ensure adequate processing and storage capability is available when needed. This *information* will be used to identify and avoid potential bottlenecks that might present a *threat* to *system* security or *user* services.
- C. Acceptance criteria must be developed and documented for new *information systems*, upgrades and new versions of existing *systems*. Acceptance testing will be performed to ensure security requirements are met prior to the *system* being migrated to the production environment. *SE* managers will ensure that the security requirements and criteria for acceptance are clearly defined, agreed, documented and tested.

Protection against Malicious Code

Software and associated *controls* must be implemented across *SE systems* to prevent and detect the introduction of malicious code. The introduction of malicious code such as a *computer virus*, network *worm* program and *Trojan horse* can cause serious damage to networks, workstations and business *data*. *Users* must be made aware of the dangers of unauthorized or malicious code. *SE* must implement *controls* to detect and prevent a *computer virus* from being introduced to the *SE* environment. The types of *controls* and frequency of updating signature files, is dependent on the value and *sensitivity* of the *information* that could be potentially at *risk*. For *SE* workstations, malware signatures may need to be updated as much as hourly if possible. On *host systems* or servers, the signature files and patches should be updated as often as internal change management allows.

Software Maintenance

- A. All *system* software must be maintained at a vendor-supported level to ensure software accuracy and *integrity*, unless *SE ISO* approves otherwise in writing.
- B. Maintenance of *SE*-developed software will be logged to ensure changes are authorized, tested and accepted by *SE* management.
- C. All known security patches must be reviewed, evaluated and appropriately applied in a timely manner to reduce the *risk* of security *incidents* that could affect the *confidentiality*, *integrity* and *availability* of business *data* or software *integrity*.

Information Back-up

The scope of this section is limited to the IT infrastructure, and the *data* and applications of the local *SE* environment. A *threat* and *risk assessment* must be performed by the *SE* to determine the criticality of business *systems*, and the time frame required for recovery. To ensure interruptions to normal *SE* business operations are minimized, and *critical SE* business applications and processes are protected from the effects of major failures, each *SE* business unit, including *SE Security Management*, in cooperation with the *SE CIO*, must develop plans that can meet the IT backup and recovery requirements of the *SE*. Back-ups of *critical SE data* and software must be performed regularly.

Assessment

An assessment of the criticality of the services provided and the *sensitivity* of the *information* held on all *hosts* and servers (including all installed software and operating *system* versions, *firewalls*, switches, routers and other communication equipment operating *systems*) will be maintained.

System Security Checking

- A. *Systems* and services that process or store sensitive or confidential *information* or provide support for *critical* processes must undergo *technical security reviews* to ensure compliance with implementation *standards* and for vulnerabilities to subsequently discovered *threats*. Reviews of *systems* and services that are essential

to supporting a *critical SE* function must be conducted at least once every year. Reviews of a representative sample of all other *systems* and services must be conducted at least once every 24 months.

- B. Any deviations from expected or required results that are detected by the *technical security review* process must be reported to the *SE ISO* and corrected immediately. In addition, the *SE* application owner must be advised of the deviations and must initiate investigation of the deviations (including the review of *system* activity log records if necessary).

Part 10. Access Control Policy

- A. To preserve the properties of *integrity*, *confidentiality* and *availability*, the *SE*'s *information assets* will be protected by logical and physical access control mechanisms commensurate with the value, *sensitivity*, consequences of loss or compromise, legal requirements and ease of recovery of these assets.
- B. *Information owners* are responsible for determining who should have access to protected resources within their jurisdiction, and what those access privileges will be (read, update, etc.). These access privileges will be granted in accordance with the *user*'s job responsibilities.

User Registration and Management

- A. A *user* management process shall be established and documented by the *SE* to outline and identify all functions of *user* management, to include the generation, distribution, modification and deletion of *user* accounts for access to resources. The purpose of this process is to ensure that only authorized individuals have access to *SE* applications and *information* and that these *users* only have access to the resources required for authorized purposes.
- B. The *user* management process must include the following sub-processes as appropriate:
- enrolling new *users*;
 - removing user-IDs;
 - granting "privileged accounts" to a user;
 - removing "privileged accounts" from a user;
 - periodic reviewing "*privileged accounts*" of *users*;
 - periodic reviewing of *users* enrolled to any *system*; and
 - assigning a new *authentication* token (e.g. password reset processing).
- C. The appropriate *information owner* or other authorized officer will make requests for the registration and granting of access rights for *State* employees.
- D. For applications that interact with individuals that are not employed by an *SE*, the *information owner* is responsible for ensuring an appropriate *user* management

process is implemented. *Standards* for the registration of such external *users* must be defined, to include the credentials that must be provided to prove the identity of the *user* requesting registration, validation of the request and the scope of access that may be provided.

Logon Banner

Logon banners should be implemented on all *systems* where that feature exists to inform all *users* that the *system* is for *SE* business or other approved use consistent with *SE* policy, and that *user* activities may be monitored and the *user* should have no expectation of *privacy*. Logon banners are usually presented during the *authentication* process.

Privileged Accounts Management

The issuance and use of *privileged accounts* will be restricted and controlled. Inappropriate use of *system* account privileges is often found to be a major contributing factor to the failure of *systems* that have been breached. Processes must be developed to ensure that uses of *privileged accounts* are monitored, and any suspected misuse of these accounts is promptly investigated. Passwords of *multi-user system privileged accounts* must be changed more often than normal user accounts.

User Password Management

- A. Passwords are a common means of authenticating a *user's* identity to access an *information system* or service. Password *standards* must be developed and implemented to ensure all authorized individuals accessing *SE* resources follow proven password management practices. These password rules must be mandated by automated *system controls* whenever possible. These password best practices include but are not limited to:
- passwords must not be stored in clear text;
 - use passwords that are not easily guessed or subject to disclosure through a dictionary attack;
 - keep passwords confidential – do not share individual;
 - change passwords at regular intervals;
 - change temporary passwords at the first logon;
 - when technology permits, passwords must contain a mix of alphabetic, numeric, special, and upper/lower case characters; and
 - do not include passwords in any automated logon process, e.g., stored in a macro or function key, web browser or in application code
- B. To ensure good password management, password *standards* must be implemented on all *SE* platforms when technically feasible.

Network Access Control

Access to a *SE's* trusted internal network must require all authorized *users* to authenticate themselves through use of an individually assigned user-ID and an *authentication* mechanism, e.g., password, token, smart card.... Network *controls* must be developed and implemented that ensure that an authorized *user* can access only those network resources and services necessary to perform their assigned job responsibilities.

User Authentication for External Connections (Remote Access Control)

(Also see Part 8. Communication and Network Management Policy, External Connections)

- A. To maintain *information security*, *SE* requires that individual accountability be maintained at all times, including during remote access. For the purposes of this policy, “remote access” is defined as any access coming into the *SE*’s network from off the *SE*’s private, trusted network. This includes, but is not limited to:
- connecting from another location (including but not limited to hotels, broadband locations, kiosks, wireless hotspots, etc.) over public lines by an employee or other authorized individual for the purpose of telecommuting
 - connecting from a *third party* network via dial or other temporary access technology to the *SE* network;
- B. Connection to *SE*’s networks must be done in a secure manner to preserve the *integrity* of the network, *data* transmitted over that network, and the *availability* of the network. Security mechanisms must be in place to control access to *SE systems* and networks remotely from fixed or mobile locations.
- C. Advance approval for any such connection must be obtained from the *SE* management and the *SE ISO*. An assessment must be performed and documented to determine the scope and method of access, the *risks* involved and the contractual, process and technical *controls* required for such connection to take place.
- D. Because of the level of *risk* inherent with remote access, use of a strong password or another comparable method is required prior to connecting to any *SE* network. All sessions are subject to periodic and random monitoring.
- E. When accessing a *SE* network remotely, identification and *authentication* of the entity requesting access must be performed in such a manner as to not disclose the password or other *authentication information* that could be intercepted and used by a *third party*.
- F. Use of a common access point is required. This means that all remote connections to a *computer* must be made through managed central points-of-entry. Using this type of entry *system* to access a *SE computer* provides many benefits, including simplified and cost effective security, maintenance, and support.
- G. For a vendor to access *SE computers* or software, individual accountability is also required. For those *systems* (hardware or software) for which there is a built-in user-ID for periodic maintenance, the account must be disabled until the user-ID is needed. The activity performed while this vendor user-ID is in use must be logged. Since these accounts are not regularly used, the vendor user-ID must be disabled, the password changed or other *controls* implemented to prevent or monitor unauthorized use of these *privileged accounts* during periods of inactivity.
- H. In the special case where servers, storage devices or other *computer* equipment has the capability to automatically connect to a vendor to report problems or suspected

problems, the *SE ISO* must review any such connection and process to ensure that connectivity does not compromise the *SE* or other *third party* connections.

- I. Working from a remote location must be authorized by *SE* management and appropriate arrangements made for this activity through written policy and procedure, to ensure the work environment at the remote location provides adequate security for *SE data* and computing resources. Appropriate protection mechanisms commensurate with *risk* and exposure must be in place to protect against theft of *SE* equipment, unauthorized disclosure of *SE information*, misuse of *SE* equipment or *unauthorized access* to the *SE* internal network or other facilities by anyone including family and friends. To ensure the proper security *controls* are in place and all *SE* security *standards* are followed, the following must be considered:
 - the *physical security* of the remote location including using a laptop at any location other than an employee's work station;
 - the accessing mechanism given the sensitivity of *SE's* internal *system* the sensitivity of and method of transmitting *information*.
 - appropriate business continuity procedures including backing up critical *information*.
- J. The following *controls* must be considered and appropriately implemented. If/when implemented, they must be monitored and audited:
 - a definition of the *classification* of the *information* and the *systems* and services that the remote *user* is authorized to access;
 - documented procedures and necessary tools allowing for secure remote access such as *authentication* tokens and/or passwords, including procedures for revocation of authorization and return of equipment;
 - hardware and software support and maintenance procedures including anti-*virus* software and maintenance of current signature files;
 - implementation of suitable network boundary *controls* to prevent unauthorized *information* exchange between *SE* networks connected to remote *computers* and externally connected networks, such as the *Internet*. Such measures include *firewalls* and *intrusion detection* techniques at the remote location;
 - *encryption* of sensitive *information* in transit and on the local computer workstation;
 - *physical security* of the equipment used for remote access (e.g. such as cable locking device, or locking computer cabinet/secure storage area);

Segregation of Networks

When the *SE* network is connected to another network, or becomes a segment on a larger network, *controls* must be in place to prevent *users* from other connected networks access to sensitive areas of the *SE's* private network. Routers or other technologies must be implemented to control access to secured resources on the trusted *SE* network.

Operating System Access Control

- A. Access to operating *system* code, services and commands must be restricted to only those individuals necessary in the normal performance of their job responsibilities. All individuals (*systems* programmers, database administrators, network and security administrators, etc.) will have a unique *privileged account* (user-ID) for their personal and sole use so that activities can be traced to the responsible person. User-IDs must not give any indication of the *user's* privilege level, e.g., supervisor, manager, administrator. These individuals should also have a second user-ID when performing normal business transactions, such as when accessing the *SE* E-mail *system*.
- B. In certain circumstances, where there is a clear business requirement or *system* limitation, the use of a shared user-ID/password for a group of *users* or a specific job can be used. Approval by *SE ISO* and *SE* management must be documented in these cases. Additional compensatory *controls* must be implemented to ensure accountability is maintained (refer to Part 3. Information Policy, Individual Accountability)
- C. Where technically feasible, default administrator accounts must be renamed, removed or disabled. The default passwords for these accounts must be changed if the account is retained, even if the account is renamed or disabled.

Application Access Control

Access to *SE* business and *systems* applications must be restricted to those individuals who have a business need to access those applications or *systems* in the performance of their job responsibilities. Access to source code for applications and *systems* must be restricted, and these accesses should be further restricted so that authorized *SE* staff and contractors can access only those applications and *systems* they directly support.

Monitoring System Access and Use

Systems and applications must be monitored and analyzed to detect deviation from the access control policy and record events to provide evidence and to reconstruct lost or damaged *data*. Audit logs recording exceptions and other security-relevant events must be produced and kept consistent with record retention schedules developed in cooperation with the State Archives and History (SAH) and *SE* requirements to assist in future investigations and access control monitoring. Audit logs will be created and protected.

Part 11. Systems Development and Maintenance Policy

- A. Software applications are developed or acquired to provide efficient solutions to *SE* business problems. These applications generally store, manipulate, retrieve and display *information* used to conduct *SE* business. The *SE* business units become dependent on these applications, and it is essential the *data* processed by these applications be accurate. It is also *critical* that the software that performs these activities be protected from *unauthorized access* or tampering.
- B. To ensure that security is built into all *SE information systems*, all security requirements, including the need for rollback arrangements, must be identified during

the requirements phase of a project and justified, agreed to and documented as part of the overall business case for an *SE information system*. To ensure this activity is performed, the *SE ISO* must be involved in all phases of the *System* Development Lifecycle from the requirements definition phase, through implementation and eventual application retirement.

- C. Security requirements and *controls* must reflect the business value of the *information* involved, and the potential business damage that might result from a failure or absence of security measures. This is especially *critical* for *Internet* Web and other online applications. The framework for analyzing the security requirements and identifying *controls* to meet them is associated with *threat* assessment and *risk management* which must be performed by the *information owner*, reviewed by the *SE ISO* and written approval by *SE* executive management
- D. A process must be established and implemented for each application to:
- address the *business risks* and develop a profile of the *data* to help to understand the *risks*;
 - identify security measures based on the *risk* profile and protection requirements;
 - identify and implement specific *controls* based on security requirements and technical architecture;
 - implement a method to test the effectiveness of the security *controls*;
 - identify processes and *standards* to support changes, ongoing management and to measure compliance.
- B. *Controls* in *systems* and applications can be placed in many places and serve a variety of purposes. The specific control mechanisms must be documented at the application level, *SE*'s *System* Development Methodology, and in the *SE*'s security *standards* documents. The security measures that are implemented must be based on the *threat* and *risk assessments* of the *information* being processed and cost/benefit analysis.

Input Data Validation

An application's input *data* must be validated to ensure it is correct and appropriate including the detection of data input errors. Personnel must be clearly identified to perform these functions. The checks that are performed on the client side must also be performed at the server to ensure *data integrity*. Checks will be performed on the input of business transactions, static *data* (names, addresses, employee numbers, etc.) and parameter tables. Set up a process to verify and correct fields, characters, completeness of *data* and range/volume limits.

Control of Internal Processing

Data that has been entered correctly can be corrupted by processing errors or through deliberate acts. Checks and balances must be incorporated into *systems* to prevent or stop an incorrect program from running. Application design must ensure that *controls* are implemented to minimize the *risk* of processing failures leading to a loss of *data* or *system integrity*. Consider the use of correction programs to recover from failures and access to add and delete functions to make changes to application data and to ensure the correct processing of *data*.

Message Integrity

It is necessary to put into place a method to detect unauthorized changes to the content of a transmitted electronic message. Message *integrity* must be considered for applications where there is a security requirement to protect the message or *data* content e.g. electronic funds transfer, EDI transactions, etc. An assessment of threats and *risks* will be performed to determine if message *integrity* is required and to identify the most appropriate method of implementation. It should also be noted that message *integrity* will not protect against unauthorized disclosure. *Encryption* techniques should be used as a means of implementing message *integrity*.

Cryptographic Controls

Use of cryptography for protection of high-*risk information* must be considered when other *controls* do not provide adequate protection. *Encryption* is a technique that can be used to protect the *confidentiality* of *information*. It must be considered for the protection of sensitive or *critical information*. Based on a *risk assessment*, the required level of protection will be identified taking into account the type and quality of the *encryption* algorithm used and the length of cryptographic keys employed. To the extent possible, consideration must also be given to the regulations and national restrictions that may apply to the use of cryptographic techniques in different parts of the world. In addition, and to the extent possible, consideration must be given to *controls* that apply to the export and import of cryptographic technology.

Key Management

Protection of cryptographic keys is essential if cryptographic techniques are going to be used. A secured environment must be established to protect the cryptographic keys used to encrypt and decrypt *information*. Access to these keys must be tightly controlled to only those individuals who have a business need to access the keys. Loss of *confidentiality* of a cryptographic key would cause all *information* encrypted with that key to be considered compromised.

Protection of System Test Data

- A. Test *data* is intended to test the expected behavior of software, *systems* and applications. Test *data* is developed to test a comprehensive set of conditions and outcomes, including exception processing and error conditions to demonstrate accurate processing and handling of *information* and the stability of the software, *system* or application.
- B. Once test *data* is developed, it must be protected and controlled for the life of the testing. In those cases where test *data* is reused, whenever modifications are made to the software, *system* or application then the test *data* must be protected and controlled during the entire useful life. This protection mechanism is essential to ensuring a valid and controlled simulation with predictable outcomes.
- C. Production *data* may be used for testing only if the following *controls* are applied;

- a business case is documented, approved in writing by the *information owner* and access *controls*, system configurations and logging requirements for the production *data* are applied to the test environment; or
- a business case is documented, approved in writing by the *information owner* and personal, sensitive or confidential *data* will be masked or overwritten with fictional *information* and the *data* will be deleted as soon as the testing is completed.

Change Control Procedures

- A. To minimize the possibility of corruption of *information systems*, strict *controls* over changes to *information systems* must be implemented. Formal change control *procedures* for business applications must be developed, implemented and enforced. They must ensure that security and control *procedures* are not compromised, that support programmers are given access only to those parts of a *system* necessary to perform their jobs, and that formal agreement and approval processes for changes are implemented. These change control *procedures* will apply to *SE* business applications as well as *systems* software used to maintain operating *systems*, network software, hardware changes, etc.
- B. In addition, access to source code libraries for both *SE* business applications and operating *systems* must be tightly controlled to ensure that only authorized individuals have access to these libraries and that access is logged to ensure all activity can be monitored.

Part 12. Cyber Security Citizens' Notification Policy

- A. This policy requires notification to impacted South Carolina residents and non-residents. South Carolina values the protection of *private information* of individuals. All *SEs* are required to notify an individual when there has been or is reasonably believed to have been a compromise of the individual's *private information* in compliance with the Information Security Breach and Notification sections of this policy.
- B. The *SE*, after consulting with the internal Security team as well as possibly external consultants or the CIO ISO to determine the scope of the breach and restoration measures, shall notify an individual when it has been determined that there has been, or is reasonably believed to have been a compromise of *private information* through unauthorized disclosure.
- C. A compromise of *private information* shall mean the unauthorized acquisition of unencrypted computerized *data* with *private information*.
- D. If encrypted *data* is compromised along with the corresponding encryption key, the *data* shall be considered unencrypted and thus fall under the notification requirements.

- E. Notification may be delayed if a law enforcement agency determines that the notification impedes a criminal investigation. In such case, notification will be delayed only as long as needed to determine that notification no longer compromises any investigation.
- F. *SE* will notify the affected individual. Such notice shall be directly provided to the affected persons by one of the following methods:
- written notice;
 - electronic notice, provided that the person to whom notice is required has expressly consented to receiving said notice in electronic form and a log of each such notification is kept by the *SE* who notifies affected persons in such form;
 - telephone notification provided that a log of each such notification is kept by the *SE* who notifies affected persons; or
 - Substitute notice, if a *SE* demonstrates to the state attorney general that the cost of providing notice would exceed two hundred fifty thousand dollars, or that the affected class of subject persons to be notified exceeds five hundred thousand, or such *SE* does not have sufficient contact information. Substitute notice shall consist of all of the following:
 - e-mail notice when such *SE* has an e-mail address for the subject persons;
 - conspicuous posting of the notice on such *SE's* web site page, if such *SE* maintains one; and
 - notification to major statewide media.
- G. The *SE* shall notify the CIO ISO as to the timing, content and distribution of the notices and approximate number of affected persons as per the *SE's* accepted IRP
- H. The *SE* shall notify the Attorney General and the Department of Consumer Affairs, whenever notification to a South Carolina resident is necessary, as to the timing, content and distribution of the notices and approximate number of affected persons.
- I. Regardless of the method by which notice is provided, such notice shall include contact *information* for the *SE* making the notification and a description of the categories of information that were, or are reasonably believed to have been, acquired by a person without valid authorization, including specification of which of the elements of *personal information* and *private information* were, or are reasonably believed to have been, so acquired.
- J. This Policy also applies to *information* maintained on behalf of a *SE* by a *third party*.
- K. When more than five thousand South Carolina residents are to be notified at one time, then the *SE* shall notify the *consumer reporting agencies* as to the timing, content and distribution of the notices and the approximate number of affected individuals. This notice, however, will be made without delaying notice to the individuals.

Part 13. Compliance Policy

Monitoring

Consistent with applicable law and *SE* policies, the *SE* reserves the right to monitor, inspect, and/or search at any time all *SE information systems*. Since *SE's computers* and networks are provided for business purposes, staff members shall have no expectation of *privacy* in the *information* stored in or sent through these *information systems*. *SE* management additionally retains the right to remove from its *information systems* any unauthorized material.

Compliance

- A. At the *state* government entity level, each *SE* shall implement a process to determine the level of compliance with this policy. A review to ensure compliance with this policy must be conducted at least annually and *SE* Executive Management will certify and report the *SE's* Level of Compliance to the AOC or its designated committee/group/organization in writing by July 10th of each year. The periodic review for compliance by the organization may also involve an additional request for review originating with the *SE* by either an outside security and audit organization or the CIO ISO's office. Such reviews may include, but are not limited to, reviews of the technical and business analyses required to be developed pursuant to this policy, and other project documentation, technologies or *systems* which are the subject of the published policy or *standard*.
- B. Compliance with this policy is mandatory. Each *user* must understand his/her role and responsibilities regarding *information security* issues and protecting *SE's information*. The failure to comply with this or any other *security policy* that results in the compromise of *SE information confidentiality, integrity, privacy, and/or availability* may result in appropriate action as permitted by law, rule, regulation or negotiated agreement. Each *SE* will take every step necessary, including legal and administrative measures, to protect its assets and shall establish the post of *SE* Information Security Officer to monitor compliance with policy matters.
- C. *SE* managers and supervisors will ensure that all security processes and *procedures* within their areas of responsibility are followed. In addition, all business units within the *SE* may be subject to regular reviews to ensure compliance with security policies and *standards*.

Enforcement and Violation Handling

- A. Any compromise or suspected compromise of this policy must be reported to the appropriate *SE* management, the *SE* CIO and ISO, and other entities as required by law. Any violations of security policies may be subject to disciplinary or other appropriate action in accordance with law, rule, regulation, policy or negotiated agreement.
- B. Security *incident* reports indicating the *risk* level of the violation must be reported to responsible entities in accordance with *SE* internal policy. Access *authorization* for *user* accounts involved in a compromise may be suspended during the time when a suspected violation is under investigation. Automated violation reports generated by

the various security *systems* will be forwarded to the appropriate management and the *SE* Information Security Officer for timely resolution.

DOCUMENT CHANGE MANAGEMENT

Requests for changes to this policy must be presented by the *SE* CIO or *ISO* to the AOC Security Sub-Committee. If the AOC Security Sub-Committee agrees to the change, it will formally draft the change and have it reviewed and approved through the AOC's normal policy approval process where warranted. Each *SE ISO* will be responsible for communicating the approved changes to their organization.

This policy and supporting policies and *standards* will be reviewed at a minimum on an annual basis.

DEFINITIONS

Authentication: The process to establish and prove the validity of a claimed identity.

Authenticity: This is the exchange of security *information* to verify the claimed identity of a communications partner.

Authorization: The granting of rights, which includes the granting of access based on an authenticated identity.

Availability: This is the 'property' of being operational, accessible, functional and usable upon demand by an authorized entity, e.g. a *system* or *user*

Business Risk: This is the combination of *sensitivity*, *threat* and *vulnerability*.

Broadband: A transmission medium that can carry signals from multiple independent network carriers on a single coaxial or fiber optic cable, by establishing different bandwidth channels. Broadband technology can support a wide range of frequencies and is used to transmit data, voice, and video over long distances.

CIO: Chief Information Officer.

Classification: The designation given to *information* or a document from a defined category on the basis of its *sensitivity*.

Computer: All physical, electronic and other components, types and uses of computers, including but not limited to hardware, software, central processing units, electronic communications and *systems*, databases, memory, *Internet* service, *information systems*, laptops, Personal Digital Assistants and accompanying equipment used to support the use of computers, such as printers, fax machines and copiers, and any updates, revisions, upgrades or replacements thereto.

Consumer Reporting Agency: Consumer reporting agency shall mean any person which, for monetary fees, dues, or on a cooperative nonprofit basis, regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of furnishing consumer reports to third parties, and which uses any means or facility of interstate commerce for the purpose of preparing or furnishing consumer reports. A list of consumer reporting agencies shall be compiled by the state attorney general and furnished upon request to state entities required to make a notification under this policy.

Conferencing: Conferencing allows an organization to hold an online meeting that allows sharing of screens with others and the use of an online whiteboard for collaborative discussions. Conferencing technology allows groups of *users* in a networked environment to collaborate by communicating via voice and text messages, sharing access to files and supporting the creation and modification of work products by the entire team.

Confidentiality: The property that *information* is not made available or disclosed to unauthorized individuals, entities, or processes.

Controls: Countermeasures or safeguards that are the devices or mechanisms that are needed to meet the requirements of policy.

Copyright: A property right in an original work of authorship fixed in any tangible medium of expression, giving the holder the exclusive right to reproduce, adapt, distribute, perform and display the work (*Black's Law Dictionary, 7th ed. 1999*).

Cracking: Breaking into or attempting to break into another *system* in excess of one's access rights or *authorization* with or without malicious intent.

Critical: A condition, *vulnerability* or threat that could cause danger to *data*, a *system*, network, or a component thereof.

Custodian of Information: An employee or organizational unit acting as a caretaker of an automated file or database on behalf of its owner.

Data: Any *information* created, stored (in temporary or permanent form), filed, produced or reproduced, regardless of the form or media. *Data* may include, but is not limited to personally identifying *information*, reports, files, folders, memoranda, statements, examinations, transcripts, images, communications, electronic or hard copy.

Data Security: The protection of *information assets* from accidental or intentional but unauthorized disclosure, modification, or destruction, or the inability to process that *information*.

Decryption: The reversal of a corresponding reversible *encryption* to render *information* intelligible using the appropriate algorithm and key.

Denial of Service: An attack that takes up so much of the company's business resource that it results in degradation of performance or loss of access to the company's business services or resources.

Disaster: A condition in which *information* is unavailable, as a result of a natural or man-made occurrence, that is of sufficient duration to cause significant disruption in the accomplishment of the SE's business objectives as determined by SE's management.

DMZ: Demilitarized zone; a semi-secured buffer or region between two networks such as between the public *Internet* and the trusted private *State* network.

DSL: Digital Subscriber Line (DSL): a data communications link to the local telephone company using copper telephone wiring. DSL and cable (broadband) have become popular means of delivering always-connected Internet access at speeds much faster than dial-up.

E-commerce: The electronic conducting of business transactions and exchanging something of value for something else of value e.g. exchanging money for goods or services.

Encryption: The cryptographic transformation of *data* to render it unintelligible through an algorithmic process using a cryptographic key.

Extranet: The expanded use and logical connection of various local and wide area networks beyond their traditional *Internet* configuration that uses the *standard Internet* protocol, TCP/IP, to communicate and conduct *E-commerce* functions.

Firewall: A security mechanism that creates a barrier between an internal network and an external network.

Host: A *system* or *computer* that contains business and/or operational software and/or *data*.

HTTP: The protocol that delivers hypertext documents, via the *World Wide Web*, is called the Hypertext Transfer Protocol (http).

Incident: Any adverse event that threatens the *confidentiality, integrity* or accessibility of *information* resources.

Incident Response: The manual and automated *procedures* used to respond to reported network intrusions (real or suspected); network failures and errors; and other undesirable events.

Information: Information is defined as the representation of facts, concepts, or instructions in a formalized manner suitable for communication, interpretation, or processing by human or automated means.

Information Assets: (1) All categories of automated *information*, including but not limited to: records, files, and databases, and (2) *information* technology facilities, equipment (including *microcomputer systems*), and software owned or leased by the *State*.

Information Owner: An individual or a group of individuals that has responsibility for making *classification* and control decisions regarding use of *information*.

Information Security: The concepts, techniques and measures used to protect *information* from accidental or intentional *unauthorized access*, modification, destruction, disclosure or temporary or permanent loss (See Availability).

Information Security Architecture: A framework designed to ensure *information security Principles* are defined and integrated into business and IT processes in a consistent manner.

Information Theft: Loss of business *information* through theft of *data*.

Instant Messaging (IM): The ability to exchange short messages online with co-workers or others. IM solutions can take several forms. They can use an existing *Internet* based service, or they can be an *Intranet* only solution implemented and controlled within an IT department. The latter is significantly more secure than the former, but lacks access to business partners.

Integrity: The property that *data* has not been altered or destroyed from its intended form or content in an unintentional or an unauthorized manner.

Internet: A *system* of linked *computer* networks, international in scope, that facilitate *data* transmission and exchange, which all use the *standard Internet* protocol, TCP/IP, to communicate and share *data* with each other.

Internet E-mail (Electronic mail): While most organizations use an E-mail *system* on their internal network (e.g., cc mail, Banyan Beyond mail, etc.) the *Internet* uses its own mail protocol called Simple Mail Transport Protocol (*SMTP*). This allows everyone, no matter what type of E-mail *system* their organization is using internally, to exchange electronic messages with any other *Internet user*. Files can be attached to *Internet* e-mail messages and e-mail messages can be broadcast to many *Internet users*.

Intranet: An internal (i.e., non-public) network that uses the same technology and protocols as the *Internet*.

Intrusion Detection: The monitoring of network activities, primarily through automated measures, to detect, log and report upon actual or suspected unauthorized access and events for investigation and resolution.

Irrefutable Business Transaction: A business transaction of reproducible and provable *integrity* which can be proven to have taken place at a known and trusted date and time, to have been executed by its instigator and to have been received and/or accepted by its human or *system* recipient. See also *Non Repudiation*.

ISO: Information Security Officer.

Malicious Code: Malicious Code refers to code that is written intentionally to carry out annoying, harmful actions or use up the resources of a target *computer*. They sometime masquerade as useful software or are embedded into useful programs, so that users are induced into activating them. Types of malicious code include *Trojan horses* and computer *viruses*.

Media Access Control (MAC) address: A hardware address that uniquely identifies each node of a network.

MIME: Multipurpose *Internet* Mail Extension. The format for *Internet* mail that includes objects other than just text.

Multi-User System: Multi-user *system* refers to *computer systems* that support two or more simultaneous users. All mainframes, servers and minicomputers are multi-user systems, but most personal computers, laptops and workstations are not.

NNTP: The protocol, which delivers *USENET* news documents, via the *Internet*, to *USENET* news group servers, is called the NetNews Transport Protocol.

Non-public Information: Any *information* that is covered by an exception to the Freedom of Information Law or is otherwise protected from disclosure by law.

Non Repudiation: The *availability* of irrefutable proof of the provenance of, the content *integrity* of a transaction or of *data*, and the receipt and, optionally, the acceptance of, a transaction or of *data*, such that refutation of any of these is not possible. See also *Irrefutable Business Transaction*.

Owner of Information: An individual or organizational unit having responsibility for making *classification* and control decisions regarding use of *information*.

Penetration Testing: The portion of security testing in which evaluators attempt to exploit physical, network, *system* or application weaknesses to prove whether these weaknesses can be exploited by gaining extended, unauthorized or elevated privileged access to protected resources.

Personal Information: Personal information means any *information* concerning a natural person which, because of a distinct combination of name, number, personal mark or other identifier, can be definitively used to identify such natural person.

Physical Security: The protection of *information* processing equipment from damage, destruction or theft; *information* processing facilities from damage, destruction or unauthorized entry; and personnel from potentially harmful situations.

Principles: General, comprehensive, fundamental and durable statements or guidelines which underpin an architecture - relate to the role, use or direction of security in a business.

Privacy: The right of individuals and organizations to control the collection, storage, and dissemination of *information* about themselves.

Private Information: Private Information means *personal information* in combination with any one or more of the following *data* elements, when either the *personal information* or the *data* element is not encrypted or encrypted with an encryption key that has also been acquired:

- social security number; or
- driver's license number or non-driver identification card number; or
- account number, credit or debit card number, in combination with any required security code, access code, or password which would permit access to an individual's financial account

"Private information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

Privileged Account: The user-ID or account of an individual whose job responsibilities require special *system authorization*, such as a network administrator, security administrator, etc. Special *authorizations* are allocated to this account such as RACF Administrator, auditor, Special, UNIX root or Microsoft Administrator.

Procedures: Specific operational steps that individuals must take to achieve goals stated in this policy.

Programming Error: Introduction of a *programming error* either accidentally or maliciously.

Public Information: Information on *SE* programs and services, disseminated *information* through publications and through the news media.

Risk: The probability of suffering harm or loss. It refers to an action, event or a natural occurrence that could cause an undesirable outcome, resulting in a negative impact or consequence.

Risk Assessment: The process of identifying *threats* to *information* or *information systems*, determining the likelihood of occurrence of the *threat*, and identifying *system* vulnerabilities that could be exploited by the *threat*.

Risk Management: The process of taking actions to assess *risks* and avoid or reduce *risk* to acceptable levels.

SE: *State Entity* for the purpose of this policy, shall include all *state* agencies, departments, offices, divisions, boards, bureaus, commissions, educational entities (including but not limited to K-12, Higher Education Universities, and Tech Schools) and other entities

Security Administration: The actions and responsibility for administering the security mechanisms including identification and *authentication* establishment and *authorization* maintenance.

Security Management: The responsibility and actions required to manage the security environment including the security policies and mechanisms.

Security Policy: The set of criteria for the provision of security services based on global rules imposed for all *users*. These rules usually rely on a comparison of the *sensitivity* of the resources being accessed and the possession of corresponding attributes of *users*, a group of *users*, or entities acting on behalf of *users*.

Security Zone: An area or grouping within which a defined set of security policies and measures are applied to achieve a specific level of security. Zones are used to group together those entities with similar security requirements and levels of *risk* and ensure each zone is adequately segregated from another zone.

Sensitive Business Information: Disclosure or modification of this *data* would be in violation of law, or could harm an individual, business, or the reputation of the *SE*.

Sensitivity: The measurable, harmful impact resulting from disclosure, modification, or destruction of *information*.

SMTP-Simple Mail Transfer Protocol: A TCP/IP based protocol for the transmission of electronic mail. See definition for *Internet* e-mail.

Sniffing: Monitoring network traffic.

Social Engineering: Manipulation of people to obtain security *critical* assets that allow security perils to take place.

Spamming: Blindly posting something to a large number of groups.

Spoofing: Representing yourself as someone else.

Standard: Sets of rules for implementing policy. *Standards* make specific mention of technologies, methodologies, implementation *procedures* and other detail factors.

State: The State of South Carolina.

State Entity(ies): See *SE*.

System(s): An interconnected set of *information* resources under the same direct management control that shares common functionality. A *system* may include hardware, software, *information*, *data*, applications or communications infrastructure.

Teamroom: Technology or database *system* that allows specific group of individuals to develop and share *information* among themselves, such as documents or tools related to a specific project, or share *information* of common interest among the participants.

Technical Security Review: A technical security review would consist of reviewing the *controls* built into a *system* or application to ensure they still perform as designed and are in compliance with documented security policies and procedures. It would also include reviewing security patches to ensure they have been installed and are operational, reviewing security rules such as access control lists for currency, testing of *firewall* rules, etc. This type of testing includes intrusion and/or *penetration testing* of controls.

TELNET: The protocol, which allows *users* to use *Internet* services to remotely log onto a *computer* and run a program across the *Internet*. A TCP/IP based protocol used for remote terminal access to a server or network device. Telnet is inherently unsecured, being that all *data*, including username/password *authentication* are transmitted in clear-text.

Third Party: Any non-*SE* employees such as a contractor, vendor, consultant, intern, another *SE*, etc.

Threat: A force, organization or person, which seeks to gain access to, or compromise, *information*. A threat can be assessed in terms of the probability of an attack. Looking at the nature of the threat, its capability and resources, one can assess it, and then determine the likelihood of occurrence, as in *risk assessment*.

Trademark: A word, phrase, logo or other graphic symbol used by a manufacturer or seller to distinguish its product or products from those of others which is registered with the United States Patent and Trademark Office (*Black's Law Dictionary, 7th ed. 1999*).

Trojan Horse: Illegal code hidden in a legitimate program that when executed performs some unauthorized activity or function.

Unauthorized Access Or Privileges: Insider or outsider who gains access to network or *computer* resources without permission.

USENET News group: A USENET news group is a bulletin board where people can read or post Netnews messages on specific topics. There are many specialized business news groups. Many news groups are subscribed to by experts in the given topic and these individuals can provide valuable *information* and will sometimes respond to direct queries.

User: Any *state entity*(ies), federal government entity(ies), political subdivision(s), their employees or *third party* contractor(s) or business associates, or any other individual(s) who are authorized by such entities to access a *System* for a legitimate government purpose.

User of Information: An individual having specific limited authority from the *Owner of Information* to view, change, add to, disseminate or delete such *information*.

Virus: A program that replicates itself on *computer systems* by incorporating itself into other programs that are shared among *computer systems*. Once in the new *host*, a *virus* may damage *data* in the *host's* memory, display unwanted messages, crash the *host* or, in some cases, simply lie dormant until a specified event occurs (e.g., the birth date of a historical figure).

VPN: Virtual Private Network. *Internet* protocol (IP) virtual private networks (VPNs) are a collection of technologies that ensure the *privacy* of *data* over a shared unsecured IP network infrastructure. The two key points as to what constitutes an IP VPN are *privacy* and an IP network.

Vulnerability: A weakness of a *system* or facility holding *information* which can be exploited to gain access or violate *system integrity*. Vulnerability can be assessed in terms of the means by which the attack would be successful.

Vulnerability Scanning: The portion of security testing in which evaluators attempt to identify physical, network, *system* or application weaknesses to discover whether these weaknesses may be exploited by persons or machines seeking to gain either unauthorized or elevated privileged access to otherwise protected resources.

World Wide Web (WWW): A hypertext-based *system* designed to allow access to *information* in such a way that the *information* may physically reside on locally or geographically different servers. This access was greatly improved through the introduction of a graphical interface to the World Wide Web called a web browser. Netscape and *Internet Explorer* are two of the most popular web browsers.

Worm: A program similar to a *virus* that can consume large quantities of network bandwidth and spread from one network to another.