TABLE OF CONTENTS

1. TECHNICAL SECURITY 2

1.1. PURPOSE 2
1.2. BACKGROUND 2
1.3. POLICY 3
1.4. RESPONSIBILITIES 11

2. SOFTWARE AND DATA SECURITY 13

2.1. PURPOSE 13
2.2. BACKGROUND 13
2.3. POLICY 13
2.4. RESPONSIBILITIES 19

3. NETWORK AND COMMUNICATION SECURITY 21

3.1. PURPOSE 21
3.2. BACKGROUND 21
3.3. POLICY 21
3.4. RESPONSIBILITIES 32

4. APPENDIX A 34

4.1. ACRONYMS 34

5. APPENDIX B 35

5.1. GLOSSARY 35

6. APPENDIX C 46

6.1. REFERENCES 46

1. TECHNICAL SECURITY

1.1. PURPOSE

1.1.1. This chapter provides policy and guidance to implement technical controls that will reduce the exposure of computer equipment and assist in achieving an optimum level of protection for the State of Rhode Island information technology (IT) systems.

1.1.2. The policy contained in this chapter covers all the State IT resources maintained in-house or in the interest of the State. These policies are mandatory on all agencies, organizational units, employees, contractors, and others having access to and/or using the IT resources of the State.

1.1.3. This policy applies to all automated information systems currently in existence and any new automated technology acquired after the effective date of this policy document.

1.2. BACKGROUND

1.2.1. The issues that will be covered in this chapter under technical security are:

- Identification and Authentication
- Authorization/ Access Control
- Audit Trails

1.2.2. Identification and Authentication are critical building blocks of computer security since they are the basis for most types of access control and for establishing user accountability. Identification and Authentication are technical measures that prevent unauthorized people (or unauthorized processes) from entering an automated information system. Access control usually requires that the system be able to identify and differentiate among users. Access control is based on least privilege, which refers to the granting to users of only those accesses minimally required to perform their duties. User accountability requires the linking of

activities on a system to specific individuals and therefore, requires the system to identify users.

1.2.3. Access to the State's IT resources must be managed by a combination of technical and administrative controls. Uniform policy for access control across all the State's systems and networks is needed to support today's highly inter-connected environment and ensure that weaknesses at one agency do not place all the State information assets at unnecessary risk.

1.2.4. These controls will ensure that only authorized individuals gain access to information systems resources, that these individuals are assigned an appropriate level of privilege and that they are individually accountable for their actions. Access will be controlled and limited based on positive identification and authentication mechanisms.

1.3. POLICY

1.3.1. Identification is the means by which a user provides a claimed identity to the system. The most common form of identification is the user ID.

1.3.1.1. Unique Identification. Every State information system must ensure that users are uniquely identified before being allowed to perform any actions on the system.

1.3.1.2. Correlate Actions to Users. Each system must internally maintain the identity of all active users and be able to link actions to specific users.

1.3.1.3. Maintenance of User IDs:

- Offices and facilities must ensure that all user IDs belong to currently authorized users
- Identification data must be kept current by adding new users and deleting former users
- Inactive User IDs. User IDs that are inactive for 90 days must be disabled

1.3.2. Authentication is the means of establishing the *validity* of this claim. There are three means of authenticating a user's identity *which can be used alone or in combination*: something the individual knows (a secret –e.g., a password, Personal

Identification Number (PIN), or cryptographic key); something the individual *possesses* (a token – e.g., a bank's ATM card or a smart card); and something the individual *is* (a biometric – e.g., characteristics such as a voice pattern, handwriting dynamics, or a fingerprint).

1.3.2.1. Require Users to Authenticate. Users must authenticate their claimed identities on all IT resources.

1.3.2.2. Limit Log-on Attempts. The State IT Organizations must limit the number of log-on attempts to five (5). This helps to prevent guessing of authentication data. Where round-the-clock system administration service is available, system administrator intervention will be required to clear a locked account. Where round-the-clock system administration service is not available, accounts will remain locked out for at least ten (10) minutes.

1.3.2.3. Administer Data Properly. The State IT Organizations must have procedures to disable lost or stolen passwords and must monitor systems to look for stolen or shared accounts.

1.3.2.4. Passwords - Acceptable passwords must be carefully chosen by the user and enforced by the system. Controls must be implemented to require strong passwords.

1.3.2.5. Acceptable passwords must include each of the following characteristics:

- Letters - Upper or Lower Case Letters (A, B, C,.....Z, a, b,c,.....z)
- Westernized Arabic Numerals (0, 1, 2.....9)
- Non-alphanumeric "special characters." For example, punctuation or symbols. ([};"!$=)

1.3.2.6. At a minimum, user passwords must be at least **8** characters long.

- The password must not contain the user's e-mail name, user ID or the full name as shown in the domain registry.
- New passwords shall never be the same as any of the last 3 passwords.
- The password must not contain dictionary words from any language because numerous password-cracking programs exist that can run through millions of possible word combinations in seconds. Simply adding a

number onto the end of a word is not sufficient. The numeric and/or special characters should be integrated into the password. However, a complex password that cannot be broken is useless if you cannot remember it. For security to function, you must choose a password you can remember and yet is complex. For example, Msi5!Yold (My son is 5 years old) or IhliCf5#yN (I have lived in California for 5 years now).

- Passwords must be stored in irreversible encrypted form and the password file cannot be viewed in unencrypted form.
- A password must not be displayed on the data entry/display device.
- Operating systems, systems software, and other systems at high risk of compromise are sometimes installed with a standard set of default accounts and associated standard passwords. Like all accounts, these access routes must be protected by strong passwords. Additional measures, such as disabling, renaming, or decoying these standard accounts, will be employed.
- During the first instance of access with a new account, the initial password must be changed by the individual responsible for the account, in compliance with the password controls defined in this policy.
- The proper and secure use of passwords must be included in user training.

1.3.2.7. If system-supplied password generation is available, it must enforce the above requirements and also include the following additional features:

- The system will give the user a choice of alternative passwords from which to choose.
- Passwords will be reasonably resistant to brute-force password guessing attacks.
- The generated sequence of passwords will have the property of randomness (i.e., consecutive instances shall be uncorrelated and the sequences shall not display within a predictable time period).

1.3.3. **Access Control/Authorization**_- Access is the ability to perform a function with a computer resource (e.g., use, change, or view). Access controls are the system-based means by which the ability is explicitly enabled or restricted in some way. Access controls can prescribe not only who (a user) or what (a process) is to have access to a specific system resource, but also the level of access that is permitted.

1.3.3.1. The Division of Information Technology must establish a process to authorize and document access privileges based on a legitimate and demonstrated need to have system access.

1.3.3.2. Access privilege documentation must be maintained in a manner that makes it easily retrievable by individual user account.

1.3.3.3. Prior to initial account distribution, positive identification of individuals receiving accounts must be conducted. Positive physical identification can be done by anyone the system administrator can trust to perform this task. For example, if an employee needs access to a system located off-site, the employee's supervisor can make positive physical identification of the employee and request access via electronic mail. During the first instance of access with a new account, the initial password must be changed by the individual responsible for the account, in compliance with the password controls defined in this policy.

1.3.3.4. When system users are no longer part of an organization, or their duties change, their account access must be appropriately modified or terminated. Requests to change access privileges must be signed and forwarded to the appropriate designated individual by the responsible manager.

1.3.3.4.1. The default "Guest" account on servers and workstations will be disabled. Use of Guest-type accounts is strongly discouraged but, if needed, these accounts must conform to the naming conventions and the password policy established in this policy.

1.3.3.4.2. The State IT organization must control access to resources based on the following access criteria, as appropriate:

- *Identity* (user ID). The identity must be unique in order to support individual accountability.
- *Roles.* Access to information must also be controlled by the job assignment or function (i.e., the role) of the user who is seeking access.
- *Location.* Access to particular system resources will be based upon physical or logical location.

- Access would be denied for a sixth user, even if the user were otherwise authorized to use the application.
- *Access Modes.* The State IT Organizations will consider the types of access, or access modes. Common access modes, which can be used in both operating and application systems, include read, write, execute, and delete.

1.3.3.5. **Access Control Mechanisms:** The State IT Organization must implement both internal and external access control mechanisms. *Internal* access controls are a logical means of separating what defined users (or user groups) can or cannot do with system resources. *External* access controls are a means of controlling interactions between the system and outside people, systems, and services. When setting up access controls, the State IT organization shall incorporate the following mechanisms where appropriate and applicable:

- *Access Control Lists (ACLs).* ACLs are a register of users (including groups, machines, and processes) who have been given permission to use a particular system resource and the types of access they have been permitted. The State IT Organizations will maintain Access Control Lists and establish a procedure to identity and remove users who have left the organization or whose duties no longer require access to the application. Access Control Lists will be reviewed regularly.
- *Constrained User Interfaces.* The State IT Organizations will restrict access to specific functions by never allowing users to request information, functions, or other resources for which they do not have access.
- *Encryption.* Encrypted information can only be decrypted, and therefore read, by those possessing the appropriate cryptographic key. While encryption can provide strong access control, it is accompanied by the need for strong key management. Encryption will be utilized where appropriate and required.
- *Port Protection Devices.* Fitted to a communications port of a host computer, a port protection device (PPD) authorizes access to the port itself, often based on a separate authentication (such as a dial-back modem) independent of the computer's own access control functions.

- *Secure Gateways/Firewalls.* Secure gateways block or filter access between two networks (e.g. Intranet, Internet, State partners, contractors, vendors, and other state agencies). Secure gateways allow internal users to connect to external networks while protecting internal systems from compromise. Additional information and requirements regarding gateways and firewalls are contained in the "Network" Chapter of this Handbook and on the State's Information Security web site.
- *Host-Based Authentication.* Host-based authentication grants access based upon the identity of the host originating the request, instead of the identity of the user making the request. The State IT Organization shall use network applications utilizing host-based authentication where appropriate and required.
- *System Log-On Banner.* A security log on banner shall be incorporated on all networked systems. This is displayed to users as part of the log on dialogue, followed by a pause requiring manual intervention to continue. The State Log-on banner displayed each time a user logs on to the State Log-on Banner is a reminder that any use of the State information technology resources is made with the understanding that such use is generally not secure, is not private, and is not anonymous.

WELCOME TO THE DEPARTMENT of ADMINISTRATION

This is a State of Rhode Island system operated and maintained by the Department Of Administration, Division of Information Technology. We encourage you, as a Department employee, researcher, contractor, or member of the public, to use this system. You should not expect privacy while using this system and your activity may be monitored to protect the system from unauthorized use. Authorized employees have the right to examine active and stored email and files within all systems. By using this system you expressly consent to such monitoring and to reporting your unauthorized use to the proper authorities. Unauthorized use of this system and/or unauthorized access may be prosecuted to the full extent of the law.

1.3.4. ***Audit Trails*** - Audit trails maintain a record of system activity by system or application processes and by user activity. In conjunction with appropriate tools and procedures, audit trails provide a means to help accomplish several security-

related objectives, including individual accountability, reconstruction of events, intrusion detection, and problem identification.

1.3.4.1. The State IT Organization audit trails will be used for the following:

- Individual Accountability. The audit trail supports accountability by providing a trace of user actions. While users cannot be prevented from using resources to which they have legitimate access authorization, audit trail analysis can be used to examine their actions.
- Reconstruction of Events. The Department will use audit trails to support after-the fact investigations of how, when, and why normal operations ceased.
- Intrusion Detection/Prevention. The State IT Organization will design and implement their audit trails to record appropriate information to assist in intrusion detection. Intrusions can be detected in real time, by examining audit trails as they are created or after the fact, by examining audit records in a batch process.
- Problem Identification. The State IT Organization will use audit trails as online tools to help identify problems other than intrusions as they occur. This is often referred to as real-time auditing or monitoring.
- The CISO must be notified of all investigative audits of IT resources.

1.3.4.2. **Contents of Audit Trail Records:** An audit trail must include sufficient information to establish what event occurred and who (or what) caused them. The scope and contents of the audit trail will balance security needs with performance needs, privacy, and costs. At a minimum the event record must specify:

- Type of event
- When the event occurred (time and day)
- User ID associated with the event
- Program or command used to initiate the event

1.3.4.3. **Audit Trail Security:** The State IT Organization will protect the audit trail from unauthorized access. The following precautions will be taken:

- Control online audit logs. Access to online audit logs will be strictly controlled.
- Separation of duties. The State IT Organizations will ensure separation of duties between security personnel who administer the access control function and those who administer the audit trail.
- Protect confidentiality. The State offices and facilities will ensure the confidentiality of audit trail information.

1.3.4.4. Audit Trail Reviews. Audit trails will be maintained, at a minimum, for six months. The following must be considered when reviewing audit trails:

- Recognize normal activity. Reviewers must know what to look for to be effective in identifying unusual activity. They need to understand what normal activity looks like.
- Utilize a search capability. Audit trail review can be easier if the audit trail function can be queried by user ID, device ID, application name, date and time, or some other set of parameters to run reports of selected information.
- Follow-up reviews. The appropriate system administrator will review the audit trails following a known system or application software problem, a known violation of existing requirements by a user, or some unexplained system or user problem.
- Develop review guidelines. Application owners, data owners, system administrators, and the CISO will determine how much review of audit trail records is necessary, based on the importance of identifying unauthorized activities.

1.3.4.5. Automated tools. Traditionally, audit trails are analyzed in a batch mode at regular intervals (e.g., daily). Audit analysis tools, such as those based on audit reduction, attack signature, and variance techniques, can be utilized in real-time or near real-time fashion. the State IT Organizations should use the many types of tools that have been developed to help reduce the amount of information contained in audit trails, as well as to distill useful information from the raw data.

1.3.4.6. All the State information systems must have the ability to audit password activity, specifically when and who last changed a password, and when and who last changed account privileges.

1.3.4.7. Annually, individual accounts must be audited to ensure compliance with the minimum standards outlined in this policy.

1.3.5. The State IT systems that cannot meet these minimum standards must be modified to remedy any deficiencies. Until such time as deficient systems are brought up to these security standards, system owners, as part of their DOIT mandated security plans and risk assessments, must accept in writing any risk to the State infrastructure.

1.4. RESPONSIBILITIES

1.4.1. **The State CIO:** Ensures that the provisions of this chapter are implemented at all agencies within the State.

1.4.2. **Agency Directors:** Ensure that adequate technical security controls are implemented on all systems for which they hold responsibility.

1.4.3. **The Agency Manager:**

1.4.3.1. Certifies the systems under their control. The technical controls must be in place and functioning as intended, prior to certification of the system.

1.4.3.2. Ensures that during the development and acquisition phase of developing local systems that security requirements and specifications are incorporated into any purchase of automated information systems.

1.4.4. **System administrators**:

1.4.4.1. Ensures that the technical controls are functioning as expected and report any significant discrepancies noted to the CISO.

1.4.4.2. Monitors the system by reviewing system logs and utilizing various automated tools such as virus scanners, check-summing, password crackers, integrity verification programs, intrusion detectors, and system performance monitoring.

1.4.4.3. Evaluates account and password management controls yearly to ensure that the State password policy is being technically implemented.

1.4.4.4. Ensures that the CISO is notified of all investigative audits of IT systems.

1.4.5. **CISO/ACISO**:

1.4.5.1. Assists the State CIO in performing sensitivity assessments and in determining security requirements and specifications for technical controls in any new systems to be purchased and operated at the facility.

1.4.5.2. Audits the technical controls. This can be accomplished by conducting regular audits of the system. The CISO must work with the system manager and the State CIO in developing effective measures to audit the various systems in a facility.

1.4.5.3. Develops procedures and policy concerning authorizing and documenting access privileges for users based on a legitimate and demonstrated need to have system access.

1.4.6. **Individual users:** Select strong passwords in accordance with this policy.

2. SOFTWARE AND DATA SECURITY

2.1. PURPOSE

2.1.1. This chapter provides security guidance on software selection, development, testing, implementation and maintenance of State of Rhode Island software.

2.1.2. Security controls for operating system and application software are detailed below and are applicable to all software (the State developed and Commercial Off-The-Shelf (COTS)) used in the State IT resources.

2.2. BACKGROUND

2.2.1. The State currently buys COTS software. Security controls must be met in these circumstances to ensure that mission critical and all other sensitive data is established, maintained, transported and utilized in a secure manner.

2.3. POLICY

2.3.1. General Software Security Elements are:

2.3.1.1. Controlling what software is used on a system

- All COTS application software purchases must be certified and accredited prior to use.
- Application software used on the State IT resources must be obtained through authorized procurement channels.
- Each system installation of the State developed or off-the-shelf software must be reviewed and approved by the review board prior to installation. This also includes software acquired by any other means (e.g., public domain software, bulletin board services, personally owned software, Internet obtainable freeware). All application software authorized to run on the State IT resource must be identified in the system's security plan.

2.3.1.2. Ensuring that software has not been modified without proper authorization

- Willful and intentional modification of the State software for illegal or disruptive purposes or for personal gain is a crime. There must not be any modifications of these programs except by an authorized agent of the CIO.
- Safeguards must be in place to detect and minimize inadvertent or malicious modification or destruction, or attempts to do so, of the State's IT application software, operating system software, and critical data files.
- The safeguards should achieve the integrity objectives and be documented in the system's security plan. The level of protection must be commensurate with the sensitivity of the information processed.
- Approved software, regardless of source, must be scanned for viruses prior to initial use.
- Anti-Virus and malicious code (software) must be employed on every the State IT resource to protect the integrity of the software and data.

2.3.1.3. Ensuring that software is properly licensed, as required

- Use of copyrighted software will comply with copyright laws and license agreements.
- The State licensed software may not be installed on other systems without management approval (e.g. anti-virus software).

2.3.2. **Operating System Software Controls**: The operating system software employed to process data by multiple users, including local area networks, must control user access to resources and capabilities that are required and authorized. The operating system software should also have the capability to identify, journal, report, and assign accountability for the functions performed or attempted by a user and to deny user access to capabilities or resources that have not been authorized. At a minimum, the operating system must:

2.3.2.1. Control all transfers between memory and on-line storage devices between a central computer and remote devices and between on-line storage devices.

2.3.2.2. Control all operations associated with allocating system resources (e.g. memory, peripheral devices, etc.), memory protection, system interrupts and changes between the privileged and non-privileged states.

2.3.2.3. Identify a valid system user and direct the user to authorized options or applications. Use of such a feature (log-on dialogue) limits user access and protects system programs and data files from unauthorized access.

2.3.2.4. Provide the capability to limit the types of operations (e.g., read, write, and delete) that can be performed by individual users on given data or program files.

2.3.2.5. Control system access through an approved form of user authentication.

2.3.2.6. Provide the capability to record actual or attempted access to the system and other activity.

2.3.2.7. Provide the capability to terminate a process automatically and log-off a user when an access session remains inactive for some specified length of time.

2.3.2.8. Provide the capability upon a break of connection or a log-off to terminate an access session.

2.3.2.9. Control programs or utilities which may be used to maintain and/or modify the operating system, access control systems, sensitive databases and other software modules which could affect or compromise the integrity of the general purpose software or sensitive applications.

2.3.2.10. Prevent a user program from executing privileged instructions.

2.3.2.11. Isolate the programs and data areas of one user from those of other users and the operating system software.

2.3.2.12. Assure error detection when accessing memory as well as parity and hardware register checking.

2.3.2.13. Cause a screen warning message to be displayed at logon to identify to the user that access is restricted to authorized users for legitimate purposes only and that their activities are subject to monitoring.

2.3.2.14. Be maintained by the minimum number of authorized persons. This is accomplished by limiting the number of employees with administrative privileges.

2.3.2.15. Be copied after each modification with the copy to be immediately stored as a backup for emergency use.

2.3.3. **Application Software Controls:** An application that processes sensitive data, or requires protections because of the risk and magnitude of loss or harm that could result from improper operation, manipulation or disclosure must be provided protection appropriate to its sensitivity. The following will be considered as the minimum controls to be applied to sensitive applications, with additional controls or safeguards to be imposed if appropriate:

2.3.3.1. The State approved security requirements and specifications will be defined prior to acquiring or starting development of applications, or prior to making a substantial change to the existing application.

2.3.3.2. Design reviews will be conducted at periodic intervals during the developmental process to assure that the proposed design will satisfy the functional and security requirements specified.

2.3.3.3. New or substantially modified sensitive applications must be thoroughly tested prior to implementation to verify that the user functions and the required administrative, technical, and physical safeguards are present and are operationally adequate. This is to be accomplished as part of the certification and accreditation process.

2.3.3.4. Sensitive data or files will not be used to test applications software until software integrity has been reasonably assured by testing with non-sensitive data or files.

2.3.3.5. Sensitive application software will not be placed in a production status until the system tests have been successfully completed and the application has been properly certified and accredited. Prototypes that process production data must be certified and accredited before they are deployed or implemented.

2.3.3.6. Current backup copies of critical application software, documentation, data bases and other resources required for its operation, will be maintained and be readily available for use in the event of an emergency.

2.3.3.7. Sensitive applications will be re-certified every three years or following major changes.

2.3.3.8. Sensitive software documentation must be provided the same degree of protection as that provided for the software.

2.3.4. **Software Security Implementation Procedures**. Software designed to provide information security is limited by the effectiveness of the procedures implemented to support it. Procedural issues, which relate to the use of the system software and which should be addressed, are as follows:

2.3.4.1. A minimum length of eight characters is required for passwords. The minimum length will be software controlled.

2.3.4.2. Default User Accounts. Operating systems are sometimes installed with a standard set of default user accounts and associated standard security passwords. The access route shall be protected by either disabling the standard user account or by changing the passwords.

2.3.4.3. All security problem fix software, patches, command scripts, and the like provided by vendors, official computer emergency response teams (CERTs), and other trusted third parties must be promptly installed and documented.

2.3.5. **Processing Environments:** The State automated information systems use several processing environments that meet the specific and varied needs of users. Following are descriptions of processing environments and the unique information security aspects related to them:

2.3.5.1. Production environment is the environment for the processing of official data utilized in support of office and facility missions and management. Information security procedures for production environments must specifically address controls for:

- Viewing, modifying, downloading or deleting production system data and programs
- Generation and disposition of outputs
- Tracking production program version changes (maintenance of a software update history log is required under configuration

management discussed in Chapter 4 of the State Operational Controls Handbook)

- Access to the computer and its peripheral devices

2.3.5.2. Development and Verification is the environment for the development, testing, and verification of program code for the maintenance, modification or enhancement of existing applications, or the development of new applications. Information security procedures for this environment must specifically address controls for:

- Viewing, modifying, or deleting test data
- Creating, viewing, modifying, or deleting development programs
- Generation and disposition of outputs
- Transfer of application programs and data files from the development and verification environment to the production environment
- The computer system and its peripheral and telecommunication devices

2.3.5.3. Demonstration and/or Training enables use of system or application software functions in an on-line mode (using production or development computer resources) without affecting the production or development environments. The demonstration and/or training environment must simulate on a demonstration or training disk, the production environment and use non-sensitive data to test, train, or demonstrate the system. Information security procedures for this environment must specifically address:

- Protecting production and development system programs and data files
- Accessing the "Demonstration" account by the general public (other than the State staff)
- Limiting user access to only those capabilities necessary to utilize the demonstration programs
- Limiting access to the computer and its peripheral and communications devices
- Generic access codes may be used to enter the "Demonstration" environment and is the only exception to the mandated requirement for individual password codes

2.4. RESPONSIBILITIES

2.4.1. **State Software Developers**:

2.4.1.1. Ensure that security controls are incorporated in the design, development, and testing of contractor-developed software.

2.4.1.2. Ensure that the State developed application software and patches are certified prior to release to the State.

2.4.2. **State CIO, Technical Services, or designee**:

2.4.2.1. Accredit all the State software and patches prior to release to the State

2.4.2.2. Ensure that all the State IT Organizations are in compliance with the policy outlined in this chapter.

2.4.3. **Office Heads, and Facility Directors:** Ensure that adequate application security controls on locally purchased application software are implemented at their sites.

2.4.4. **Agency Manager**:

2.4.4.1. Ensures that the operating system and application software security controls on all software used throughout the State meet the agency requirements.

2.4.4.2. Ensures that any COTS applications purchased by offices and regional facilities meet the State security controls.

2.4.5. **System administrators**:

2.4.5.1. Maintain the software utilized on their systems.

2.4.5.2. Ensure that the operating system and application software controls are operating as intended on the systems under their responsibility.

2.4.5.3. Install all problem fix software, patches, command strips on appropriate systems in a timely manner.

2.4.6. **CISO/ACISO**:

2.4.6.1. Ensure that locally procured software has been approved by the review board and certified and accredited by the office head or facility director.

2.4.6.2. Audit to ensure that software (application and operating system) controls are in place and functioning as designed.

3. NETWORK AND COMMUNICATION SECURITY

3.1. PURPOSE

3.1.1. This chapter provides guidance and policy related to network and communication security for the State sites. Independent Internet gateways, electronic mail, facsimile (fax) transmissions, local areas networks (LANs), and wide area networks (WANs) need security controls established to ensure the confidentiality, integrity, and availability of the data being transmitted.

3.1.2. The policy contained in this chapter covers all the State IT resources maintained in-house or in the interest of the State. These policies are mandatory on all organizational units, employees, contractors, and others having access to and/or using the IT resources of the State.

3.1.3. This policy applies to all the State automated information systems processing sensitive data currently in existence and any new automated technology acquired after the effective date of this policy document.

3.2. BACKGROUND

3.2.1. Network security is not any different from single host security in terms of confidentiality, integrity, and availability of resources. The real difference in providing basic security services occurs because of the increased complexity of the networked environment. Providing confidentiality of information, for example, is difficult enough when the entire system resides in a single room. Consider the implications of allowing access to information from multiple locations both inside and outside of the State. Security for a single host is generally the responsibility of a single individual. In a networked environment, the security of individual systems is the responsibility of numerous individuals. Intruders to networks continually count on finding a single weak link in the network chain that will then allow them access to the rest of the network. Network security measures must account for this, as well as other complexities, in an attempt to maintain the security of the network data and resources.

3.3. POLICY

3.3.1. **General Network Policy**

The State IT safeguards must ensure the privacy of sensitive information during storage, processing, and transmission.

3.3.1.1. The State users will be granted access to the State networks based upon duty requirements and the need to access resources.

3.3.1.2. The State IT Organizations will implement the necessary mechanisms and procedures to protect information processed on networks, to include:

- Maintaining a record of authorized users of a network and their network privileges and reviewing this record on a regular basis to ensure that access to the network is limited to only those individuals with a justified need.
- Ensuring that all networks are certified and accredited. (See Management Controls Handbook for details)
- Ensuring that computer systems are configured to terminate a user process if that user-network connectivity is interrupted before a proper log out.
- Ensuring that the network and systems automatically terminate sessions after periods of inactivity.
- Establishing individual accounts for each user on the network. "Generic accounts" that allow users access to network resources anonymously, are prohibited.
- Establishing formal reporting procedures for unexpected events and activity.

3.3.2. **External Connections.** An external connection is any connection (not just an Internet connection) from an outside network (a source other than the State) that is electronically linked to a system or network that is owned or operated by or in behalf of the State.

3.3.2.1. External connections must incorporate adequate controls to safeguard the State IT resources.

3.3.2.2. At a minimum, all external connections must incorporate a firewall. Network firewalls are devices used to protect a trusted computer network from an untrusted one.

3.3.2.3. The State policy has established the following as the minimum specifications for a firewall:

3.3.2.3.1. Configuration and Installation:

- Activate the minimum set of operating system services to support firewall operation. Activate no other operating system services.
- Configure the firewall computer's operating system with all current patches and updates to known exploits.
- Support high availability configurations and load balancing through integrated capabilities or by integration of third party products.
- Configure the firewall so that it cannot be identifiable as such to other network(s), or, at most, appears to be just another router.
- Disguise or hide internal Domain Name Systems (DNS) to prevent direct external requests.
- Ignore service requests like "echo" or "chargen" that could be used in a denial of service attack.
- Prevent network connections from bypassing the firewall.
- Be installed in locations that are physically secure from tampering.

3.3.2.3.2. Access Management:

- Restrict use of a particular application only to customers authorized to access the application.
- Implement a "deny all services except those specifically permitted" design policy.
- Implement two-factor authentication for administrative log-in to permit secure remote log-in by the authorized system administrator.
- Support integration of external authentication databases, such as RADIUS or LDAP.
- Employ techniques such as content filtering to permit or deny services to specific external hosts, such as web sites that the State staffs are restricted from accessing.

- Incorporate and operate a systematic method of intrusion detection/prevention. Data from intrusion detection/prevension must be stored such that it can serve as evidence in forensic investigations.

3.3.2.3.3. Auditing and Filtering

- Log access to and through the firewall.
- Capture log-in attempts by authorized and unauthorized users.
- Employ a flexible, user-friendly IP-filtering language that is easy to program and can filter on a wide variety of attributes, including source and destination IP addresses, protocol types, port numbers, and inbound and outbound interfaces.
- Screen data coming through the firewall.
- Concentrate, filter, and log dial-in and VPN access.
- Generate an audit trail of calls passing through the firewall for review of security anomalies at future times.
- Support third-party products for log analysis and data reduction. **Notification**

3.3.2.4. Provide notification of threats, including unsolicited distribution of executable files, and notification of efforts by accepted users to gain access to systems or applications that they do not have permission to enter.

3.3.2.5. Generate alarms, predicated on the occurrence of a specific event or combination of events, on a timely basis (e.g., within 60 seconds) after the event occurs.

3.3.3. **Future Security Enhancements**

3.3.3.1. Accommodate new services and needs to allow for changes in the State and the State security policy.

3.3.3.2. Contain advanced authentication measures, or the hooks for installing advanced authentication measures, if strong authentication for inbound access is required.

3.3.3.3. External connections must be accredited prior to use.

3.3.3.4. External connections will be periodically independently reviewed by an organization other than that which sponsors the use and administration of the external connection. These reviews will be conducted when there is significant change to the protected asset, or at least every other year after initial accreditation. These reviews will ensure that external connections remain in compliance with the minimum security standards outlined in this policy, and will ensure that risk assessments, security plans, and contingency plans remain current.

3.3.3.5. Where user access originates from outside the internal the State protected network, all users must be identified and authenticated at the gateway prior to being granted access to internal resources.

3.3.3.6. Where sensitive data is to be accessed from or through untrusted networks, the entire session must be encrypted.

3.3.4. **Internet/Public Access**

3.3.4.1. There are several methods available for connecting to the Internet system. They include, but are not limited to purchasing a commercial service, establishing an independent gateway or connecting through the State Internet Gateways.

3.3.4.2. The Division of IT (DOIT) Internet Gateway has been established as a common resource for all the State IT Organizations to use. The DOIT Internet Gateway is provided to support information sharing, research, and education in and among the State IT Organizations, research and instructional institutions, and other government agencies and commercial services. Use of the DOIT Internet Gateway is mandatory.

3.3.4.3. Those sites with their own connection to the Internet or to other networks external to the State (i.e., universities, vendors, other state government agencies) must meet all of the security requirements established by the DOIT

3.3.4.4. The State must approve external connections prior to operation.

3.3.4.5. The State employees are expected to conduct themselves professionally in the workplace and must not use the Internet for activities that are inappropriate or offensive to co-workers or the public. Such activities include

playing electronic games, or accessing sexually explicit materials or materials that ridicule others on the basis of race, creed, religion, color, sex, disability, national origin or sexual orientation.

3.3.4.6. Employees must ensure that all sites accessed have no cost attached. For example, a prompt to enter a special password or to register prior to entering the database may indicate that it is fee-based.

3.3.4.7. Government-issued credit cards must not be used for personal access to the Internet, or to purchase items from the Internet for personal use.

3.3.4.8. Employees must not use dial-out modems to connect to commercial Internet service providers, such as America Online. If exceptions are required, approval must be obtained from senior management.

3.3.4.9. Employees using the State resources to access the Internet are subject to monitoring. Incidents of inappropriate access will be reported to supervisors and the CISO for disciplinary action.

3.3.4.10. All software and files downloaded from non-the State sources via the Internet (or any other public network) must be screened with virus detection software. The screening must take place prior to being run or examined via another program such as a word processing package.

3.3.4.11. All public access systems will be located outside the internal the State network.

3.3.4.12. Systems that are exposed to the Internet, such as the State public access systems, will not be permitted direct access to the internal the State network.

3.3.5. **Modem communications**

3.3.5.1. Data communication connections via modems are to be limited and tightly controlled as they pose a serious risk that can circumvent security controls intended to protect the State networks from external, "untrusted" networks.

3.3.5.2. Employees are prohibited from connecting dial-up modems to the State workstations that are simultaneously connected to the State network or another internal communication network.

3.3.5.3. Remote users (telecommuters and employees on travel) dialing into the State systems must be routed through a modem pool that includes an approved extended user authentication security system.

3.3.5.4. Reliable and confidential hardware and software authentication systems are to be incorporated into the State approved communication servers. Positive authentication is to be established prior to granting access to network resources.

3.3.5.5. Event logging functions are to be provided to enable a review of suspicious activities.

3.3.5.6. Controls are required for remote access to the State systems. A log will be maintained and reviewed quarterly of individuals granted remote access to ensure that accountability is maintained.

3.3.6. **Electronic Mail** (email)

3.3.6.1. Only authorized email software may be used.

3.3.6.2. The State employees who utilize email systems will do so with the understanding that they have no expectation of personal privacy relating to that use.

3.3.6.3. When appropriately authorized by management, electronic mail messages flowing through the State systems may be monitored for internal policy compliance, suspected criminal activity, and other systems management reasons.

3.3.6.4. The State users are prohibited from sending or forwarding any messages via the State's information systems that a reasonable person would consider to be defamatory, harassing, or explicitly sexual. Employees are also prohibited from sending or forwarding messages or images via the State systems that would be likely to offend on the basis of race, gender, national origin, sexual orientation, religion, political beliefs, or disability.

3.3.6.5. When employees receive unwanted and unsolicited e-mail (also known as SPAM), they must refrain from responding directly to the sender. Instead, forward the message to the email administrator who will take steps to prevent further transmission.

3.3.6.6. The State projects and commercial products for secure electronic mail (email) systems are undergoing rapid development and will be available in the near future. Until such products are implemented, users must not send sensitive information via email.

3.3.6.7. The State system administrators establish and maintain a systematic process for the retention and destruction of electronic mail messages and accompanying logs.

3.3.6.8. Users must regularly move important information from electronic mail message files to word processing documents, databases, and other files. Electronic mail systems are not intended for the archival storage of important information. Stored electronic mail messages are periodically expunged by system administrators, mistakenly erased by users, and otherwise lost when system problems occur.

3.3.7. **Telecommuting Security**

3.3.7.1. The security of the State property at an alternative work site (i.e., home, hotel, etc.) is just as important as it is at the State IT Organization. At alternative work sites, reasonable precautions must be taken to protect the State hardware, software, and information from theft, damage, and misuse.

3.3.7.2. Users must not discard sensitive information at home, in hotel wastebaskets or other publicly accessible trash containers. Instead, sensitive information must be retained until it can be shredded, or destroyed by other approved methods.

3.3.7.3. Telecommuters must ensure that the systems they utilize remotely maintain the current anti-virus software.

3.3.7.4. Remote users should not maintain sensitive data on their systems unless adequately secured via encryption or authenticated access control mechanisms. This is especially important if the system is also used to connect to the Internet.

3.3.7.5. Telecommuters must use the password facility in their screen saver.

3.3.7.6. Only authorized telecommuters will be given access to the State's networks. Managers must take steps to ensure that telecommuting employees do not compromise the integrity of the State systems.

3.3.7.7. Telecommuters must be authenticated prior to access to the State's network. Where possible, user access should be limited to specific systems specified during the log-in process.

3.3.7.8. Sensitive data should not be transmitted unless appropriately secured via encryption.

3.3.7.9. Employees are responsible for the integrity and confidentiality of the data on remote systems. Access controls must be in place to protect the State systems and electronic information located at remote sites (i.e., home, telecommuting work locations, hotels and convention centers).

3.3.8. **Facsimile (fax) transmission**

3.3.8.1. Sensitive information will only be transmitted via a secure facsimile system (e.g., encrypted or via a protected network). Commercial-off-the-shelf (COTS) software and hardware are available to provide the necessary safeguards and should be employed as appropriate.

3.3.8.2. Each office and facility should develop policies and procedures to protect privacy while transmitting information via facsimile. The policy and procedures must:

- Limit use to urgent situations
- Ensure appropriate location of facsimile machines

- Assign accountability for managing each facsimile machine
- Define appropriate safeguards to ensure transmissions are sent to the appropriate individual
- Define procedures for cases of misdirected transmissions and receipts
- Routine disclosure of information should be made through regular mail or courier
- Auto-faxing, which allows automatic facsimile transmission of reports, should be set up carefully to ensure that they are necessary and that correct facsimile numbers are contained in the system
- A cover letter should accompany each transmission and include:
  - Date/time transmission
  - Sending facility's name, address, telephone and facsimile numbers
  - Authorized receiver's name
  - Number of pages transmitted
  - Confidentiality notice, including instructions on re-disclosure and destruction

3.3.8.3. A procedure must be developed to cover instances when a site is notified that a fax was received by other than the intended recipient. The internal logging system of the facsimile machine should be checked to obtain the number to which the transmission was sent in error. If the number was incorrect a facsimile should be sent to that number explaining that the information was misdirected and ask for the documents to be returned by mail to the sending facility.

3.3.8.4. A procedure must be developed regarding the receipt of facsimile documents containing sensitive information. The procedure should address the following areas:

- Accountability for monitoring the facsimile machine. A fax machine must be located in a secure, controlled area.
- Ensuring the removal of documents promptly
- Checking for completeness and legibility of received information

- Notifying senders of transmission problems
- Following the instructions on the cover page
- Arranging for secure delivery of the documents

3.3.9. **PBX (Telephone) Security**

3.3.9.1. Keep PBX attendant console rooms, telephone wiring closets, telephone equipment rooms, and Local Exchange Company (LEC) demarcation rooms locked and secured. These rooms shall meet the same physical security requirements as outlined in the State's Operations Handbook, Chapter 5 "Physical/Environmental Security."

3.3.9.2. Request positive identification from all service equipment vendors and technicians.

3.3.9.3. Ensure that any remote maintenance line phone number is unpublished, preferably not in the same numbers groups, and not recorded on jacks, wall field, distribution frame, etc.

3.3.9.4. Secure any reports, documentation, or other information files that may reveal the trunk access codes or passwords.

3.3.9.5. Change all default passwords immediately after installation.

3.3.9.6. Choose passwords that meet the requirements as outlined in Chapter 1 "Technical Security" of this Handbook.

3.3.9.7. Deactivate unused codes and features.

3.3.9.8. Allow only three attempts to enter a valid access code.

3.3.9.9. Have the PBX wait four or five rings before answering the remote access line.

3.3.9.10. Restrict calling privileges to individual employees

3.3.9.11. Block area codes where business is not done, especially 900, 700, and 976.

3.3.9.12. Use the maximum authorization and Remote Access barrier code length.

3.3.9.13. Use security devices on all ports.

3.3.9.14. Ensure that all unused ports are disconnected from the system.

3.3.10. **Voice Mail**

3.3.10.1. Don't allow outgoing calls from a mailbox.

3.3.10.2. Block access to long distance trunks or local lines.

3.3.10.3. Toll restrict lines between the voice mail system and PBX.

3.3.10.4. Delete all unused voice mailboxes.

3.4. RESPONSIBILITIES

3.4.1. **The State CIO** Ensures that all IT systems in the State Government are in compliance with the technical policy outlined in this chapter.

3.4.2. **Department Directors**:

3.4.2.1. Ensure that the security technical controls are established on all the systems at their departments.

3.4.2.2. Accredit all systems implementing external connections initiated from the site to non-the Department sources.

3.4.2.3. Prior to implementation, ensure that the review board has approved all external connections initiating from the site that connects the State's network with an external non-State network.

3.4.3. **Agency Managers**:

3.4.3.1. Ensures that the security technical controls outlined in this chapter are implemented on the State IT resources.

3.4.3.2. Ensures that all systems implementing external connections from the site to non-the State sources are secure and certified.

3.4.3.3. Ensures that all external connections from the State's network to non-the State networks meet the State security criteria and receive final approved of the review board prior to accreditation by the CIO.

3.4.3.4. Ensures that all systems implementing external connections from the site to non-the State sources are accredited prior to operation.

3.4.3.5. Ensures that all external connections are re-certified and accredited every other year after initial accreditation.

3.4.3.6. Ensures that all dial-up modems are justified and approved prior to use.

3.4.4. **CISO/ACISO**:

3.4.4.1. Maintains a record of authorized users of a network and their network privileges. This may be delegated to the review board if appropriate.

3.4.4.2. Reviews this record on a regular basis to ensure that access to the network is limited to only those individuals with a justified need.

3.4.4.3. Work with the system administrators and the CIO to ensure that all systems are certified and accredited.

3.4.4.4. Conducts audits to ensure that technical controls are implemented and performing as required.

4. APPENDIX A

4.1. ACRONYMS

ACL	Access Control List
ACISO	Alternate Chief Information Security Officer
CIO	Chief Information Officer
CISO	Chief Information Security Officer
COTS	Commercial Off-The- Shelf
DOD	Department of Defense
DNS	Domain Name Systems
EMAIL	Electronic Mail
FAX	Facsimile
IP	Internet Protocol
IRS	Internal Revenue Service
ISO	Information Security Officer
IT	Information Technology
LAN	Local Area Network
LEC	Local Exchange Company
PBX	Private Branch Exchange
PIN	Personal Identification Number
PPD	Port Protection Device
SAM	Security Account Manager
SSA	Social Security Administration
WAN	Wide Area Network

5. APPENDIX B

5.1. GLOSSARY

Access Control	Security control designed to permit authorized access to an IT system or application.
Accreditation	A formal declaration by the Agency Manager that the IT is approved to operate in a particular security mode using a prescribed set of safeguards. Accreditation is the official management authorization for operation of IT and is based on the certification process, as well as other management considerations. The accreditation statement affixes security responsibility with the Agency Manager and shows that due care has been taken for security.
Authentication	Verification of the identity of a user, user device, or other entity, or the integrity of data stored, transmitted, or otherwise exposed to unauthorized modification in an IT.
Audit Trail	A record showing who has accessed a computer system and what operations he or she has performed during a given period of time. Audit trails are useful both for maintaining security and for recovering lost transactions.
Automated Information System(s) (AIS)	An assembly of computer hardware, software and/or firmware configured to collect, create, communicate, compute, disseminate, process, store, and/or control data or information.
Availability of Data	The state when data are in the place needed by the user, at the time the user needs them, and in the form needed by the user.
Backup	A copy of data and/or applications contained in the IT stored on magnetic media outside of the IT to be used in the event IT data are lost.
Certification	The comprehensive evaluation of the technical and non-

	technical security features of an IT and other safeguards, made in support of the accreditation process that establishes the extent to which a particular design and implementation meet a specified set of security requirements.
Ciphertext	Form of cryptography in which the *plaintext* is made unintelligible to anyone, who intercepts it by a transformation of the information itself, based on some key.
Confidentiality	The concept of holding sensitive data in confidence limited to an appropriate set of individuals or organizations.
Configuration Management	The process of keeping track of changes to the system, if needed, approving them.
Contingency Plan	A plan for emergency response, backup operations, and post-disaster recovery maintained by an activity as a part of its security program that will ensure the availability of critical resources and facilitate the continuity of operations in an emergency situation.
COTS Software	Commercial Off The Shelf Software – software acquired by government contract through a commercial vendor. This software is a standard product, not developed by a vendor for a particular government project.
Data Integrity	The state that exists when automated data is the same as that in source documents, or has been correctly computed from source data, and has not been exposed to alteration or destruction.
Degaussing Media	Method to magnetically erase data from magnetic tape.
Default	A value or setting that a device or program automatically selects if you do not specify a substitute.
Dial-up	The service whereby a computer terminal can use the telephone to initiate and effect communication with a computer.

Encryption The process of making information indecipherable to protect it from unauthorized viewing or use, especially during transmission or storage. Encryption is based on an algorithm and at least one key. Even if the algorithm is known, the information cannot be decrypted without the key(s).

Facsimile A document that has been sent, or is about to be sent, via a fax machine.

Firewall A system or combination of systems that enforces a boundary between two or more networks.

Friendly Termination The removal of an employee from the organization when there is no reason to believe that the termination is other than mutually acceptable.

Gateway A bridge between two networks.

Hardware Refers to objects that you can actually touch, like disks, disk drives, display screens, keyboards, printers, boards, and chips.

Identification The process that enables recognition of a user described to an IT.

Internet A global network connecting millions of computers. As of 1999, the Internet has more than 200 million users worldwide, and that number is growing rapidly.

Intranet A network based on TCP/IP protocols (an internet) belonging to an organization, usually a corporation, accessible only by the organization's members, employees, or others with authorization. An intranet's Web sites look and act just like any other Web sites, but the firewall surrounding an intranet fends off unauthorized access.

Intrusion Detection Pertaining to techniques, which attempt to detect intrusion into a computer or network by observation of actions, security logs, or audit data. Detection of break-ins or attempts either manually or via software expert systems that operate on logs

	or other information available on the network.
CISO/ACISO	The persons responsible to the CIO for ensuring that security is provided for and implemented throughout the life cycle of an IT from the beginning of the concept development plan through its design, development, operation, maintenance, and secure disposal.
Issue-specific Policy	Policies developed to focus on areas of current relevance and concern to an office or facility. Both new technologies and the appearance of new threats often require the creation of issue-specific policies (e.g., e-mail, Internet usage).
IT Security	Measures and controls that protect an IT against denial of and unauthorized (accidental or intentional) disclosure, modification, or destruction of IT and data. IT security includes consideration of all hardware and/or software functions.
IT Security Policy	The set of laws, rules, and practices that regulate how an organization manages, protects, and distributes sensitive information.
IT Systems	An assembly of computer hardware, software and/or firmware configured to collect, create, communicate, compute, disseminate, process, store, and/or control data or information.
LDAP	Short for Lightweight Directory Access Protocol, a set of protocols for accessing information directories. LDAP is based on the standards contained within the X.500 standard, but is significantly simpler. And unlike X.500, LDAP supports TCP/IP, which is necessary for any type of Internet access.
Least Privilege	The process of granting users only those accesses they need to perform their official duties.

Local Area Network A short-haul data communications systems that connects IT devices in a building or group of buildings within a few square miles, including (but not limited to) workstations, front-end processors, controllers, switches, and gateways.

Management Controls Security methods that focus on the management of the computer security system and the management of risk for a system.

Modem An electronic device that allows a microcomputer or a computer terminal to be connected to another computer via a telephone line.

Network Two or more systems connected by a communications medium; a network is composed of a communications medium and all components attached to that medium whose responsibility is the transference of information.

Operating System The most important program that runs on a computer. Every general-purpose computer must have an operating system to run other programs. Operating systems perform basic tasks, such as recognizing input from the keyboard, sending output to the display screen, keeping track of files and directories on the disk, and controlling peripheral devices such as disk drives and printers.

Operation Controls Security methods that focus on mechanisms that primarily are implemented and executed by people (as opposed to systems).

Overwriting media Method for clearing data from magnetic media. Overwriting uses a program to write (1s, Os, or a combination) onto the media. Overwriting should not be confused with merely deleting the pointer to a file (which typically happens when a "delete" command is used).

Password Protected/private character string used to authenticate an identity or to authorize access to data.

Parity — The quality of being either odd or even. The fact that all numbers have parity is commonly used in data communication to ensure the validity of data. This is called parity checking.

PBX — Short for private branch exchange, a private telephone network used within an enterprise. Users of the PBX share a certain number of outside lines for making telephone calls external to the PBX.

Peripheral Device — Any external device attached to a computer. Examples of peripherals include printers, disk drives, display monitors, keyboards, and mice.

Port — An interface on a computer to which you can connect a device.

Port Protection Device — A device that authorizes access to the port itself, often based on a separate authentication independent of the computer's own access control functions.

RADIUS — Short for Remote Authentication Dial-In User Service, an authentication and accounting system used by many Internet Service Providers (ISPs). When you dial in to the ISP you must enter your username and password. This information is passed to a RADIUS server, which checks that the information is correct, and then authorizes access to the ISP system.

Real Time — Occurring immediately. Real time can refer to events simulated by a computer at the same speed that they would occur in real life.

Remote Access — The hookup of a remote computing device via communication lines such as ordinary phone lines or wide area networks to access network applications and information

Risk	The probability that a particular threat will exploit a particular vulnerability of the system.
Risk Analysis	The process of identifying security risks, determining their magnitude, and identifying areas needing safeguards. Risk analysis is a part of risk management.
Risk Management	Process of identifying, controlling, and eliminating or reducing risks that may affect IT resources.
Router	An interconnection device that is similar to a bridge but serves packets or frames containing certain protocols. Routers link LANs at the network layer.
Rules of Behavior	Rules established and implemented concerning use of, security in, and acceptable level of risk for the system. Rules will clearly delineate responsibilities and expected behavior of all individuals with access to the system. Rules should cover such matters as work at home, dial-in access, connection to the Internet, use of copyrighted works, unofficial use of Federal Government equipment, the assignment and limitation of system privileges, and individual accountability.
Security Incident	An adverse event in a computer system or the threat of such an event occurring.
Security Plan	Document that details the security controls established and planned for a particular system.

Security Specifications	A detailed description of the safeguards required to protect a system.
Sensitive Data	Any information, the loss, misuse, modification of, or unauthorized access to, could affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under Section 552a of Title 5, U.S. Code, but has not been specifically authorized under criteria established by an Executive order or an act of Congress to be kept classified in the interest of national defense or foreign policy.
Separation of Duties	A process that divides roles and responsibilities so that a single individual cannot subvert a critical process.
Server	The control computer on a local area network that controls software access to workstations, printers, and other parts of the network.
Smart Card	A credit-card-sized device with embedded microelectronics circuitry for storing information about an individual. This is not a key or token, as used in the remote access authentication process.
Software	Computer instructions or data. Anything that can be stored electronically is software.
Software Copyright	The right of the copyright owner to prohibit copying and/or issue permission for a customer to employ a particular computer program.

SPAM	Process designed to crash a program by overrunning a fixed-site buffer with excessively large input data. Also, to cause a person or newsgroup to be flooded with irrelevant or inappropriate messages.
System	Set of processes, communications, storage, and related resources that are under the same direct management control, have the same function or Mission objective, have essentially the same operating characteristics and security needs, and reside in the same general operating environment.
System Availability	The state that exists when required automated information can be performed within an acceptable time period even under adverse circumstances.
System Integrity	The quality that a system has when it performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system.
System Administrator	The individual responsible for defining the system's operating parameters, authorized functions, and security requirements. This individual is usually the person who maintains the system on a day-to-day basis.
System Owner	The individual who is ultimately responsible for the function and security of the system.
TCP/IP	Transmission Control Protocol/Internet Protocol. The Internet Protocol is based on this suite of protocols.

Technical Controls	Security methods consisting of hardware and software controls used to provide automated protection to the system or applications. Technical controls operate within the technical system and applications.
Technical Security Policy	Specific protection conditions and/or protection philosophy that express the boundaries and responsibilities of the IT product in supporting the information protection policy control objectives and countering expected threats.
Telecommunications	Any transmission, emission, or reception of signals, writing, images, sound or other data by cable, telephone lines, radio, visual or any electromagnetic system.
Threat	Any circumstance or event with the potential to cause harm to a system in the form of destruction, disclosure, modification of data, and/or denial thereof.
Trojan Horse	Any program designed to do things that the user of the program did not intend to do, or that disguise its harmful intent. A program that installs itself while the user is making an authorized entry; and, then is used to break-in and exploits the system.
Unfriendly Termination	The removal of an employee under involuntary or adverse conditions. This may include termination for cause, RIF, involuntary transfer, resignation for "personality conflicts," and situations with pending grievances.
User	Any person who is granted access privileges to a given IT.

User Interface — The part of an application that the user works with. User interfaces can be text-driven, such as DOS, or graphical, such as Windows.

Virus — A self-propagating Trojan horse (a program that surreptitiously exploits the security/integrity of a program), composed of a mission component, a trigger component, and a self-propagating component.

Vulnerability — A weakness in automated system security procedures, technical controls, environmental controls, administrative controls, internal controls, etc., that could be used as an entry point to gain unauthorized access to information or disrupt critical processing.

Wide Area Network — A physical or logical network that provides capabilities for a number of independent devices to communicate with each other over a common transmission-interconnected topology in geographic areas larger than those served by local area networks.

6. APPENDIX C

6.1. REFERENCES