

ILLINOIS SECRETARY OF STATE
DATA ACCESS SECURITY AND
STANDARDS GUIDE
September, 2006

ILLINOIS SECRETARY OF STATE
DATA ACCESS SECURITY AND STANDARDS GUIDE
September 2006

This guide provides the details concerning the rules, procedures, and process for the security and access to data maintained by the Illinois Secretary of State's office.

The Department of Information Technology is responsible for overall management of data security and access to data, while each department is responsible for establishing the conditions, costs, billing, and access criteria for the use of departmental data, both internally and to outside users.

This guide is intended to give employees a general knowledge of the types of information managed by the Office of the Secretary of State, what information may be released and the manner in which the release may occur.

While it is true that a great portion of data managed by the office may be released to the public, this release may occur only after certain procedural guidelines have been met. These guidelines may be set out in specific statutes or established through office policy. Either way, it is imperative that employees understand that until the guidelines for release have been met, the information requested must be considered confidential and treated as such.

As a general rule, any request for information should be directed to the specific department that has primary responsibility for the maintenance of the data requested. In addition, no information should be released unless the employee handling the request is specifically authorized to do so.

Employees are encouraged to contact their respective supervisors concerning issues of data security. Any questions that arise concerning the release of information that cannot be resolved on the department level should be referred to the Office of the General Counsel

Jesse White
Illinois Secretary of State

TABLE OF CONTENTS:

INTRODUCTION AND SCOPE.....4
MANAGEMENT OF INFORMATION AND IT SYSTEMS.....6
ACCEPTABLE USE OF IT DATA AND RESOURCES.....7
INVENTORY AND CLASSIFICATION.....8
GENERAL AND OTHER CONTROLS.....9
SECURITY POLICY.....11
DATA SECURITY STANDARDS.....19
DATA CLASSIFICATION.....20
MINICOMPUTERS/SERVERS.....22
PERSONAL COMPUTER INSTALLATIONS.....26
MAINFRAME COMPUTERS.....28
EMPLOYEE SECURITY AWARENESS PROGRAM.....30
DEFINITIONS.....32

➤ **Introduction and Scope**

Information is collected, maintained and used by the Illinois Secretary of State to fulfill the primary mission of the Office, which is to serve the people of Illinois. The objective of data security is protecting the interests of those relying on data, and the systems and communications that deliver the information, from harm resulting from failures of integrity, confidentiality and availability. The data must be secured against unauthorized use or misuse, disclosure, inappropriate modification, destruction, loss, and denial of use. This Guide provides basic requirements regarding the security of information maintained within electronic systems (“Information Technology” or “IT” systems). This Guide applies to all departments within the Office.

The following Office Policies filed in the Secretary of State Policy Manual mandate the development and implementation of this Guide.

Security Policy - Chapter 7, Number 6, Effective Date 7-29-05

Terms used in this Guide are defined as set forth in the section entitled “Definitions” on pages 32.

➤ **Ownership**

The cornerstone to enterprise-based data security rests with enterprise data or information architecture, established ownership, rules of information ownership and custodial responsibilities, defined security requirements, established security levels, and the mechanisms to support the security levels. The information obtained, created, stored, provided and used must be examined to determine the necessary security. Secondly, the systems and media, upon which the data resides, must be reviewed and secured to insure the integrity of the information.

The departments have the responsibility to ensure that they provide all users with a secure information systems environment. To secure the information, standards and guidelines for the use and maintenance of the information must be written, accepted and adhered to. The directors of their respective departments are the owners of the information entity and are thus responsible for the information within their department. The directors cannot delegate their responsibility. However they can delegate their authority and the daily tasks necessary to a designated Departmental Liaison to insure the security of their information and systems. Ultimately, the directors are responsible for the information entrusted to their care.

The directors shall insure that adequate security standards and guidelines are written and followed by the department for which they are responsible. Each department shall have standards and guidelines regarding:

➤ **Information security**

Acceptable use of the information and IT systems, both hardware and software.

Risk analysis, data classification and business continuity.

Physical security.

Training of the department personnel.

Other standards and guidelines to insure the protection and integrity of the department's information.

➤ **Departmental Management of Information and IT Systems**

The Office Department Directors may assign responsibility for department information security to a Designated Departmental Liaison. The Liaison should have direct authority for establishing and administering the Department's information security program. Care should be taken to ensure the proper checks and balances and segregation of duties. The person functioning as the Liaison should report to the department director.

The Office Department Director's responsibilities include ensuring that appropriate internal and general controls are in place and in effect to provide reasonable assurance that control objectives related to information and security are addressed. Those responsibilities include establishing control objectives and encompass a wide variety of security-related tasks and activities. Issues to be addressed include understanding of residual risk; assessment of security risks, objectives and controls; monitoring and evaluation; and assurance mechanisms.

The identification of where the information resides should be augmented by identifying system interfaces for information sources and destinations, as security controls would need to be applied to both. The identification of the information should lead toward defining the department's data or information architecture model. This, in turn, leads one to establishing data syntax rules, office data dictionary, and data classification schemes. The identification of the information serves as a primary foundation upon which the department establishes, implements and exercises security controls appropriate to the classification scheme. The objectives of information security are the integrity, confidentiality and availability of the information. As part of their responsibilities, the department directors must insure that adequate security is maintained over the information and the systems, which process and maintain the information.

➤ Acceptable Use

The department director is responsible to insure that the use of information and IT resources are in conformance with stated policy and are used solely for intended, authorized purposes. Many of the departments must restrict the access to, and use of, their information because of federal law, state privacy law, and separation of powers within the branches of government. Such restrictions may not result in the total isolation of departments from participation in the larger IT environment of the Office. Inter-agency and inter-department access should be adequately addressed in policy, standards and guidelines and the Information Technology environment's design.

By applying the mechanisms of organizational, logical access security, and physical security we guard against unauthorized access that, in turn, could lead to unauthorized use, alteration, disclosure, or loss of information. In addition, unauthorized access could lead to contract infringement due to the failure to protect proprietary information. Unauthorized changes could lead to a loss in the integrity of information. The department director must also apply information security controls to prevent the loss of data availability by guarding against denial of service attacks and by developing appropriate contingency plans in the event of damaged or lost data files, or systems becoming inoperative or inaccessible. The directors must also have controls in place to prevent unauthorized disclosure via employees, third parties, or systems having authorized access to the data or information.

All users of information systems and IT resources in the Office are responsible for their actions. Misuse of information and IT resources may lead to consequences as detailed in the policies, executive orders and laws of the Office and the State of Illinois.

The directors must clearly define the appropriate and inappropriate uses of information and IT resources.

- All departments must formally adopt, and comply with the Office policies addressing the security of data and its appropriate use.
- Departments must provide a copy of the acceptable use policy to each new and current employee and ensure that it is enforced.
- Departments must ensure that temporary employees and third parties adhere to policy that requires that they maintain the confidentiality of the information obtained by them in the course of their work with the Office.
- Departments should check to see if there are executive orders or administrative orders that apply to data security.
- Departments are to ensure that employees and third parties do not commit copyright infringement regarding the use of software.
- Departments must examine the activities of employees, third parties, users and anyone with access to the information and IT Systems to ensure that these policies are being followed.

➤ **Inventory and Classification**

Classification of information is the process of establishing which information assets are to be protected to a specified level of effort and cost. To implement comprehensive security controls, department directors must inventory and classify their information. The systems, which process and maintain the information, must also be classified. A system may include the information, and the supporting hardware, software, and network infrastructure used to access, manipulate, transport, and store it.

- Department directors should ensure that each system and the information within it, is analyzed and classified in order to determine its value and importance to the organization.
- At a minimum, the analysis of information systems must include consideration of the integrity, confidentiality and availability of the system and information. Classification includes the determination of the amount of time the information and system can be unavailable. The department directors should know and have documented the costs and ramifications of a temporary or permanent loss of information and/or systems. Business continuity in the event of a disaster must be documented.
- The department directors should have a business contingency plan developed and documented including plans to recover the information and IT system in the event of loss.

➤ **General and other Controls**

The department director's Data Access Security and Standards document should contain sections pertaining to controls and their implementation and monitoring. This document must address controls over information as it travels through the Office and external entities. For example, networks require a wide range of security controls. Information systems and information are particularly vulnerable to unauthorized access and/or alteration during transmission. The department director's Data Access Security and Standards document should also address these controls:

- Networks must provide end-to-end security appropriate to the nature of the data that is being transported.
- Office staff access to internal networks must be subject to access control procedures (such as user-ids and passwords).
- Remote access to an internal state network(s), including, via the Internet or dedicated circuit connecting other external networks, must be consistent with Office and State of Illinois remote access policy and guidelines.

Identification of users must also be addressed. Various methods of identification and authentication are available for use. Depending on the sensitivity of the environment, information and/of IT resources, various levels of user identification may be required.

Additional controls that must be addressed include security monitoring and evaluation, assurance mechanisms, policy enforcement, personnel screening, vendor screening, audit trails, incident workflow and security breaches. Physical access and environmental controls related to IT systems and hardware facilities must have established policies and procedures to provide appropriate protection. Facilities housing information systems must be physically secured in a manner appropriate to the confidential nature of the data and the asset value of the systems. Due to the wide distribution of resources, physical security is more of a concern. On-site and off-site backup of media also should be addressed. The implemented controls must be monitored and evaluated periodically.

➤ **Risk Assessment**

Department directors should quantify risk by considering the potential threats to the information, the IT system and the IT resource, and the likelihood of each threat occurring. Potential threats include the loss of the information or systems due to accident or malicious intent, loss of availability such as the system being unavailable for a period of time, and unknown changes to the information or system so the information is no longer reliable. These risks should be weighed against the value of the system by evaluating the ensuing cost if each threat were to actually occur. Costs should be interpreted broadly to include money, resources, time, and loss of reputation among others. The department directors should understand the theories of "reasonable assurance", "residual risk", and the objectives of risk assessment. Security solutions should be selected based on the level of risk assessed for each information system.

➤ **Training**

Training and awareness are essential components of a well-designed and executed Data Access Security document. This is the most effective means of reducing vulnerability to error and fraud, and must be continually emphasized and reinforced. Office Data Access Security documents must include a formal security-training plan that will promote awareness of the Office's Data Access Security document and procedures.

➤ **Summary**

In summary, each department director is responsible for developing a Data Access Security document and procedures for their department. Each director is responsible to accomplish the following within their department:

- Provide all users with a secure information systems environment.
- Secure the information, including the IT systems, within their department.
- Ensure that proper internal and general controls are in place.
- Adopt, and comply to, an acceptable use policy.
- Adopt, and comply with, policies regarding information security, data classification and risk analysis, business continuity, physical security, training and copyright protection.
- Examine the activities of their employees, third parties, users and anyone with access to their information, relating to acceptable use and confidentiality of information.
- Inventory and classify their information.
- Determine the various levels of risk to their department's data and systems.
- Develop and implement a business continuity plan.
- Train their employees and users.

OFFICE OF THE SECRETARY OF STATE POLICY MANUAL

➤ **Introduction**

This security policy is a formal set of rules by which those people who are given access to the Illinois Secretary of State's technology and information assets must abide. The Security Policy serves several purposes. The main purpose is to inform department users, Department of Information Technology (DoIT) staff, managers, and contractors of their obligatory requirements for protecting the technology and information assets of the Secretary of State.

The Security Policy describes the technology and information assets that we must protect and also identifies the threats to those assets.

The Security Policy also describes the user's responsibilities and privileges. What is considered acceptable use? What are the rules regarding Internet access? The Security Policy answers these questions, describes user limitations and informs users there will be penalties for violation of the Security Policy.

This document also contains procedures for responding to incidents that threaten the security of the Secretary of State's computer systems and network.

➤ **What We Are Protecting**

It is the obligation of all users of the Secretary of State's systems to protect the technology and information assets of the Secretary of State's office. The computer systems and networks of the Secretary of State perform a valuable service to the people of this state and contain confidential information about the citizen of the state and the state's business. This information must be protected from unauthorized access, theft, and destruction.

The technology and information assets of the Secretary of State's office are made up of the following components:

- Computer Hardware including processor, memory, disk, and peripheral components of: the Enterprise Server, mid-range Unix Web Servers, Application Servers, Database Servers, Print and File Servers, and MS-Windows PC systems. (This includes all Novell and Windows Servers.)
- System Software including Operating Systems, database management systems, TP monitors, backup and restore software, communications protocols, and so forth.
- Application Software used by the various departments within the Secretary of State's office. This includes custom written software application, and commercial off the shelf software packages
- User department information stored on various database systems including IBM DB2, Oracle, and Sybase. This includes information stored off-line on magnetic tape media as well as information available from on-line disk systems.
- Communications Network hardware and software including routers, routing tables, hubs, modems, multiplexers, switches, firewalls, private lines, and associated network management software and tools.

➤ **Classification of Information**

User department information found in computer system files and databases shall be classified as either confidential or non-confidential.

The Department Directors shall classify the information controlled by them. The Chief Information Officer is required to review and approve the classification of the information and determine the appropriate level of security to best protect it. Furthermore, the CIO shall classify information controlled by units not administered by a Department Director.

➤ **Threats to Security**

➤ **Amateur Hackers and Vandals**

These people are the most common type of attackers on the Internet. The probability of attack is extremely high and there is also likely to be a large number of attacks.

These are usually crimes of opportunity. These amateur hackers are scanning the Internet and looking for well-known security holes that have not been plugged. Web servers and electronic mail are their favorite targets. Once they find a weakness they will exploit it to plant viruses, Trojan horses, or use the resources of your systems for their own means. If they do not find an obvious weakness they are likely to move on to an easier target.

➤ **Criminal Hackers and Saboteurs**

The probability of this type of attack is low, but not entirely unlikely given the amount of sensitive information contained in the Secretary of States' databases. The skill of these attackers is medium to high as they are likely to be trained in the use of the latest hacker tools. The attacks are well planned and are based on any weaknesses discovered that will allow a foothold into the network.

➤ **User Responsibilities**

This section establishes usage policy for the computer systems, networks and information resources of the Secretary of State. It pertains to all employees and contractors who must use the computer systems, networks, and information resources in the course of their job duties. It also pertains to Illinois State agencies, business partners, and individuals who are granted access to the network for the business purposes of the Secretary of State.

➤ **Acceptable Use**

User accounts on Secretary of State computer systems are to be used only for business of the Secretary of State and are not to be used for personal activities. Unauthorized use of a Secretary of State system is in violation of the law constitutes theft and is punishable by law. Therefore, unauthorized use of Secretary of State

computing system and facilities may constitute grounds for either civil or criminal prosecution.

Users are personally responsible for protecting all confidential information used and/or stored on their accounts. This includes their logon ids, passwords and dialup or dial back modem phone numbers. Furthermore they are prohibited from making unauthorized copies of such confidential information and/or distributing it to persons outside of the Secretary of State's office.

Users shall not purposely engage in activity with the intent to: harass other users; degrade the performance of the system; divert system resources to their own use; or gain access to Secretary of State systems for which they do not have authorization.

Users shall not attempt to access any data, scripts or programs contained on Secretary of State computer systems for which they do not have authorization or the explicit consent of the owner of the data, scripts or programs.

Users shall not attach unauthorized modems to their PCs or workstations for the purpose of remote access through a dialup phone line. Users shall not install remote access software, such as PC AnyWhere, on their PCs or workstations unless they have received specific authorization from the employee's manager and security administrator.

Users shall not download unauthorized software from the Internet onto their PCs or workstations.

Users are required to report any weaknesses in the Secretary of State computer security, any incidents of misuse or violation of this policy to the Security Administrator.

➤ **Use of the Internet**

The Secretary of State will provide Internet access to employees and contractors connected to the internal Department of Information Technology network who have a business need for this access. Employees and contractors must obtain permission from their Department Director and file a request with the Security Administrator.

The Internet is a business tool for the Secretary of State. It is to be used primarily for business-related purposes such as: communicating via electronic mail with suppliers and business partners, obtaining useful business information, and researching relevant technical and business topics. Limited, occasional or incidental use of the Internet for personal, non-business purposes are understandable and acceptable – as is the case with personal phone calls. However, employees must demonstrate a sense of responsibility and must not abuse the privilege.

The Internet service may not be used for transmitting, retrieving or storing any communications of a discriminatory or harassing nature or which are derogatory to any individual or group, obscene or pornographic, or defamatory or threatening in nature or for "chain letters" or any other purpose which is illegal or for personal gain.

➤ **User Classification**

All users are expected to have knowledge of these security policies and are required to report violations to the Security Administrator or the Office of the Inspector General. Furthermore, all users must conform to the Acceptable Use Policy defined in this document.

➤ **Monitoring Use of Computer Systems**

The Secretary of State has the right and capability to monitor electronic information created and/or communicated by persons using Secretary of State computer systems and networks, including e-mail messages and usage of the Internet. It is not the

Secretary of State's policy or intent to continuously monitor all computer usage by employees or other users of the Secretary of State's computer systems and network. However, users of the systems should be aware that the Secretary of State may monitor usage, including, but not limited to, patterns of usage of the Internet (e.g. site accessed, on-line length, time of day access), and employees' electronic files and messages to the extent necessary to ensure that the Internet and other electronic communications are being used in compliance with the law and with Secretary of State policy.

➤ **Access Control**

A fundamental component of our Security Policy is controlling access to the critical information resources that require protection from unauthorized disclosure or modification. The fundamental meaning of access control is that permissions are assigned to individuals or systems that are authorized to access specific resources. Access controls exist at various layers of a system, including the network, Unix hosts, Enterprise Server, databases, and user applications. At the system and network level, access control is implemented by logon id and password. At the application and database level, other access control methods can be implemented to further restrict access. The application and database systems can limit the number of applications and database tables available to users based on their job requirements.

➤ **Departmental User System and Network Access- Normal User Identification**

All users will be required to have a unique logon id and password for access to the Enterprise Server; Unix based client/server systems and the LAN network operating system. The user's password should be kept confidential and MUST NOT be shared with management/supervisory personnel and/or any other employee whatsoever.

All users must comply with the following rules regarding the creation and maintenance of passwords:

- Password must be a minimum of six (6) characters long.
- Password must not be found in any English or foreign dictionary. That is, do not use any common name, noun, verb, adverb, or adjective. These can be easily cracked using standard "hacker tools".
- Passwords should not be posted on or near computer terminals or otherwise be readily accessible in the area of the terminal.
- Password must be changed every 35 days.
- User accounts will be frozen after 3 failed logon attempts.
- Logon Ids and passwords will be suspended after 31 days without use.

Users are not allowed to access password files on the Enterprise Server, Unix systems, Windows servers, routers, firewalls, or any network infrastructure component. Password files on servers will be monitored for access by unauthorized users. Copying, reading, deleting or modifying a password file on any computer system is prohibited.

Users will not be allowed to logon as "root" on production Unix systems or "system administrator" on production Windows systems. Users who need this level of access to production systems must request a Special Access account as outlined elsewhere in this document.

Employee Logon Ids and passwords will be deactivated as soon as possible if the employee is terminated, fired, suspended, placed on leave, or otherwise leaves the employment of the Secretary of State.

Departments should immediately contact the Department of Information Technology directly to report change in employee status that requires terminating or modifying employee logon access privileges.

Employees who forget their password must call the Help Desk to get a new password assigned to their account. The employee must identify himself or herself by providing the last four digits of their social security number to the Help Desk administrator.

Employees will be responsible for all transactions occurring during Logon sessions initiated by use of the employee's password and Id. Employees should not Logon to a computer and then allow another individual to use the computer or otherwise share access to the computer systems.

➤ **System Administrator Access**

System administrators, network administrators, and security administrators will have root or system administrator level access to host systems, routers, hubs, and firewalls as required to fulfill the duties of their job.

The root password for Unix systems and system administrator passwords will be shared by a small group of systems administrators. The same rules for password creation apply to the root and system administrator passwords. The passwords should be chosen so that it is not easily cracked by hackers' tools designed to decrypt passwords. These passwords should also be changed every 35 days.

All root and system administrator passwords will be changed immediately after any employee who has access to such passwords is terminated, fired, or otherwise leaves the employment of the Secretary of State.

➤ **Special Access**

Special access accounts are provided to individuals requiring temporary root or system administrator privileges in order to perform their job. These accounts are monitored by the Secretary of State Security Administrator and require the permission of the user's Department Director. Monitoring of the special access accounts is done by entering the users into a Special Access Database and periodically generating reports to management. The reports will show who currently has a special access account, for what reason, and when it will expire. Special access accounts will expire in 35 days and will not be automatically renewed without written permission.

In cases where an individual has special access accounts on multiple systems, there will be a separate entry in the database for each account. Unix accounts requiring UID 0 must be approved by the Department Director and the Secretary of State Security Administrator and are monitored by the Operations Manager using the Special Access Database.

➤ **Connecting to Third-Party Networks**

This policy is established to ensure a secure method of connectivity provided between the Secretary of State and all third-party companies and other government agencies required to electronically exchange information with the Secretary of State. "Third-party" refers to other government agencies, vendors and consultants doing business with the State of Illinois, and other business partners that have a need to exchange information with the Secretary of State.

Third-party network connections are to be used only by the employees of the third-party for the business purposes of the Secretary of State. The third-party company will ensure that only authorized users will be allowed to access information on the Secretary of State's network. The third-party will not allow Internet traffic or other private network traffic to flow into the Secretary of State network.

A third-party network connection is defined as one of the following connectivity options:

- Leased line. Leased lines (e.g. T1) will terminate at a Secretary of State router on a third-party subnet.
- VPN encrypted Tunnel. A VPN network connection will terminate on a Secretary of State firewall, and the third-party will be subject to standard Secretary of State authentication rules.
- Dial-up Connection. Dial up connection to third-party networks will be permitted with a secure one-time password system.
- Third-party network connections will be configured for TCP/IP and SNA/LLC protocols.

This policy applies to all new third-party connection requests and any existing third-party connections. In cases where the existing third-party network connections do not meet the requirements outlined in this document, they will be re-designed as needed.

All requests for third-party connections must be made by submitting a Third-Party Network Connection Document and be approved by the Chief Information Officer and the relevant Department Director of the Secretary of State.

➤ **Connecting Devices to the Network**

Only authorized devices may be connected to the Secretary of State network. Authorized devices include PCs and workstations owned by the Secretary of State that comply with the configuration guidelines of the Secretary of State. Other authorized devices include: network file and print servers; Unix hosts used as application and database servers; and network routers, hubs, firewalls and other authorized network infrastructure devices used for network management and monitoring.

Users shall not attach to the network: Windows PCs, workstations, or Unix-based (including Linux) host computers that are not owned and/or controlled by the Secretary of State. Users are specifically prohibited from attaching PCs or workstations running host port scanning, "sniffers" or TCP/IP filtering programs to the Secretary of State network.

Users are not authorized to attach any device that would alter the routing or bridging characteristics of the Secretary of State's network. These devices include routers, bridges, and host computers equipped with two or more network interface cards running a routing protocol. Installation and maintenance of bridges and routers is restricted to the Secretary of State Department of Information Technology.

➤ **Remote Access**

Only authorized persons may remotely access the Secretary of State network over dialup facilities. Remote access is provide to those employees, contractors and business partners of the Secretary of State that have a legitimate business need to exchange information, copy files or programs, or access computer applications. Authorized connection can be remote PC to the SOS network or a remote network to SOS network connection.

The only acceptable method of remotely dialing in to the internal Secretary of State network is using a secure one-time password.

➤ **Unauthorized Remote Access**

The attachment of modems and dialup lines to an user's PC or workstation that are connected to the Secretary of State's LAN is not allowed without the written

permission of the Secretary of State Security Administrator. Additionally, users may not install personal software designed to provide remote control of the PC or workstation (e.g. PC AnyWhere). This type of remote access bypasses the authorized, highly secure methods of remote access and poses a threat to the security of the entire network.

➤ **Penalty For Security Violation**

The Secretary of State's Office takes the issue of security seriously. Those people who use the technology and information resources of the Secretary of State must be aware that they can be disciplined if they violate this policy. Upon violation of this policy, an employee of the Office of Secretary of State may be subject to discipline up to and including discharge. The specific discipline imposed will be determined by a case-by-case basis, taking into consideration the nature and severity of the violation of the Security Policy, prior violations of the policy committed by the individual, and all other relevant information. Discipline, which may be taken against an employee, shall be administrated in accordance with any appropriate collective bargaining agreement, the Merit Employment Code, as well as the Rules of the Department of Personnel and the Office of the Secretary of State's Policy Manual.

In a case where the accused person is not an employee of the Secretary of State's Office, the matter shall be submitted to the Security Administrator and the Inspector General shall be notified. The Security Administrator, with the advice and consent of the applicable Department Director, may recommend to the Inspector General that local, state, or federal law enforcement is notified and formal charges filed against the accused security violators. The Inspector General may refer the information to law enforcement agencies and/or prosecutors for consideration as to whether criminal charges should be filed against the alleged violator(s).

➤ Security Incident Handling Procedures

This section provides some policy guidelines and procedures for handling security incidents. The term “security incident” is defined as any irregular or adverse event that threatens the security, integrity, or availability of the information resources on any part of the Secretary of State’s network. Some examples of security incidents:

- Illegal access of a Secretary of State computer system. For example, a hacker logs on to a production Unix server and copies the password file.
- Damage to a Secretary of State computer system or network caused by illegal access. Releasing a virus or worm would be an example.
- Denial of service attack against a Secretary of State Web server. For example, a hacker initiates a flood of packets against a Web server designed to cause the system to crash.
- Malicious use of system resources to launch an attack against other computer outside of the Secretary of State’s network. For example, the Unix system administrator notices a connection to an unknown network and a strange process accumulating a lot of server time.

Employees, who believe their terminals or computer systems have been subjected to a security incident, or has otherwise been improperly accessed or used, should report the situation to their information technology liaison immediately. The employee should not turn off the computer or delete suspicious files. Leaving the computer in the condition it was in when the security incident was discovered will assist in identifying the source of the problem and in determining the steps that should be taken to remedy the problem.

ILLINOIS SECRETARY OF STATE DATA SECURITY STANDARDS

The following standards and guidelines have been prepared to assist departments in developing computer security procedures. They are issued in accordance with Policy, and should be included within each department's Standards and Procedures Manual. These standards apply to all Illinois Secretary of State departments and employees, including persons providing contractual services to the Secretary of State.

A secure and accountable environment can only result from conscious action by the Department Directors controlling the data. As custodian of the Secretary's data, each Department Director shall implement adequate measures as specified by these security standards and guidelines with regard to use, identification, classification and protection of these assets. If it is determined that any specific standard or guideline is not required or does not need to be fully implemented, a clear explanation within the department's Data Security Procedures is required.

The Standards are subdivided into five categories:

1. Data Classification
2. Minicomputer/Servers
3. Personal Computer
4. Mainframe
5. Employee Security Awareness

Categories 2, 3 and 4 contain the Standards applicable to any department using such equipment. The other two categories are applicable to all departments regardless of the type of equipment used.

Each Standard may be accompanied by one or more Guidelines that will provide insight to the elements of concern within the issue that the Standard addresses. Further clarification of some Standards can be obtained by referring to the appendix and glossary of terms.

STANDARDS AND GUIDELINES FOR DATA CLASSIFICATION

➤ **Standards:**

- The Office of the Secretary of State shall classify computer-generated data as 1) confidential or 2) non-confidential.
- Directors shall classify data controlled by them. The Deputy Secretary of State/Chief of Staff shall 1) approve each data classification and 2) classify data controlled by units that are not administered by Directors. When two or more departments or units share the use of computer data, the Director primarily responsible for the maintenance of that data shall determine its classification and procedures for handling it.
- Directors and the Deputy Secretary of State/Chief of Staff must have written procedures for handling the confidential information and update them following changes or modifications.
- All confidential information produced on a computer screen must have adequate computer access controls to prevent its unauthorized disclosure.
- The Office must not violate the Freedom of Information Act or the Privacy Act when classifying data as confidential.

➤ **Guidelines:**

- The Secretary of State will protect its computer data from being misused by establishing confidential and non-confidential classifications.
- The Directors and, where appropriate, the Deputy Secretary of State/Chief of Staff, are responsible for establishing internal procedures to classify, reclassify and declassify computer-generated information. If two or more departments or units use the same data, the Director maintaining the data will classify it and establish the procedures for handling it.
- A directory that lists information about handling confidential computer-generated information may be developed and printed in booklet form and may be made available on-line for supervisors and employees handling classified data. The Deputy Secretary of State/Chief of Staff shall designate the individuals responsible for producing the office-wide directory and how often it should be updated. The information in the directory should include, at minimum, the following: 1) document or computer data title; 2) department or unit responsible for producing and classifying the document or data; 3) format; 4) whether that information is exempt from the Freedom of Information Act; 5) special instructions.
- The Directors and Deputy Secretary of State/Chief of Staff will maintain any written procedures that are developed for handling confidential information, including documents transmitted through fax machines.

- Information about computer access control procedures are provided in other sections of the Data Access Standards manual.
- The Technology Advisory Council will provide updated information for Directors to use in understanding any effect that the Freedom of Information, Privacy Act or any other relevant laws, rules or regulations would have on department procedures to properly classify information.
- The Data Security Administrator will keep the Technology Advisory Council and the Deputy Secretary of State informed of technological developments or other matters that would have an impact on data classification standards and procedures.

STANDARDS AND GUIDELINES FOR MINICOMPUTERS/SERVERS

- **Standards**
- **Administrative Duties and Controls**
 - **Each Director shall provide:**
 - Administrative controls and reviews to assure that:
 - Computer security procedures are current.
 - Computer security procedures are implemented in a reasonable period of time in accordance with these Standards and Guidelines.
 - Computer security procedures are maintained within the Department Standards and Procedures Manual.
 - Computer security procedures are implemented and conformed to.
 - Breaches of computer security procedures are reported to management, administrative personnel or the Director.
 - Access to minicomputers/servers and peripherals are limited to authorized users.
- **Computer Availability and Application Scheduling**
 - **The IT Director shall provide Computer availability:**
 - Adequate trained support to provide/maintain the availability of all minicomputers/servers and application scheduling under its control.
 - Personnel trained to turn on/off the system.
 - Personnel trained to initiate standard operating commands.
 - Personnel trained in trouble shooting computer equipment.
 - The scheduling of the Applications shall include personnel trained.
 - Monitoring of software programs running on the system.
 - The control of the information input and data output for security purposes.

➤ **Environmental Concerns**

➤ **Each Director shall provide:**

- Adequate protection to ensure that environmental issues are addressed.
- That only authorized personnel are allowed in computer rooms.
- Adequate alternative power sources are operable and available, where appropriate.
- A system to restrict and monitor access only to areas necessary for job performance.

➤ **The IT Director will be responsible for:**

- Adequate security and alarm devices are used, including temperature, humidity and fire controls.
- Adequate precautions when visitors or outside users have access to the computer room.
- The controlled movement, and library storage of Data Media.
- Formal procedures existing to ensure a well-maintained environment for safe computer operations.
- Provide that back-ups of data, programs and documentation, are readily available.

➤ **Hardware**

➤ **Each Director shall provide:**

- Adequate physical protection to ensure that hardware issues are addressed.
- All minicomputers/servers and peripherals are recorded in the department's inventory records.
- All equipment is physically identified as Secretary of State property by tag or other marking.
- When not in use, equipment is secured against theft.
- Minicomputers/servers are protected against power surges and static electricity.
- Employees are cautioned that eating, or drinking, in the vicinity of the computer equipment may damage the equipment or data files.

➤ **The IT Director will be responsible for:**

- Data storage media is protected against damage such as exposure to excessive cold or heat or to magnetic fields.
- Adequate written documentation is maintained to familiarize users with existing/new hardware (i.e., printers, terminals, scanners).

- Formal procedures exist for servicing computers.
- **System operations Controls**
 - **The IT Director shall:**
 - Implement adequate computer management practices to ensure that system-operating controls are addressed.
 - Maintain a computer operations log, if appropriate.
 - Insure that computer operators have access to all information necessary for the operation of the system.
 - Insure that computer operations log is reviewed and purged on a periodic basis.
 - Insure that hardware and software error correction capabilities as designated by the manufacturer, including:
 - Procedures for restarts;
 - Shifting an application from one computer to another in the event of extended hardware failure or scheduled maintenance.
 - Backup copies of the operating systems and information maintained in an off-site location.
 - Operating system controls exist to prevent unauthorized bypasses and/or overrides of operating system parameters.
 - Application scheduling procedures are in use.
 - Distribution procedures for computer printouts exist and are used.
 - Computer operating problems are analyzed and subjected to management review.
 - **Software Security**
 - **The IT Director shall instill that:**
 - Software security features for minicomputers/servers are to be used to prevent unauthorized access or data entry to operating systems, system utilities, application programs or data files.
 - Operating Systems and purchased System Utilities software security controls are to be established for purposes of:
 - Protecting the vendor's copyrights and licensing.
 - Verifying and assuring proper administrative access.
 - Planning installations and modifications when necessary.

- Providing adequate documentation when installation and, modification occurs.
- Providing accessibility to reserved or backup copies through on-site backup or vendor supplied backup.
- Application Program security controls are to include:
 - A methodology for planning, development, system design, documenting, testing and implementing of new or modified applications.
 - Verification and assurance of proper administrative access and operation of software.
 - Documented backup and recovery process.
 - Establish program test area and procedures for moving the programs from the test area to production.
 - Contractual agreement procedures for vendor developed or vendor assisted development of software.
- Informational Data security controls are to include:
 - Sufficient processing edits and passwords through Operating Software and application programs for the protection of data and its conversion to machine-readable form using procedural controls, mechanical or visual verification, internal computer comparisons and questioning.
 - Adequate control over transmittal and input of data to detect loss or non-processing.
 - Appropriate manual verification and checking of inputs and outputs by personnel other than computer operators and entry operators.

Note: These Standards and Guidelines have been based on recommendations in the Fiscal Control and Internal Auditing Act.

STANDARDS AND GUIDELINES FOR PERSONAL COMPUTER INSTALLATIONS

➤ **Standard**

All computerized data, hardware and media will be analyzed for appropriate security; each Director shall ensure the presence of this data security program and the implementation of appropriate data control procedures from two perspectives:

- Control systems must be maintained that assure against unauthorized modification of data. Illegal copying of purchased programs is prohibited.
- Control systems also must be maintained that assure against unauthorized-disclosure of computerized data.

➤ **Guidelines:**

➤ **Each Director should:**

- Designate a Departmental Liaison. The Liaison should have direct authority for establishing and administering the Department's information security program.
- Ensure that security measures and retention periods are implemented.
- Protect computer hardware, applications, data and media from the hazards of natural disaster, theft, computer viruses and other malicious acts.
- Restrict computer applications and data access to authorized persons.
- Provide appropriate data security training.
- Develop and maintain documentation to ensure continuity of programs and access to data by authorized users.

➤ **The IT Director shall:**

- Install methods to detect unauthorized attempts to access computer applications.
- Implement appropriate backup procedures and make necessary provisions for recovery of computer applications and data.

➤ **Application Developers should:**

- Obtain authorization in writing prior to making changes to a computer application, except in the case of the emergency repair of a processing failure. On these occasions, authorization should be obtained promptly after repair of the failed software.
- Assure that only authorized changes are implemented to computer applications.
- Document all modifications to applications. Using the BIZ FLOW PIR system.

➤ **Users should:**

- Follow procedures issued or approved by the Director.
- Protect computer readable media as if it were a document of the same security classification.
- Management must understand these processing environments, and evaluate the need for separation of duties.

STANDARDS AND GUIDELINES FOR MAINFRAME COMPUTERS

➤ **Standards:**

Each SOS Director has the responsibility for controlling and modifying data and shall exercise adequate measures with regard to the use, identification, classification, and protection of these data assets.

➤ **Each Director Shall Enforce:**

- Standards and report observations of, computer fraud and misuse. The Secretary of State's Department of Information Technology Director shall assist other Directors with this enforcement.
- The use of state-owned or leased computer systems shall be for authorized purposes only. Directors shall be responsible for the proper authorization of computer utilization.
- Acknowledgement of selling computer data/information is prohibited without meeting the written requirements of the legal counsel.
- That programs or data owned by or under the control of the Secretary of State shall not be released to non-Secretary of State agencies without written authorization of the legal counsel and the Director responsible for the data.
- To advise their employees that passwords and other Information Technology security procedures shall be protected from unauthorized use or disclosure as a condition of employment. Misuse of such material or unauthorized disclosure will be subject to disciplinary action.
- The established procedures to assure that employees who are terminated shall return all Secretary of State property and equipment used in conjunction with state computer systems. Failure to return such property will cause the Secretary of State to create a lien for its return.
- To maintain an adequate level of access control to prevent unauthorized access to equipment, documentation and data. Storage areas and work areas for data, equipment, and documentation are to be kept secure through the use of locks, card access systems, guards, inventory and other appropriate measures.
- To identify to the Department of Information Technology Director the individual(s) liaisons that will be responsible for computer and data security.

➤ **The IT Director:**

- Has responsibility for implementing the following requirements on its mainframe computers and all satellite computer operations:
 - All timesharing Users will be automatically logged off after a specified period of non-use.

- The availability and use of User Identification (User-ID) to control security shall be provided to all Users.
- A forced password change is in effect of 35 Days.
- Passwords shall be prevented from being used repetitively.
- Access privileges for any LAN Access (E-Mail) which has not been used for 31 days, is automatically Suspended and Deleted: until authorized personnel (*IT Liaisons*) request reinstatement of such access.
- Access Privileges for User Identification User-ID (RACF-ID), which has not been used for 31 days, is automatically Suspended, then Deleted After 90 days: until authorized personnel (*IT Liaisons*) request reinstatement of such access.
- A comprehensive plan will be established to recover the information assets entrusted to it in the event of accidental or intentional destruction of data through natural or man-made disasters.
- Unless otherwise stipulated, all computer programs and data developed by employees, consultants or other contractors, or provided to employees, consultants or other contractors for use in conjunction with programmers or data developed, are the property of the Secretary of State.
- A computer or data contract, lease, license, or agreement cannot be entered into without a provision advising vendors of the Secretary of State's requirements for Information Technology security, including maintenance, return and ownership.

STANDARDS AND GUIDELINES FOR EMPLOYEE SECURITY AWARENESS PROGRAM

➤ Standards:

- An office-wide training program shall be devised by the Technology Advisory Council and approved by the Deputy Secretary of State/Chief of Staff to ensure uniformity within the departments' Employee Security Awareness Programs. This training will be given to Administrative and Supervisory Personnel.
- Each Director is responsible for conducting security awareness workshops or announcements to instruct employees in security procedures for protecting computer data assets.
- The Director of Personnel shall be responsible for informing new employees about the Office's data security program. The Director of Personnel shall also have new employees sign a statement indicating that they are aware of the program. The statement shall be placed in the employee's personnel file.

➤ Guidelines:

- The Secretary of State's office will make all employees aware of the necessity for protection of computer data assets by making office-wide presentations through assemblies, memoranda, posters, and other employee communication techniques chosen by the Deputy Secretary of State/Chief of Staff.
- The Data Security Administrator will plan periodic announcements, presentations, or other training techniques to keep employees aware of the necessity for computer data asset protection and informed about program changes or updates. Directors should maintain written records documenting the training done and the employees who participated.
- The Director of Personnel should prepare written or visual presentations informing new employees of the necessity for protecting computer data assets.
- The Secretary of State relies heavily on its Information Technology (IT) systems to meet its operational, financial and informational requirements. It is essential that these systems are protected from misuse and that both the computer systems and the data used therein be operated and maintained in a secure environment. The data security program should provide the framework for protecting the Secretary of State computer data, hardware, and media without necessarily hindering its natural flow or incurring unnecessary cost. The objectives for our data security program are to:
 - Enhance protection from incidents or acts that would cause equipment or software malfunction, errors, omissions, unauthorized disclosure of data, or destruction of data or equipment.
 - Upgrade active detection and prevention of unauthorized disclosure, accidental or deliberate, of information.

- Encourage planning to enable our organization to survive business interruptions due to security failure, and function adequately after survival.
 - Foster timely damage assessment following detection of data contamination, unauthorized disclosure of information or physical penetration of the processing facility, or loss of the processing facility.
 - Improve employee education, awareness, and participation in the security program.
 - Promote accuracy and integrity of data.
 - Advance management awareness of need for security and their active participation in development and enforcement of the security policy.
- **The responsibilities of the Technology Advisory Council are to:**
- Continuously evaluate information technology security.
 - Identify potential threats to computers, applications, data and data communications equipment.
 - Develop Standards to safeguard the Secretary's investment in information systems.
 - Ensure the success of the security plan through an employee awareness program.

➤ **Definitions:**

- For purposes of this Guide, the following terms are defined:
 - **Application** – is a computer program designed to collect, edit, maintain, and analyze data and to report information.
 - **Assurance Mechanisms** – is a system of internal controls including monitoring, evaluation, feedback, and correction activities with respect to the proper design, implementation and operation of the system of internal controls.
 - **Authentication** – is the process of verifying the identity of a user attempting to access the information or attempting to use the IT assets of the Secretary of State. Any user, either within the Secretary of State's IT systems or those users attempting to gain access to the Secretary of State's information, must be identified and authenticated.
 - **Confidential Information** – is information, which is restricted in its use, accessibility or dissemination, by Office policy, law, regulation or executive order.
 - **Chief Information Officer.** The Director of the Department of Information Technology (DoIT) shall serve as the Chief Information Officer.
 - **Data** – is sometimes considered synonymous with information. It can also be interpreted to mean the raw, individual symbols which when collected, maintained or analyzed become information.
 - **Database** – is an organized storage of data.
 - **Data Security Administrator** – The person who has received the delegated authority for insuring that the information and IT systems of the Office have adequate security controls in place and functioning so that the Office is in conformance with its' security policies and is in conformance with good practice. The Director/CIO of DoIT shall designate an employee of DoIT as the Data Security Administrator for the Office of the Secretary of State. This person is a Department of Information Technology employee and reports to the Director/CIO of the DoIT.
 - **Department** – is a defined entity within the Secretary of States' Office with specific mission to fulfill the laws and directives applicable to the Illinois Secretary of State.
 - **Departmental IT liaison** – A person assigned within a department with the responsibility for departmental information security. The Liaison will have direct authority for establishing and administering their Department's information security program. Ensure that proper internal and general controls are in place. Adopt and comply with an acceptable use policy, policies regarding information security, data classifications, risk analysis, business continuity, physical security, training, and copyright protection. Examine the activities of their employees, third

party users, and anyone with access to their information. Inventory, and classify their information. Determine the various levels of risk to their department's data and systems. Develop and implement a business continuity plan, and train their employees and users.

- **DMZ** – is Demilitarized Zone. DMZ within the context of this Guide is defined as a network between a protected network and an external network in order to provide a layer of security. A DMZ is sometimes referred to as a “perimeter network.”
- **Encryption** – is the process of encoding electronic data that makes it unintelligible to anyone except the intended recipient. There are different levels of encryption. Stronger levels of encryption may be more costly in terms of resources and thus be used for the most sensitive information. Lower levels of encryption may be used for less sensitive information. The use of different levels of encryption should be used based on the level of sensitivity of the data to be encrypted. Decryption is the method used to convert the coded, encrypted data to understandable form.
- **Externally accessible to public** - The system may be accessed via the Internet by persons outside of the Secretary of State without a logon id or password. The system may be accessed via dial-up connection without providing a logon id or password. It is possible to “ping” the system from the Internet. The system may or may not be behind a firewall. A public Web Server is an example of this type of system.
- **Firewalls** – are specialized computers and programs, residing in a virtual area between an organization's network and outside networks, which are designed to check the origin and type of incoming data in order to control access, and block suspicious behavior or high-risk activity.
- **General Controls** – are controls that operate over and within an information technology facility and/or processing environment. General control areas include IT-related organization and management, physical and system access security, environment protection, program change control, business continuity planning, hardware and software maintenance, IT-related asset inventory control, computer operations, and IT-related contract services.
- **Host** – is a computer that mediates access to databases and/or provides other services to a computer network.
- **Information** – is a collection of pieces of data which when collected, maintained and/or analyzed becomes usable.
- **Internally accessible only** - Users of the system must have a valid logon id and password. The system must have at least two levels of firewall protection between its network and the Internet. The system is not visible to Internet users. It may have a private Internet (non-translated) address and it does not respond to a “ping” from the Internet. A private intranet Web Server is an example of this type of system.

- **Information Technology Resources or IT Resources** – are resources, which include computers, printers and other peripherals, programs, data, local and wide area networks, and means of internet access.
- **Information Security** – is measures, procedures, and controls that provide an acceptable degree of safety for information and IT resources, protecting them from accidental or intentional disclosure, modification, or destruction.
- **Internal Controls** – are the policies, procedures, practices and organizational structures designed to provide reasonable assurance that business objectives will be achieved and that undesired events would be prevented or detected and corrected.
- **Non-Public, Externally accessible** - Users of the system must have a valid logon id and password. The system must have at least one level of firewall protection between its network and the Internet. The system may be accessed via the Internet or the private Intranet. A private FTP server that is used to exchange files with business partners is an example of this type of system.
- **Office** – refers to all Secretary of State departments as an entity.
- **Owner** – Is the department director responsible for the data for their respective department. The owner is ultimately responsible for the information and IT systems within his/her purview. The owner must insure that the entity for which they are responsible has the security policies and procedures in place to safeguard the information and IT resources of the department.
- **Password** – is a string of characters known to a computer system or network and to a user who must enter the password in order to gain access to information or an IT resource.
- **PC** – is an abbreviation for a personal computer. The personal computer is designed for an individual's use rather than for use as a shared resource such as a mainframe, mid-range, or server computer.
- **Residual Risk** – is risk, which is not mitigated by controls and security measures. Residual risk remains even after the proper design, implementation and exercise of a system of internal controls that provide, at least, a reasonable level of assurance that control objectives will be met. Residual risk should be identified, documented and formally accepted. The residual risk should be offset with adequate insurance coverage, contractually negotiated liabilities and self-insurance.
- **Security Breach** – is an unauthorized access, loss, disclosure, modification, or destruction of information resources, whether deliberate or accidental.
- **Security Controls** – are the procedures, policies, programs, and physical safeguards including hardware, that are put in place to assure the integrity of

information. Security Controls may be used to protect the means of processing information.

- **Sensitive Information** – is information that is created, received or held by departments, which requires special precautions to protect it from unauthorized access, disclosure, modification, or deletions.
- **Third Party** – is a non-State entity or other State Agency that performs information technology services for, or accesses the Secretary of States' information or IT resources or, otherwise maintains a network-to-network connection with, the Secretary of State.