State of Oklahoma

Information Security

Policy, Procedures, Guidelines

Issued September 1, 2003

Version 1.5 Revised July 18, 2011 by the Office of State Finance

Table of Contents

Preface

The contents of this document include the minimum Information Security Policy, as well as procedures, guidelines and best practices for the protection of the information assets of the State of Oklahoma (hereafter referred to as the State). The Policy, as well as the procedures, guidelines and best practices apply to all state agencies. As such, they apply equally to all State employees, contractors or any entity that deals with State information.

The Office of State Finance will communicate the Policy, procedures, guidelines and best practices to all state agencies. In turn, all agencies are required to review the Policy and make all staff members aware of their responsibility in protecting the information assets of the State. Those agencies that require additional controls should expand on the content included in this document, but not compromise the standards set forth.

The Policy and those procedures prefaced by “must” are mandatory as the system involved will be classified as insecure without adherence. Guidelines and best practices are generally prefaced with “should” and are considered as mandatory unless limited by functional or environmental considerations.

It is recognized that some agencies have their own proprietary systems that may not conform to the Policy, procedures, guidelines and best practices indicated in this document. A plan for resolution of these system limitations should be created. Any exceptions are to be documented and be available on request. Other non system related standards that do not require system modification, should be instituted as soon as possible.

Revisions to this document are maintained collectively in Appendix E: Revisions, which includes a “Revision Table” describing each addition, change or deletion and the date it was implemented. All revisions are referenced using this procedure. The original document will remain intact.

State of Oklahoma

Information Security Policy

Information is a critical State asset. Information is comparable with other assets in that there is a cost in obtaining it and a value in using it. However, unlike many other assets, the value of reliable and accurate information appreciates over time as opposed to depreciating. Shared information is a powerful tool and loss or misuse can be costly, if not illegal. The intent of this Security Policy is to protect the information assets of the State.

This Security Policy governs all aspects of hardware, software, communications and information. It covers all State Agencies as well as contractors or other entities who may be given permission to log in, view or access State information.

Definitions:

- *Information includes any data or knowledge collected, processed, stored, managed, transferred or disseminated by any method.*
- *The Owner of the information is the State Agency responsible for producing, collecting and maintaining the authenticity, integrity and accuracy of information.*
- *The Hosting State Agency has physical and operational control of the hardware, software, communications and data bases (files) of the owning Agency. The Hosting Agency can also be an Owner.*

The confidentiality of all information created or hosted by a State Agency is the responsibility of that State Agency. Disclosure is governed by legislation, regulatory protections and rules as well as policies and procedures of the owning State Agency. The highest of ethical standards are required to prevent the inappropriate transfer of sensitive or confidential information.

All information content is owned by the State Agency responsible for collecting and maintaining the authenticity, integrity and accuracy of the information. The objective of the owning State Agency is to protect the information from inadvertent or intentional damage, unauthorized disclosure or use according to the owning Agency's defined classification standards and procedural guidelines.

Information access is subject to legal restrictions and to the appropriate approval processes of the owning State Agency. The owning State Agency is responsible for maintaining current and accurate access authorities and communicating these in an agreed upon manner to the security function at the State Agency hosting the information. The hosting State Agency has the responsibility to adhere to procedures and put into effect all authorized changes received from the owning State Agencies in a timely manner.

Information security - The State Agency Director whose Agency collects and maintains (owns) the information is responsible for interpreting confidentiality restrictions imposed by laws and statutes, establishing information classification and approving information access. The hosting State Agency will staff a security function whose responsibility will be operational control and timely implementation of access privileges. This will include access authorization, termination of access privileges, monitoring of usage and audit of incidents. The State Agencies that access the systems have the responsibility to protect the confidentiality of information which they use in the course of their assigned duties.

Information availability is the responsibility of the hosting State Agency. Access to information will be granted as needed to all State Agencies to support their required processes, functions and timelines. Proven backup and recovery procedures for all data elements to cover the possible loss or corruption of system information are the responsibility of the hosting State Agency.

The hosting State Agency is responsible for securing strategic and operational control of its hardware, software and telecommunication facilities. Included in this mandate is the implementation of effective safeguards and firewalls to prevent unauthorized access to system processes and computing / telecommunication operational centers. Recovery plans are mandatory and will be periodically tested to ensure the continued availability of services in the event of loss to any of the facilities.

Development, control and communication of Information Security Policy, Procedures and Guidelines for the State of Oklahoma are the responsibility of the Office of State Finance. This Policy represents the minimum requirements for information security at all State Agencies. Individual agency standards for information security may be more specific than these state-wide requirements but shall in no case be less than the minimum requirements.

1.0 Introduction

This document states the Policy and outlines procedures, guidelines and best practices required for creating and maintaining a secure environment for the storage and dissemination of information.

It is critical that all agencies and their staff are fully aware of the Policy, procedures, guidelines and best practices and commit to protecting the information of the State. Common sense and high ethical standards are required to complement the security guidelines.

The Policy, procedures, guidelines and best practices outlined represent the minimum security levels required and must be used as a guide in developing a detailed security plan and additional policies (if required).

1.1 Background

The Policy, procedures, guidelines and best practices are developed to coincide with the introduction of CORE systems to be hosted by the Office of State Finance; however they are not restricted to the systems being introduced. The information Policy, procedures, guidelines and best practices apply to all agencies and are inclusive of their hardware facilities, software installations, communication networks / facilities as well as information.

1.2 Policy, Procedures, Guidelines

The Office of State Finance has, among other responsibilities, the mandate to establish minimum mandatory standards for information security and internal controls as well as contingency planning and disaster recovery (reference: Oklahoma Statute, Title 62.Public Finance, Chapter 1, Budget Law of 1947, Section 41.5a – Duties of Information Systems Division).

In reference to the responsibilities stated above, the Statute reads as follows:

“Such standards shall, upon adoption, be the minimum requirements applicable to all agencies. These standards shall be compatible with the standards established for the Oklahoma Government Telecommunications Network created in Section 1 of this act. Individual agency standards may be more specific than state-wide requirements but shall in no case be less than the minimum mandatory standards. Where standards required of an individual agency of the state by agencies of the federal government are more strict than the state minimum standards, such federal requirements shall be applicable.”

1.3 Audience

The Policy, procedures, guidelines and best practices are for distribution to all State agencies through their respective Security Representative who will then be responsible for communicating the details to State employees as well as contractors or other entities whose position responsibilities include the creation, maintenance, or access of State information residing on any computer system or platform. Appendix C assigns the primary responsibility of the procedures, guidelines and best practices to the User, Owning Agency, or Hosting Agency.

2.0 Information

Management of information requires a working set of procedures, guidelines and best practices that provide guidance and direction with regards to security. The primary focus is on the confidentiality and integrity of the information required for delivering information throughout the State.

2.1 Information Confidentiality

The overriding premise is that all information hosted or created by a State Agency is property of the State. As such, this information will be used solely for performance of position related duties. Any transfers or disclosures are governed by this rule.

The confidentiality of all information created or hosted by a State Agency is the responsibility of all State Agencies. *Disclosure is governed by legislation, regulatory protections, rules as well as policies and procedures of the State and of the owning State Agency*. The highest of ethical standards are required to prevent the inappropriate transfer of sensitive or confidential information.

Release of information is strictly for job related functions. Confidentiality is compromised when knowingly or inadvertently, information crosses the boundaries of job related activities.

Users must be required to follow good security practices in the selection and use of passwords. Passwords provide a means of validating a user's identity and thereby establish access rights to information processing facilities or services. All agency staff must be advised to:

- keep passwords confidential,
- avoid keeping a paper record of passwords, unless this can be stored securely,
- change passwords whenever there is any indication of possible system or password compromise,
- select quality passwords with a minimum length of eight characters which are:
    - easy to remember,
    - not based on anything somebody else could easily guess or obtain using person related information, e.g. names, telephone numbers and dates of birth etc.,
    - free of consecutive identical characters or all-numeric or all-alphabetical groups,
- change passwords at regular intervals (passwords for privileged accounts should be changed more frequently than normal passwords),
- avoid reusing or cycling old passwords,
- change temporary passwords at the first log-on,
- not include passwords in any automated log-on process, e.g. stored in a macro or function key, and
- not share individual user passwords.

2.2 Information Content

All information content hosted by a state agency is owned by and is the primary responsibility of the Agency responsible for collecting and maintaining the authenticity, integrity and accuracy of information. The objective of the owning State Agency is to protect the information from inadvertent or intentional damage as well as unauthorized disclosure or use according to the classification standards and procedural guidelines of the owning State Agency.

The following procedures must be followed by all State Agencies:

- All information content must reflect the actual state of affairs of the respective Agency.
- Changes in the status of personnel who have system access are entered in the system immediately and the appropriate authorization / change form sent to the hosting agency's Security Administration.
- In the event of a dismissal, the respective Agency is to call and notify the hosting agency's Security Administration immediately.

2.3 Information Access

Information access is subject to legal restrictions and to the appropriate approval processes of the owning State Agency. The owning State Agency is responsible for maintaining current and accurate access authorities and communicating these in an agreed upon manner to the security function at the State Agency hosting the information.

All agencies must designate a security representative whose role includes:

- communicating the information security Policy to all their respective agency's employees,
- communicating the appropriate procedures, guidelines and best practices to the responsible user, owner, or people directly responsible for hosting activities as indicated in Attachment C,
- granting, on behalf of their agency, user access to system functions, and
- reporting all deviations to the Policy, procedures, guidelines and best practices.

Procedures for the Security Administration function at the Hosting Agency are:

- Confirm set up to the Agency Director and the individual concerned via email when the set up is complete for the role of Security Representative.
- Confirm set up to the Security Representative and the individual concerned when the set up is complete for the use roles assigned. The email confirmation will include access rights assigned in the system.
- A daily report will be run by the hosting agency to list terminations. Security Administration at the hosting agency will lock the access privileges at the end of day on the effective date. This does not preclude the responsibility of all agencies to notify the hosting agency of terminations using agreed upon formal notice or by the phone and/or email in the case of dismissals.
- The hosting agency will run a weekly report of transfers and follow up with the agencies concerned if a change notification is not received.

- Users not using the system for 60 days will be automatically deactivated. Security Administration at the hosting agency will notify the respective user agency and will require an email or new activation form from the user agency's security representative to reactivate the individual.

The hosting State Agency has the responsibility to adhere to procedures and put into effect all authorized changes received from the owning State Agencies in a timely manner.

2.4 Information Security

The State Agency Director whose Agency collects and maintains (owns) the information is responsible for interpreting all confidentiality restrictions imposed by laws and statutes as well as establishing information classification and approving information access. The hosting State Agency will staff a Security Administration function whose responsibility will be operational control and timely implementation of access privileges.

System limitations may prevent all of the following procedures to be implemented, however, when possible, these rules apply:

- Passwords will be required to be a minimum of 8 characters long, containing at least one (1) numeric character.
- Passwords will expire in a maximum of 90 days.
- Passwords will be deactivated if not used for a period of 60 days.
- Passwords for a given user should not be reused in a 12 month period.

The State Agencies that access the systems have the responsibility to protect the confidentiality of information which they use in the course of their assigned duties.

2.5 Information Availability

Information availability is the responsibility of the hosting State Agency. Access to information will be granted as needed to all State Agencies to support their required processes, functions and timelines. Proven backup and recovery procedures for all information elements to cover the possible loss or corruption of system data are the responsibility of the hosting State Agency.

Required availability will vary with normal cycles of use (i.e. information is used constantly throughout the day, but is only periodically accessed during the evening by a backup process, becomes archival after the backup is complete). The following asset availability definitions should include a statement detailing over what time period the definition is accurate for (i.e. Constant during business hours, archival after year-end, etc.):

Availability	**Frequency of Use**	**Loss / Absence Impact**
Constant	*Accessed at all times*	*Immediate cessation of supported business functions*
Regular	*Accessed intermittently by individuals but constantly by all users as a group (i.e. email)*	*Interruption or degradation, but not cessation, of supported business functions*
Periodic	*Accessed intermittently, or on a schedule (i.e. year-end records)*	*Delay of supported business functions*
Archival	*Not normally accessible*	*Disruption of business support objectives*

The hosting State Agency will be responsible for:

- publishing a Service Level Agreement for all users of the system including response time, hours of availability and all other services contracted,
- ensuring all backups are current, secure and accessible,
- ensuring information facilities and data can be recovered, and
- ensuring adequate technical support for systems, data base access and operating systems.

3.0 Security Program Management

Managing information security within the State can be layered into three components:

- Central organization (Office of State Finance) is responsible for direction and leadership in all aspects of information security.
- Agencies that host data services are responsible for creating system specific policies and guidelines *to complement, but not contradict* those issued by the central organization.
- All agencies are required to develop procedures specific to their information and process flows to protect the integrity of information and guard against misuse or loss. This is not limited to, but includes computer based information systems.

3.1 Central Security Program

In regards to information services, the Office of State Finance will develop, maintain and communicate polices and guidelines for the protection of information assets including but not limited to hardware, software, information and communications. The Policy, Procedures, Guidelines and Best Practices will be mandatory for all agencies and represent the minimum standards that all agencies will adopt.

Minimum standards will be issued for:

- systems planning,
- systems development methodology,
- documentation,
- hardware requirements and compatibility,
- operating systems compatibility,
- software and hardware acquisition,
- information security and internal controls,
- data base compatibility, and
- contingency planning and disaster recovery.

3.2 Hosting Agency Security

Under the boundaries established by the minimum mandatory standards issued by the Office of State Finance, agencies hosting information and systems for their own use or for the use of other agencies will further develop, maintain and communicate polices and guidelines for the protection of information assets including but not limited to hardware, software, information and communications.

All hosting agencies will:

- follow a systems development methodology,
- create and maintain adequate documentation,
- develop hardware requirements and compatibility for review by the Office of State Finance,
- ensure operating systems compatibility,
- expand and apply information security and internal controls,
- ensure data base compatibility, and
- develop and test contingency planning and disaster recovery.

3.3 Agency Security

All agencies have the responsibility of protecting their information assets from disclosure, loss or misuse. As such all agencies are required to adhere to and have documented procedures for:

- security of information flow within their area of control,
- information retention,
- information disposal (including shredding and deletion of electronic information), and
- communication of information security Policy, procedures, guidelines and best practices monitoring adherence with polices.

3.4 Incident Management

Incident management responsibilities and procedures must be established by the hosting agency to ensure a quick, effective and orderly response to security incidents. Procedures must be established to cover all potential types of security incidents, including:

- information system failures and loss of service,
- denial of service,
- errors resulting from incomplete or inaccurate business information, and
- breaches of confidentiality.

In addition to normal contingency plans (designed to recover systems or services as quickly as possible), the procedures must also cover:

- analysis and identification of the cause of the incident,
- planning and implementation of remedies to prevent recurrence, if necessary,
- collection of audit trails and similar evidence,
- communication with those affected by or involved with recovery from the incident, and
- reporting the action to the security administration function at the hosting agency.

Audit trails and similar evidence must be collected and secured as appropriate, for:

- internal problem analysis,
- use as evidence in relation to a potential breach of contracts, policies, or regulatory requirements,
- use in the event of civil or criminal proceedings, e.g. under computer misuse or information protection, and
- use in negotiating for compensation from software and service suppliers.

Action to recover from security breaches and correct system failures should be carefully and formally controlled. The procedures must ensure that:

- only clearly identified and authorized staff are allowed access to live systems and information,
- all emergency actions taken are documented in detail,
- emergency action is reported to management and reviewed in an orderly manner, and

- the integrity of business systems and controls is confirmed with minimal delay.

3.5 Event Logging and Monitoring

Audit logs recording exceptions and other security-relevant events must be produced and kept for an agreed period to assist in future investigations and access control monitoring. Audit logs should include:

- user IDs,
- dates and times for log-on and log-off,
- terminal identity or location if possible,
- records of successful and rejected system access attempts, and
- records of successful and rejected data and other resource access attempts.

Certain audit logs may be required to be archived as part of the record retention procedures or because of requirements to collect evidence.

Procedures for monitoring use of information processing facilities must be established and the result of the monitoring activities reviewed regularly. Such procedures are necessary to ensure that users are only performing activities that have been explicitly authorized. The level of monitoring required for individual facilities should be determined by a risk assessment. Areas that should be considered include:

- Authorized access, including detail such as:
    - the user ID,
    - the date and time of key events,
    - the types of events,
    - the files accessed, and
    - the program/utilities used.
- All privileged operations, such as:
    - use of supervisor account,
    - system start-up and stop, and
    - I/O device attachment/detachment.
- Unauthorized access attempts, such as:
    - failed attempts,
    - access procedure violations and notifications for network gateways and firewalls, and
    - alerts from proprietary intrusion detection systems.
- System alerts or failures such as:
    - console alerts or messages,
    - system log exceptions, and
    - network management alarms.

4.0 Risk Management

Risk management encompasses risk assessment, risk mitigation as well as evaluation and assessment. The risk assessment process includes identification and evaluation of risks and risk impacts and recommendation of risk-reducing measures. Risk mitigation refers to prioritizing, implementing and maintaining the appropriate risk-reducing measures recommended from the risk assessment process. Through a continual evaluation process, the hosting agency is responsible for determining whether the remaining risk is at an acceptable level or whether additional security controls should be implemented to further reduce or eliminate the residual risk.

4.1 Risk Assessment

The hosting agency will be responsible for determining the likelihood of an adverse event, the threats to system resources, the vulnerability of the system and the impact such an adverse event may have.

To determine the likelihood of an adverse event, consider:

- Motivation
- Nature of the vulnerability
- Current controls

A threat needs, and cannot exist without a vulnerability. A vulnerability is a weakness that can be intentionally or accidentally triggered. Threats can be posed from a lot of sources, some of which are:

- System Intruders (hackers)
- Criminals
- Terrorists
- Espionage
- Insiders which could be malicious or a result of poor training

In identifying the vulnerabilities, consideration must be given to:

- Hardware
- Software
- Network
- System Interfaces
- Data and information
- People who support and use the system
- Information sensitivity

The impact of an adverse event is the:

- Loss of Integrity
- Loss of Availability
- Loss of Confidentiality

4.2 Risk Mitigation

All hosting agencies are responsible for reducing risk to all information assets. The following are options provided in analyzing the alternatives.

- Risk Assumption. To accept the potential risk and continue operating the IT system or to implement controls to lower the risk to an acceptable level.
- Risk Avoidance. To avoid the risk by eliminating the risk cause and/or consequence (e.g., forgo certain functions of the system or shut down the system when risks are identified).
- Risk Limitation. To limit the risk by implementing controls that minimizes the adverse impact of a threat exercising a vulnerability (e.g., use of supporting, preventive, detective controls).
- Risk Planning. To manage risk by developing a risk mitigation plan that prioritizes, implements and maintains controls.
- Research and Acknowledgment. To lower the risk of loss by acknowledging the vulnerability or flaw and researching controls to correct the vulnerability.
- Risk Transference. To transfer the risk by using other options to compensate for the loss, such as purchasing insurance.

5.0 Personnel / User Issues

Personnel awareness of the information security Policy, procedures, guidelines and best practices is the responsibility of all agencies. Adherence to the Policy, procedures, guidelines and best practices is the responsibility of all state agencies on behalf of their employees.

Information security must be adopted at all levels as a "norm" of job performance. Information systems and data are vulnerable. With constant re-enforcement and monitoring, individuals will accept their responsibility to protect the information assets of the State and relate their performance in this area to standards of performance.

The IT staff must be alert and trained in offensive and defensive methods to protect the State information assets. Adequate staffing and key position backup are essential to run and maintain a secure environment.

5.1 Staffing

Adequate staffing, training and backup is the responsibility of all hosting agencies. Each agency will be responsible for:

- ensuring qualifications meet position requirements,
- identifying roles that will impact operations when not filled, i.e. if the incumbent leaves or cannot perform the function,
- ensuring training is in place to keep key individuals current with the technology available in the marketplace (this is particularly important with regards to the Internet and data base controls), and
- documenting contingency plans if critical functions are not available.

5.2 Awareness / Training

Awareness is not training. The purpose of awareness presentations are simply to focus attention on security and are intended to allow individuals to recognize IT security concerns and respond accordingly. Awareness relies on reaching broad audiences, whereas training is more formal, having a goal of building knowledge and skills to facilitate job performance.

Effective IT security awareness presentations must be designed. Awareness presentations must be on-going, creative and motivational, with the objective of focusing attention so that the learning will be incorporated into conscious decision-making.

The Office of State Finance will be responsible for:

- communicating the minimum standards for all related policies and procedures,
- providing recommendations for best practices in selected areas related to information security, and
- providing all necessary information for the development of an awareness program by the agencies.

All state agencies will:

- create and present security awareness sessions for their staff members, and
- ensure all staff members have attended an awareness session.

All current employees as well as new employees or contractors when hired that have access to any information assets must be briefed by the hiring or contracting agency as follows:

- the access requirements of their position or contract,
- their responsibilities for safeguarding sensitive information and assets,
- all information security policies, procedures, guidelines and best practices, and
- a written document outlining the contents of the briefing and the date, which should be signed by the individual briefed acknowledging receipt of its contents.

5.3 Personal Computer Usage

The agency computers of the State are provided for job related activities. To this end, the hosting agency provides support in networking and information resources for its computing community.

All users are given access to computers for job related duties and this usage must remain in compliance with State and agency policies as well as all state and federal laws governing usage and communication of information. Failure to comply will result in the denial of access privileges and may for employees lead to disciplinary action up to and including dismissal. For contractors, it may lead to the cancellation of the contractual agreement. Litigation may ensue.

In the effort to protect the integrity of the statewide network and its systems, any proof of unauthorized or illegal use of any agency computer and/or its accounts will warrant the immediate access to these files, accounts and/or systems by the hosting agency's security and information systems staff and appropriate action will be taken.

Information Security Policy for computer usage prohibits the use of its resources to:

- Send email using someone else's identity (Email forgery).
- Take any action that knowingly will interfere with the normal operation of the network, its systems, peripherals and/or access to external networks.
- Install any system or software on the network without prior approval.
- Install any software systems or hardware that will knowingly install a virus, Trojan horse, worm or any other known or unknown destructive mechanism.
- Attempt IP spoofing.
- Attempt the unauthorized downloading, posting or dissemination of copyrighted materials.
- Attempt any unauthorized downloading of software from the Internet.
- Transmit personal comments or statements in a manner that may be mistaken as the position of the State.
- Access, create, transmit (send or receive), print or download material that is discriminatory, derogatory, defamatory, obscene, sexually explicit, offensive or harassing based on gender, race, religion, national origin, ancestry, age,

disability, medical condition, sexual orientation or any other status protected by state and federal laws.

Furthermore, it is the State's position that all messages sent and received, including personal messages and all information stored on the agency's electronic mail system, voicemail system or computer systems are State property regardless of the content. As such, the hosting agency reserves the right to access, inspect and monitor the usage of all of its technology resources including any files or messages stored on those resources at any time, in its sole discretion, in order to determine compliance with its policies, for purposes of legal proceedings, to investigate misconduct, to locate information or for any other business purpose.

5.4 Email Usage

Electronic mail (email) is a highly efficient form of modern communication media. Used appropriately, email provides people with a means to communicate thereby facilitating business contact. However, this convenience also tempts users to experiment or take advantage of this media, resulting in email of unwelcome types (collectively known along with other unwelcome activity as Net Abuse). The improper use of this email technology may jeopardize systems integrity, security and service levels. Access to email is provided to users to assist them to perform their work and their use of email must not jeopardize operation of the system or the reputation and/or integrity of the State.

Email accounts are made available to all agency staff that require the service for the performance of job related functions. The following statements apply:

- All email and associated system resources are the property of the State. Email is subject to the same restrictions on its use and the same review process as is any other government furnished resource provided for the use of employees. Its use and content may be monitored.
- Email usage must be able to withstand public scrutiny. Users must comply with all applicable legislation, regulations, policies and standards. This includes complying with copyright and license provisions with respect to both programs and data.
- While email is provided as a business tool to users, its reasonable, incidental use for personal purposes is acceptable. This use must not, however, detrimentally affect employee productivity, disrupt the system and/or harm the government's reputation.
- Users may not:
    - use email for commercial solicitation or for conducting or pursuing their own business interests or those of another organization,
    - use email to distribute hoaxes, chain letters or advertisements and/or send rude, obscene, threatening or harassing messages,
    - use email to distribute pornographic material or hate literature,
    - use email to harass other staff members,
    - use email to send executable programs or games,
    - use email to send potentially offensive material, and
    - propagate viruses knowingly or maliciously.

- Users must not send, forward and/or reply to large distribution lists concerning non-government business. In addition, users must consider the impact on the network when creating and using large, work-related distribution lists.
- Email is a record and therefore management of email must comply with existing legislation, regulations, policies and standards.
- Alleged inappropriate use of the email technology will be reviewed by the agency involved as well as the hosting agency on a case by case basis and may lead to disciplinary action up to and including dismissal. In respect to contractors, it may lead to cancellation of the contractual arrangement. In any of the cases, it may lead to litigation.

5.5 Internet / Intranet Security

The World Wide Web (WWW) is a system for exchanging information over the Internet. An Intranet is a proprietary network that is specific for an entity, such as the State.

At the most basic level, the Web can be divided in two principal components: Web servers, which are applications that make information available over the Internet (in essence publish information) and Web browsers (clients), which are used to access and display the information stored on the Web servers. The Web server is the most targeted and attacked host on most organizations' network. As a result, it is essential to secure Web servers and the network infrastructure that supports them.

The specific security threats to Web servers generally fall into one of the following categories:

- Malicious entities may exploit software bugs in the Web server, underlying operating system or active content to gain unauthorized access to the Web server. Examples of unauthorized access are gaining access to files or folders that were not meant to be publicly accessible or executing privileged commands and/or installing software on the Web server.
- Denial of Service attacks may be directed to the Web server denying valid users an ability to use the Web server for the duration of the attack.
- Sensitive information on the Web server may be distributed to unauthorized individuals.
- Sensitive information that is not encrypted when transmitted between the Web server and the browser may be intercepted.
- Information on the Web server may be changed for malicious purposes. Web site defacement is a commonly reported example of this threat.
- Malicious entities may gain unauthorized access to resources elsewhere in the organization's computer network via a successful attack on the Web server.
- Malicious entities may attack external organizations from a compromised Web server, concealing their actual identities and perhaps making the organization from which the attack was launched liable for damages.
- The server may be used as a distribution point for illegal copies software attack tools, or pornography, perhaps making the organization liable for damages.

The hosting agency is responsible for the Web server. Some examples of controls to protect from unauthorized access or modification are:

- install or enable only necessary services,
- install Web content on a dedicated hard drive or logical partition,
- limit uploads to directories that are not readable by the Web server,
- define a single directory for all external scripts or programs executed as part of Web content,
- disable the use of hard or symbolic links,
- define a complete Web content access matrix that identifies which folders and files within the Web server document directory are restricted and which are accessible (and by whom), and
- use host-based intrusion detection systems and/or file integrity checkers to detect intrusions and verify Web content.

Maintaining a secure Web server is the responsibility of the hosting agency and involves the following steps:

- configuring, protecting and analyzing log files,
- backing up critical information frequently,
- maintaining a protected authoritative copy of the organization's Web content,
- establishing and following procedures for recovering from compromise,
- testing and applying patches in a timely manner, and
- testing security periodically.

A firewall environment must be employed to perform the following general functions:

- filter packets and protocols,
- perform inspection of connections,
- perform proxy operations or selected applications,
- monitor traffic allowed or denied by the firewall, and
- provide authentication to users using a form of authentication that does not rely on static, reusable passwords that can be sniffed.

The hosting agency responsible for Internet security will:

- Keep operational systems and applications software up to date. Because software systems are so complex, it is common for security-related problems to be discovered only after the software has been in widespread use. Although most vendors try to address known security flaws in a timely manner, there is normally a gap from the time the problem is publicly known, the time the vendor requires to prepare corrections and the time you install the update. This gap gives potential intruders an opportunity to take advantage of this flow and mount an attack on computers and networks. To keep this time interval as short as possible, it is required to stay aware of:
    - announcements of security-related problems that may apply,
    - immediate actions to reduce exposure to the vulnerability, such as disabling the affected software and
    - permanent fixes from vendors.
- Restrict only essential network services and operating system on the host server.
    - Ensure that only the required set of services and applications are installed on the host server. Either do not install unnecessary

services or turn the services off and remove the corresponding files (and any other unnecessary files) from the host.

- Configure computers for file backup.
- Protect computers from viruses and programmed threats.
- Allow only appropriate physical access to computers.
- Design, implement and monitor an effective firewall system.

6.0 Help Desk Management

A world class Help Desk is characterized by responsiveness, knowledge, feedback and improvement. The speed at which issues are resolved, the number of requests handled by the first level in support, the follow-up with the user community on status, security and the monitoring of performance with the goal of continuous improvement are the characteristics that separate a progressive, secure, mission critical operation from the ordinary, reactive operation.

The mandate of the help desk function should include:

- Adherence to all policies and procedures as published.
- Recommendation of new and/or changes to policies and procedures.
- Ownership of all the calls until reassigned or routed.
- Performance of all front line tasks such as password resets, printer resets, etc.
- Routing of system or technical queries to the knowledge expert responsible.
- Reporting on and monitor calls.
- Reporting and escalation of all incidents of suspicious activity or violations of security.

The following is a list of suggested reports required for managing the Help Desk.

- Incident Report – Content: all known information, status. Schedule: Immediately. Distribution: Security Administration at hosting Agency.
- Call Activity – Content: calls by type agency, severity average resolution time. Schedule: Monthly. Distribution: Management.
- Open Calls – Content: calls by user agency, severity, ranked by oldest time open. Schedule: Weekly. Distribution: Help Desk, Knowledge Experts.
- Daily Activity – Content: calls received by time of day. Schedule: Daily. Distribution: Help Desk.
- Repeat Calls - Content: number of calls ranked by user (over 3) showing Agency, type. Schedule: Monthly. Distribution: Knowledge Expert and Director of the agency generating the calls.

6.1 Support Calls

Call handling and routing is the responsibility of the hosting agency’s help desk function. This function should present a standard front to all users of their services including telephone calls, emails and voice mails. Information on all calls will be logged and violations in security or suspicious activity will be reported immediately to the appropriate designated authority.

The help desk function will verify the identity of the caller by:

- Obtaining their name.
- Verifying a question and answer submitted on a Systems Access Authorization Request.
- Requesting additional information, such as:
  - User ID (*interchangeable with Log-on ID)*
  - Agency

  - Phone number

6.2 Password Resets

Password resets are the responsibility of the hosting state agency's help desk function. Identities of requestors will be verified by the help desk, logged and confirmed back to the user at the respective State Agency.

It is the responsibility of the requestor from all State Agencies, in requesting a password reset, to confirm their identity. This may be accomplished by:

- Providing their name.
- Answering a unique question and answer submitted on sign up, such as: place of birth, mother's maiden name, etc.).
- Providing additional information as may be requested, such as:
  - Agency
  - Phone number

The responsibility of the host agency's Help Desk is to:

- Confirm the identity of the requestor.
- Report all suspicious activity to the security Administrator immediately. Discrepancies in answers, inability to provide the correct User ID, frequent requests for changes to the same User ID, or obvious password sharing constitute security breaches and will be reported.
- Reset the password.
- Log details of the call.
- Confirm the password reset to the user registered to the User ID via email.
- Report activity monthly to each State Agency involved.

6.3 Voice Mail Security

The voice mail feature of many PBXs can be a particularly vulnerable feature. This is because voice mail is typically used to let someone store voice messages at a central location by calling in from any inside or outside line and then retrieve the messages from any inside or outside line. It also grants the general public access to the PBX system.

In retrieving messages, the target extension and a password are usually required to gain access to the messages. Since the target extension is usually easy to determine, the only significant restriction to an adversary is the password. Once an adversary determines a target user's password all messages left for the target user are accessible to the adversary. The adversary could also delete messages from the target user's mailbox to prevent an important message from getting to the target user. Some guidelines to secure the contents of voice mail include the following:

- Default and obvious passwords must be changed at initial log-in. The target user's extension is easily known. Default passwords established at system initialization time may never have been changed.
- Fixed length passwords are more vulnerable than variable length passwords. Variable length passwords can be terminated by a special key such as the # or * key. If not, the passwords would probably be of fixed length and it reduces the

number of random combinations that may be tried before a correct password is found.

- Non-terminated password entry should be avoided. Some systems accept a continuous string of digits, granting entry when the correct password sequence is entered. By not requiring a password entry to be terminated, the length of the average sequence needed to guess a four-digit password is reduced by a factor of five.
- A complete password must be entered before an incorrect password is rejected. If it is rejected on the first incorrect digit, sequential guessing becomes much more practical. For example, on such a system that has a fixed password length of four and uses the digits 0-9, it would take at most 40 sequential attempts to guess a password. On a system that required all four digits to be entered at most 10,000 guesses would be required.
- Disallow access to external lines via the Voice Mail system.

7.0 Physical and Environmental Security

The hosting agency has the responsibility for documentation, execution, monitoring and testing of a physical security plan for both computer and telecommunication assets. This physical security plan would evaluate the risks from potential losses due to:

- physical destruction or theft of physical assets,
- loss or destruction of information and program files,
- theft of information,
- theft of indirect assets, and
- delay or prevention of computer processing.

Included in the plan would be measures for reducing the possibility of a loss and must address:

- changes in the environment to reduce exposure,
- measures to reduce the effect of a threat,
- improved control procedures,
- early detection, and
- contingency plans.

7.1 Operations Center

The following are guidelines of the action items for establishing, implementing and maintaining a physical security program at the hosting agency:

- conduct a risk analysis (refer to section 4),
- determine local natural disaster probabilities,
- protect supporting utilities
- ensure computer reliability,
- provide physical protection
- implement procedural security,
- plan for contingencies,
- develop security awareness, and
- validate the program.

7.2 Operations Monitoring

Hosting agencies can monitor security effectiveness by comparing performance to the metrics in a service level agreement and incidents that occur in violation of security policies, procedures, guidelines and best practices.

Guidelines for hosting agencies in establishing a service level agreement are:

- hours of system availability,
- hours of application system support,
- hours of technical support,
- off hours support,
- average system response time, and
- other metrics as suitable for agency specific applications.

Hosting agencies should have a goal of achieving 99.9%+ of the metrics established in the service level agreement. Failure to achieve these targets could be an indication of security breaches.

Insofar as incidents are concerned, both offensive and defensive actions to protect the security of physical assets should be considered routine. Examples of offensive actions include:

- routine changes of passwords,
- develop an escalation procedure of incidents,
- routine changes of locks or combinations to the facilities,
- have more than one person knowledgeable for critical functions,
- rotate shifts or people between functions,
- monitor all incursion attempts,
- install latest versions of firewall software,
- maintain 24x7 vendor contact list,
- routine backups,
- off site storage of system information and programs,
- redundant components, lines for critical systems, and
- testing of recovery procedures.

Examples of defensive actions include:

- report and action all deviations to security policies, procedures, guidelines and best practices,
- shut down any infected machine immediately,
- disconnect any problem areas from the network,
- revoke privileges of users violating policies,
- assign severity to an issue and escalate, and
- acquire knowledgeable resources.

7.3 Back up of Information

Back-up copies of essential business information and software must be taken regularly. Adequate backup facilities should be provided to ensure that all essential business information and software can be recovered following a disaster or media failure. Back-up arrangements for individual systems should be regularly tested to ensure that they meet the requirements of business continuity plans. The following controls must be considered:

- A minimum level of back-up information, together with accurate and complete records of the back-up copies and documented restoration procedures, should be stored in a remote location at a sufficient distance to escape any damage from a disaster at the main site. At least three generations or cycles of back-up information should be retained for important business applications.
- Back-up information should be given an appropriate level of physical and environmental protection consistent with the standards applied at the main site. The controls applied to media at the main site should be extended to cover the back-up site.
- Back-up media should be regularly tested, where practicable, to ensure that they can be relied upon for emergency use when necessary.

- Restoration procedures should be regularly checked and tested to ensure that they are effective and that they can be completed within the time allotted in the operational procedures for recovery.
- The retention period for essential business information and also any requirement for archive copies to be permanently retained should be determined.

7.4 Access Control

Logical and physical access controls are required to ensure the integrity of the information and physical assets.

The following guidelines for controlling logical access should be implemented by all state hosting agencies:

- document and adhere to procedures for granting, modifying and revoking access,
- install detection mechanisms for unauthorized access attempts,
- timeout a session after 15 minutes of inactivity, and
- revoke access after an inactivity period of 60 days.

Physical access control guidelines for all agencies include:

- all telecommunication and computer related equipment are to be in a secured, locked environment,
- access codes for secure environments must be changed at least every 60 days or in the event of a individual departing that previously had access,
- account for all keys issued for those facilities using this method and replace locking mechanism when a key is missing,
- when the system permits, log all accesses and retain, and
- secure all peripherals such as air conditioning, generators, etc.

7.5 Network

Unsecured connections to network services can affect the whole organization. Users must only have direct access to the services that they have been specifically authorized to use. This control is particularly important for network connections to sensitive or critical business applications or to users in high-risk locations, e.g. public or external areas that are outside the organization's security management and control.

Procedures concerning the use of networks and network services should cover:

- the networks and network services which are allowed to be accessed,
- authorization procedures for determining who is allowed to access which networks and networked services, and
- management controls and procedures to protect the access to network connections and network services.

The path from the user terminal to the computer service must be controlled. Networks are designed to allow maximum scope for a sharing of resources and flexibility of routing. These features may also provide opportunities for unauthorized access to business applications, or unauthorized use of information facilities. Incorporating controls that restrict the route between a user terminal and the computer services its user is authorized to access, e.g. creating an enforced path can reduce such risks. The objective of an enforced path is to prevent any users selecting routes outside the route between the user terminal and the services that the user is authorized to access. This usually requires the implementation of a number of controls at different points in the route. The principle is to limit the routing options at each point in the network, through predefined choices.

The following methods should be implemented to limit the path to a service:

- allocating dedicated lines or telephone numbers,
- automatically connecting ports to specified application systems or security gateways,
- limiting menu and submenu options for individual users,
- preventing unlimited network roaming,
- enforcing the use of specified application systems and/or security gateways for external network users,
- actively controlling allowed source to destination communications via security gateways, e.g. firewalls, and
- restricting network access by setting up separate logical domains, e.g. virtual private networks, for user groups within the organization.

External connections provide a potential for unauthorized access to business information, e.g. access by dial-up methods. Therefore, access by remote users must be subject to authentication. There are different types of authentication method, some of these provide a greater level of protection than others, e.g. methods based on the use of cryptographic techniques can provide strong authentication. It is important to determine from a risk assessment the level of protection required. This is needed for the appropriate selection of an authentication method.

Authentication of remote users should be achieved using one of the following techniques:

- a cryptographic based technique,
- hardware tokens,
- a challenge/response protocol,
- dedicated private lines or a network user address checking, and
- call-back procedures.

Dial-back procedures and controls, e.g. using dial-back modems, can provide protection against unauthorized and unwanted connections to an organization's information processing facilities. This type of control authenticates users trying to establish a connection to an organization's network from remote locations. When using this control an organization should not use network services which include call forwarding or, if they do, they should disable the use of such features to avoid weaknesses associated with call forwarding. It is also important that the call back process includes ensuring that an actual disconnection on the organization's side occurs. Otherwise, the remote user could hold the line open pretending that call back verification has occurred. Call back procedures and controls should be thoroughly tested for this possibility.

A facility for automatic connection to a remote computer could provide a way of gaining unauthorized access to a business application. Connections to remote computer systems must therefore be authenticated. This is especially important if the connection uses a network that is outside the control of the organization's security management.

Node authentication can serve as an alternative means of authenticating groups of remote users where they are connected to a secure, shared computer facility.

Access to diagnostic ports must be securely controlled. Many computers and communication systems are installed with a dial-up remote diagnostic facility for use by maintenance engineers. If unprotected, these diagnostic ports provide a means of unauthorized access. They should therefore be protected by an appropriate security mechanism, e.g. a key lock and a procedure to ensure that they are only accessible by arrangement.

Networks are increasingly being extended beyond traditional organizational boundaries as business partnerships are formed that may require the interconnection or sharing of information processing and networking facilities. Such extensions will increase the risk of unauthorized access to already existing information systems that use the network, some of which might require protection from other network users because of their sensitivity or criticality. In such circumstances, controls must be introduced in networks to segregate groups of information services, users and information systems.

The security of large networks should be controlled by dividing them into separate logical network domains, e.g. an organization's internal network domains and external network domains, each protected by a defined security perimeter. Such a perimeter should be implemented by installing a secure gateway between the two networks to be interconnected to control access and information flow between the two domains. This gateway should be configured to filter traffic between these domains and to block unauthorized access in accordance with the organization's access control procedures. An example of this type of gateway is what is commonly referred to as a firewall. The criteria for segregation of networks into domains should be based on the access control procedures and access requirements and also take account of the relative cost and performance impact of incorporating suitable network routing or gateway technology.

The connection capability of users must be restricted in shared networks, in accordance with the access control procedures.

Such controls should be implemented through network gateways that filter traffic by means of pre-defined tables or rules. The restrictions applied should be based on the access procedures and requirements of the business applications and should be maintained and updated accordingly. Examples of applications to which restrictions should be applied are:

- electronic mail,
- one-way file transfer,
- both-ways file transfer,
- interactive access, and

- network access linked to time of day or date.

Shared networks must have routing controls to ensure that computer connections and information flows do not breach the access control procedures of business applications. This control is essential for networks shared with third party (non-organization) users.

Routing controls should be based on positive source and destination address checking mechanisms. Network address translation is also a very useful mechanism for isolating networks and preventing routes to propagate from the network of one organization into the network of another. They can be implemented in software or hardware. Implementers should be aware of the strength of any mechanisms deployed.
A wide range of public or private network services is available, some of which offer value added services. Network services may have unique or complex security characteristics.

A clear description of the security attributes of all network services used by the organization must be provided.

7.6 Electronic Commerce Security

Electronic commerce can involve the use of electronic data interchange (EDI), electronic mail and on line transactions across public networks such as the Internet. Electronic commerce is vulnerable to a number of network threats which may result in fraudulent activity, contract dispute and disclosure or modification of information and must be protected. The following issues must be resolved:

- Authentication. What level of confidence should the customer and trader require in each others claimed identity?
- Authorization. Who is authorized to set prices, issue or sign key trading documents? How does the trading partner know this?
- Contract and tendering processes. What are the requirements for confidentiality, integrity and proof of dispatch and receipt of key documents and the non-repudiation of contracts?
- Pricing information. What level of trust can be put in the integrity of the advertised price list and the confidentiality of sensitive discount arrangements?
- Order transactions. How is the confidentiality and integrity of order, payment and delivery address details and confirmation of receipt, provided?
- Vetting. What degree of vetting is appropriate to check payment information supplied by the customer?
- Settlement. What is the most appropriate form of payment to guard against fraud?
- Ordering. What protection is required to maintain the confidentiality and integrity of order information and to avoid the loss or duplication of transactions?
- Liability. Who carries the risk for any fraudulent transactions?

Electronic commerce arrangements between trading partners should be supported by a documented agreement which commits both parties to the agreed terms of trading, including details of authorization. Other agreements with information service and value added network providers may be necessary.

Consideration should be given to the resilience to attack of the host used for electronic commerce and the security implications of any network interconnection required for its implementation.

7.7 Mobile Computing

Formal procedures must be in place and appropriate controls must be adopted to protect against the risks of working with mobile computing facilities, in particular in unprotected environments. For example such procedures should include the requirements for:

- physical protection,
- access controls,
- cryptographic techniques,
- back-ups, and
- virus protection.

Procedures should also include rules and advice on connecting mobile facilities to networks and guidance on the use of these facilities in public places.

Care should be taken when using mobile computing facilities in public places, meeting rooms and other unprotected areas outside of the organization's premises. Protection should be in place to avoid the unauthorized access to or disclosure of the information stored and processed by these facilities, e.g. using cryptographic techniques.

It is important that when such facilities are used in public places care is taken to avoid the risk of overlooking by unauthorized persons. Procedures against malicious software should be in place and be kept up to date. Equipment should be available to enable the quick and easy back-up of information. These back-ups should be given adequate protection against, e.g., theft or loss of information.

Suitable protection should be given to the use of mobile facilities connected to networks.

Remote access to business information across public network using mobile computing facilities should only take place after successful identification and authentication and with suitable access control mechanisms in place.

Mobile computing facilities should also be physically protected against theft especially when left, for example, in cars and other forms of transport, hotel rooms, conference centers and meeting places. Equipment carrying important, sensitive and/or critical business information should not be left unattended and, where possible, should be physically locked away, or special locks should be used to secure the equipment.

7.8 Remote Computing

Remote computing uses communications technology to enable staff or agencies to work remotely from a fixed location outside of their organization. Suitable protection of the remote computing site should be in place against, e.g., the theft of equipment and information, the unauthorized disclosure of information, unauthorized remote access to the organization's internal systems or misuse of facilities. It is important that remote computing is both authorized and controlled by management and that suitable arrangements are in place for this way of working.

Procedures must be developed from best practices to authorize and control remote computing activities. Agencies should only authorize remote computing activities if they are satisfied that appropriate security arrangements and controls are in place and that these comply with the agency's security procedures. The following should be considered:

- the existing physical security of the remote computing site, taking into account the physical security of the building and the local environment,
- the communications security requirements, taking into account the need for remote access to the organization's internal systems, the sensitivity of the information that will be accessed and passed over the communication link and the sensitivity of the internal system, and
- the threat of unauthorized access to information or resources from other people using the accommodation.

The controls and arrangements to be considered include:

- the provision of suitable equipment and storage furniture for the remote computing activities,
- a definition of the work permitted, the hours of work, the classification of information that may be held and the internal systems and services that the user is authorized to access,
- the provision of suitable communication equipment, including methods for securing remote access,
- physical security,
- the provision of hardware and software support and maintenance,
- the procedures for back-up and business continuity, and
- audit and security monitoring.

7.9 External Facilities

The use of an external contractor to manage information processing or communication facilities may introduce potential security exposures, such as the possibility of compromise, damage or loss of data at the contractor's site.

Prior to using external facilities, the risks must be identified and appropriate controls agreed with the contractor and incorporated into the contract. Particular issues that should be addressed include:

- identifying sensitive or critical applications better retained in-house,
- obtaining the approval of business application owners,
- implications for business continuity plans,
- security standards to be specified and the process for measuring compliance,
- allocation of specific responsibilities and procedures to effectively monitor all relevant security activities, and
- responsibilities and procedures for reporting and handling security incidents.

7.10 Encryption

Encryption should be applied to protect the confidentiality of sensitive or critical information.

Based on a risk assessment, the required level of protection should be identified taking into account the type and quality of the encryption algorithm used and the length of cryptographic keys to be used.

Specialist advice should be sought to identify the appropriate level of protection, to select suitable products that will provide the required protection and the implementation of a secure system of key management. In addition, legal advice may need to be sought regarding the laws and regulations that might apply to the organization's intended use of encryption.

Procedures for the use of cryptographic controls for the protection of information must be developed and followed. Such procedures are necessary to maximize benefits and minimize the risks of using cryptographic techniques and to avoid inappropriate or incorrect use.

When developing procedures the following should be considered:

- the management guidelines on the use of cryptographic controls across the organization,
- including the general principles under which business information should be protected,
- the approach to key management, including methods to deal with the recovery of encrypted information in the case of lost, compromised or damaged keys,
- roles and responsibilities, e.g. who is responsible for: the implementation of the procedures; the key management,
- how the appropriate level of cryptographic protection is to be determined, and
- the standards to be adopted for the effective implementation throughout the organization (which solution is used for which business processes).

8.0 Business Continuity

Information Technology facilities and systems are vulnerable to a variety of disruptions, some of which are short term (measured in minutes and hours) and others lasting for a day or longer. The intent of Business Continuity Planning is to be alert and ready to sustain an organization's processes during and following a significant unforeseen disruption in services caused by disasters and security failures.

Business continuity should begin by identifying events that can cause interruptions to business processes, e.g. equipment failure, flood and fire. This should be followed by a risk assessment to determine the impact of those interruptions (both in terms of magnitude and recovery time frame). Both of these activities should be carried out with full involvement from owners of business resources and processes. This assessment considers all business processes, and is not limited to the information processing facilities.

A strategy plan, based on appropriate risk assessment, must be developed for the overall approach to business continuity.

All hosting State Agencies will develop contingency plans for each major application or general support system to meet the needs of critical IT operations in the event of a disruption extending beyond a given time period. The length of the time period may vary with the system or facility involved. The procedures for execution of such a capability will be documented in a formal contingency plan, be reviewed annually and updated as necessary by the hosting agency. The procedures must account for differential daily backups and complete weekly backups to be conducted and sent to a designated off-site facility. As well, the plans should assign specific responsibilities to designated staff or positions to facilitate the recovery and/or continuity of essential IT functions. Designated personnel will be trained to execute contingency procedures. An annual test of the recovery procedures will be conducted.

Business continuity management should include controls to identify and reduce risks, limit the consequences of damaging incidents, and ensure the timely resumption of essential operations.

8.1 Contingency Plan

A contingency plan provides the documented organizational plan to mitigate risks of business interruption and minimize the impact of any disruption of service. It must maintain instructions for achieving a full or minimally acceptable set of business objectives in the absence of assets, through cost-effective strategies to provide replacements for assets as they become unavailable. The Plan must involve advance planning and preparations to respond to external circumstances as determined by a risk assessment and continue to provide a pre-determined acceptable level of business functionality. Procedures and guidelines must be defined, implemented, tested and maintained to ensure continuity of organizational services in the event of a disruption. Each contingency plan is unique and must be tailored to organization's requirements; it must be flexible enough to allow additions, modifications and maintenance. The plan should minimize dependency on individuals for interpretation and implementation – in the event of emergency, key personnel may not be available. It must ensure completeness and establish critical decisions. Always make sure that the plan remains current. The following questions must be answered:

- What risks the organization is facing in terms of their likelihood and their impact, including an identification and prioritization of critical business processes?
- How long can the enterprise operate without this asset?
- What is the impact interruptions are likely to have on the business (it is important that solutions are found that will handle smaller incidents, as well as serious incidents that could threaten the viability of the organization), and establishing the business objectives of information processing facilities?
- What is the maximum acceptable delay before which temporary systems must be made available?
- What is the minimum time in which temporary systems may be expected to become available?
- At what minimally acceptable level of functionality can the enterprise operate?
- How long can the enterprise operate at a minimally acceptable level of performance?
- At what point can the enterprise begin to resume normal operations?
- At what point must the enterprise begin to resume normal operations?

A Contingency Plan should contain the roles, responsibilities and procedures for restoring a system or facility following a major disruption. The following guidelines represent the stages to be followed in preparing and executing a Contingency Plan:

- Documentation – A plan must be documented, tested and communicated. Included in the plan should be a mission, a scope of what is included and not included assumptions, requirements, staffing and responsibilities.
- Notification/Activation – Internally within IT, the notification, timing and paths should be documented. There should only be one voice talking for the recovery team for communication and escalation outside the boundaries of IT. Immediately following damage assessment, the plan is activated.
- Recovery – The sequence of recovery activities should be documented in procedures. These activities are to restore operations which may be in temporary locations or with incomplete data.
- Reconstitution - Restoring facilities and systems to the “norm” will include testing and proof of operations viability.

- What equipment / facilities are expected to be unavailable?
- What is the timing of the disruption?
- What records, files and materials may / may not be expected to be protected from destruction?
- What resources are available or required following the event?
    - Applications / Processes

- Functionality / Capacity
- Equipment / Infrastructure
- Staff / Skills
- Connectivity / Network
- Data Sources
- Facilities / Services / Physical Premises
- Transportation
- Documentation / Reference material
- Security Policies and Procedures
- Specific Policies and Procedures
- Authorization

Following is a list of considerations that, at a minimum, must be addressed in creating contingency plans:

- What additional security measures are required to protect assets in the planning, execution and maintenance of procedures to assure business continuity?
- What degree of functionality is still available at the main facility, if any?
- Availability of staff to perform critical functions defined within the plan.
- Ability of staff to be notified and report to the backup site(s) to execute contingency plans.
- Backup files and recovery methods.
- Off-site storage facilities and materials availability.
- Disaster recovery plan.
- Suitability of subsets of the overall plan, to be used to recover from minor interruptions.
- Availability of an alternate facility.
- Off-site availability of critical forms and supplies, either at an alternate facility or off-site storage.
- Existence of a backup site for processing the organization’s work.
- Availability of long distance and local communications lines.
- Quality of surface transportation in from local to remote sites.
- Ability of vendors to perform according to their general commitments to support the organization in a disaster.
- Provisions for staff while at off-site location (food, water, telephones, beds, etc.)

This list of considerations is not all inclusive and must be added to as appropriate.

General requirements of contingency plans must include:

- Definitions of conditions under which the Business Recovery Strategy must be implemented.
- Recovery point objective stages.
- Recovery time objective stages.
- Security preservation checklist.
- Task Assignments.
- Post-event Recovery Analysis.
- Required resources, by priority.
- Required recovery time / levels of availability of resources.
- Documentation of normal and response procedures.

Refer to the considerations outlined in Appendix D.

8.2 Disaster Recovery Plan

A Disaster Recovery Plan is intended to maintain critical business processes in the event of the loss of any of the following areas for an extended period of time:

- desktop computers and portable systems,
- servers,
- Web sites,
- local area networks,
- wide area networks,
- distributed systems, and
- mainframe systems.

Teams should be formed to address each of the areas indicated consisting of a team lead and designate as well as key knowledge personnel required for that particular area. All contact information must be available for IT management, team members, all IT personnel and designated business unit management. When available, this information should include:

- work telephone number,
- pager number,
- home telephone number,
- cellular telephone number,
- work email address,
- home email address, and
- home address.

Upon receiving the information of a serious incident any member of management can invoke the Plan. Depending on the nature of the incident a command center will be established and appropriate teams mobilized. Management and the team leads are responsible for contacting all required personnel. Appendix B represents a sample crisis team organization and roles corresponding with potential disaster situations. All roles would have designates in the event one or more individuals are unavailable.

Communications to the IT department is the responsibility of Management and the Team Lead. In respect to external communications, it is extremely important that there is a single point of disclosure in order to ensure accurate and timely updates. The following roles and individuals must be determined and documented:

- Upwards, within the affected agency’s organization.
- Outwards to affected agencies.
- Outwards to the public.

Hard copies of the Plan must be:

- stored off site at a secure location,
- stored at the personal residence of the team leads,
- stored at the personal residence of all IT managers and directors, and
- stored on a secure internet site.

As soon as an emergency is detected:

- Identify the problem and,
    - Notify emergency services in cases of physical threats to personnel or facilities,
    - Notify the IT Director and his alternate.
    - Notify the appropriate team leads. In the event of a mainframe disaster, notify all team leads.
    - Notify vendors and business partners.
- Evacuate the premises if there are concerns of personal safety. All personnel should:
    - be aware of evacuation routes and
    - have in possession or be aware of notification numbers.
- Reduce any exposure:
    - In the event of air conditioning failure, *(this usually involves powering down the systems at a temperature determined by the tolerances set by the manufacturer).*
    - In the event of fire, *(this usually involves the automatic releasing of fire retardant, cutting of power, notification to emergency services and evacuation).*
    - In the event of electrical failure, *(If a UPS and generator are available, usually the only action is to monitor fuel levels of the generator. If a UPS only is available, shut down procedures should begin and be terminated with at least 20% of rated capacity left).*
    - In the event of flood, water or wind damage, *(this usually involves the normal powering down all systems if possible. If not, the immediate cut off of power is required, followed by notification to emergency services and evacuation).*
    - In the event of malicious intrusion, *(this usually involves the immediate isolation of affected hardware from all networks and connectivity. Usually the extent of exposure and damage is not immediately known so the immediate isolation of all network links is recommended and processing on affected facilities halted pending analysis by crisis teams).*
- Initiate backup site procedures:
    - The Plan Coordinator establishes a command and control center *(usually an onsite and offsite center have been previously identified and the necessary computer and communication links are readily available)*.
    - The Plan Coordinator ensures all team leaders are notified (*usually it is the responsibility of the Team Lead to get in touch with all team members).*
    - The Plan Coordinator notifies the off site storage facility that a contingency event has occurred and to ship the necessary materials as determined in the damage assessment to the alternate site.

  - The Plan Coordinator notifies the alternate site that a contingency event has occurred and to prepare the facility for the organization’s arrival.
  - Both upward and outward communication on status is the responsibility of the Plan Coordinator *(usually set times are pre-established such as: immediate after 1 hour after 3 hours, etc. or at major milestones such as problem determination, resolution plan, when planned resumption of services is known and start up of services is accomplished).*
  - The Plan Coordinator is responsible for managing expectations.
- Initiate recovery at the alternate site:
  - Contingency plan is followed using documented recovery points and defined priorities.
  - The Plan Coordinator reviews responsibilities with all team members and establishes recovery logs.
  - Recovery goals and procedures are established and prioritized by the Plan Coordinator.

The Disaster Plan appendices should include:

- Personnel Contact List
- Vendor Contact List
- Equipment and Specifications.
- Service Level Agreements.
- Related Contracts.
- Standard Operating Procedures.

8.3 Business Recovery Strategy

A Business Recovery Strategy provides the documented organizational plan to restore full business functionality as quickly and as cost-effectively as possible. The Business Recovery Strategy is initiated as soon as the enterprise is deemed able to resume normal operations following a disaster.

The Business Recovery Strategy must involve advance planning and preparations to recover from external circumstances. Recovery strategies must be created, implemented, tested and maintained to ensure restoration of organizational services in the event of an interruption.

A “worst case scenario” must be the basis for developing the plan, where the worst-case scenario is the destruction of the main or primary facility. Because the plan is written based on this premise, less critical situations can be handled by using subsets of the plan, with minor (if any) alterations required. Recovery from, or mitigation of a scenario should not be considered an all-or-nothing proposition. Many stages may be required, each with its own success conditions, before a ‘final’ state of continuity or recovery is reached.

Specific goals of the Business Recovery Strategy must include:

- Complete service functionality recovery objectives, in stages, by delay, duration and degree.
- Details of processes already in place to recover from an incident.
- Details of what degree of business functionality they may be expected to restore.
- In what length of time existing process may be expected to restore service.
- Requirements to bridge from existing processes to sufficient processes.
- Lead time to secure additional resources.

The Business Recovery Strategy must include detailed, step-by-step instructions for how to replace / restore the following, in appropriate sequence:

- Applications / Processes
- Functionality / Capacity
- Equipment / Infrastructure
- Staff / Skills
- Execution Duration / Delay
- Connectivity / Network
- Data Sources
- Facilities / Services / Physical Premises
- Transportation
- Documentation / Reference material

9.0 Data Center Management

Related specifically to security of information and data center management, the pace of change, the reality of the World Wide Web and the increasing numbers of internal and external portals demand constant monitoring with both offensive and defensive strategies.

9.1 Operating Procedures

The operating procedures identified by security procedures should be documented and maintained. Operating procedures should be treated as formal documents and changes authorized by management.

The procedures should specify the instructions for the detailed execution of each job including the following:

- processing and handling of information,
- scheduling requirements, including interdependencies with other systems, earliest job start and latest job completion times,
- instructions for handling errors or other exceptional conditions, which might arise during job execution, including restrictions on the use of system utilities,
- support and owner contacts in the event of unexpected operational or technical difficulties,
- special output handling instructions, such as the use of special stationery or the management of confidential output, including procedures for secure disposal of output from failed jobs, and
- system restart and recovery procedures for use in the event of system failure.

Documented procedures should also be prepared for system housekeeping activities associated with information processing and communication facilities, such as computer start-up and close-down procedures, back-up, equipment maintenance, computer room and mail handling management and safety.

9.2 Operational Change Control

Changes to information processing facilities and systems must be controlled. Inadequate control of changes to information processing facilities and systems is a common cause of system or security failures. Formal management responsibilities and procedures should be in place to ensure satisfactory control of all changes to equipment, software or procedures.

Operational programs should be subject to strict change control. When programs are changed an audit log containing all relevant information should be retained. Changes to the operational environment can impact applications. Wherever practicable, operational and application change control procedures should be integrated.

In particular, the following controls must be implemented:

- identification and recording of significant changes,
- assessment of the potential impact of such changes,
- formal approval procedure for proposed changes,

- communication of change details to all relevant persons, and
- procedures identifying responsibilities for aborting and recovering from unsuccessful changes.

9.3 Segregation of Duties

Duties and areas of responsibility must be segregated in order to reduce opportunities for unauthorized modification or misuse of information or services.

Small agencies may find this method of control difficult to achieve, but the principle should be applied as far as is possible and practicable. Whenever it is difficult to segregate, other controls such as monitoring of activities, audit trails and management supervision must be implemented. It is important that security audit remains independent.

Care should be taken that no single person can perpetrate fraud in areas of single responsibility without being detected. The initiation of an event should be separated from its authorization.

The following controls must be implemented:

- It is important to segregate activities which require collusion in order to defraud, e.g. raising a purchase order and verifying that the goods have been received.
- If there is a danger of collusion, then controls need to be devised so that two or more people need to be involved, thereby lowering the possibility of conspiracy.

9.4 Separation of Development and Operational Facilities

Development and testing facilities must be separated from operational facilities. Rules for the transfer of software from development to operational status should be defined and documented.

Development and test activities can cause serious problems, e.g. unwanted modification of files or system environment or of system failure. The level of separation that is necessary, between operational, test and development environments, to prevent operational problems should be considered. A similar separation should also be implemented between development and test functions. In this case, there is a need to maintain a known and stable environment in which to perform meaningful testing and to prevent inappropriate developer access.

Where development and test staff have access to the operational system and its information, they may be able to introduce unauthorized and untested code or alter operational information. On some systems this capability could be misused to commit fraud, or introduce untested or malicious code. Untested or malicious code can cause serious operational problems.

Developers and testers also pose a threat to the confidentiality of operational information. Development and testing activities may cause unintended changes to software and information if they share the same computing environment. Separating development, test and operational facilities is therefore desirable to reduce the risk of accidental change or unauthorized access to operational software and business information.

The following controls should be considered:

- Development and operational software should, where possible, run on different computer processors, or in different domains or directories.
- Development and testing activities should be separated the best way possible.
- Compilers, editors and other system utilities should not be accessible from operational systems.
- Different log-on procedures should be used for operational and test systems, to reduce the risk of error. Users should be encouraged to use different passwords for these systems and menus should display appropriate identification messages.
- Development staff should only have access to operational passwords where controls are in place for issuing passwords for the support of operational systems. Controls should ensure that such passwords are changed after use.

9.5 Systems Planning and Acceptance

To minimize the risk of systems failure:

- Advance planning and preparation are required to ensure the availability of adequate capacity and resources.
- Projections of future capacity requirements should be made, to reduce the risk of system overload.
- The operational requirements of new systems should be established, documented and tested prior to their acceptance and use.

9.6 Capacity Planning

Capacity demands must be monitored and projections of future capacity requirements made to ensure that adequate processing power and storage are available. These projections should take account of new business and system requirements and current and projected trends in the organization's information processing.

Mainframe computers require particular attention, because of the much greater cost and lead time for procurement of new capacity. Operations managers of mainframe services should monitor the utilization of key system resources, including processors, main storage, file storage, printers and other output devices and communications systems. They should identify trends in usage, particularly in relation to business applications or management information system tools.

These managers should use this information to identify and avoid potential bottlenecks that might present a threat to system security or user services and plan appropriate remedial action.

9.7 Systems Acceptance

Acceptance criteria for new information systems, upgrades and new versions must be established and suitable tests of the system carried out prior to acceptance. Operations managers should ensure that the requirements and criteria for acceptance of new systems are clearly defined, agreed, documented and tested.

The following controls should be considered:

- performance and computer capacity requirements,
- error recovery and restart procedures and contingency plans,
- preparation and testing of routine operating procedures to defined standards,
- agreed set of security controls in place,
- effective manual procedures,
- business continuity arrangements as required,
- evidence that installation of the new system will not adversely affect existing systems, particularly at peak processing times, such as month end,
- evidence that consideration has been given to the effect the new system has on the overall security of the organization, and
- training in the operation or use of new systems.

For major new developments, the operations function and users should be consulted at all stages in the development process to ensure the operational efficiency of the proposed system design. Appropriate tests should be carried out to confirm that all acceptance criteria are fully satisfied.

9.8 Operations and Fault Logging

Operational staff must maintain a log of their activities. Logs should include as appropriate:

- system starting and finishing times,
- system errors and corrective action taken,
- confirmation of the correct handling of data files and computer output, and
- the name of the person making the log entry.

Faults must be reported and corrective action taken. Faults reported by users regarding problems with information processing or communications systems should be logged. There should be clear rules for handling reported faults including:

- review of fault logs to ensure that faults have been satisfactorily resolved, and
- review of corrective measures to ensure that controls have not been compromised and that the action taken is fully authorized.

9.9 Management of Removable Computer Media

Appropriate operating procedures must be established to protect documents, computer media (tapes, disks, cassettes, etc.), input/output data, and system documentation from damage, theft and unauthorized access. The following procedures should be followed:

- If no longer required, the previous contents of any re-usable media that are to be removed from the organization should be erased.
- Authorization should be required for all media removed from the organization and a record of all such removals maintained.
- All media should be stored in a safe, secure environment, in accordance with manufacturers' specifications.

- All procedures and authorization levels should be clearly documented.

9.10 Disposal of Media

Formal procedures for the secure disposal of media should be established to minimize this risk. The following controls should be considered:

- Media containing sensitive information should be stored and disposed of securely and safely, e.g. by incineration or shredding or emptied of information for use by another application within the organization.
- The following list identifies items that might require secure disposal:
  - paper documents,
  - voice or other recordings,
  - output reports,
  - one-time-use printer ribbons,
  - magnetic tapes,
  - removable disks or cassettes,
  - optical storage media (all forms and including all manufacturer software distribution media),
  - program listings,
  - test information, and
  - system documentation.
- It may be easier to arrange for all media items to be collected and disposed of securely, rather than attempting to separate out the sensitive items.
- Disposal of sensitive items should be logged where possible in order to maintain an audit trail.
- Disposal of certain hardware must conform to the current EPA requirements or other relevant legislation in effect.

9.11 Exchanges of Information and Software

Exchanges of information and software between organizations should be controlled and should be compliant with any relevant legislation.

Exchanges should be carried out on the basis of agreements. Procedures and standards to protect information and media in transit must be established. The business and security implications associated with electronic data interchange, electronic commerce and electronic mail and the requirements for controls should be considered.

Agreements, some of which must be formal, must be established for the electronic or manual exchange of information and software between organizations. The security content of such an agreement should reflect the sensitivity of the business information involved. Agreements on security conditions should include:

- responsibilities for controlling and notifying transmission, dispatch and receipt,
- procedures for notifying sender, transmission, dispatch and receipt,
- minimum technical standards for packaging and transmission,
- courier identification standards,
- responsibilities and liabilities in the event of loss of information,

- information and software ownership and responsibilities for information protection, software copyright compliance and similar considerations,
- technical standards for recording and reading information and software, and
- any special controls that may be required to protect sensitive items, such as cryptographic.

Information can be vulnerable to unauthorized access, misuse or corruption during physical transport, for instance when sending media via the postal service or via courier. As such, media being transported must be protected from unauthorized access, misuse or corruption.

9.12 Publicly Available Systems

Information on a publicly available system, e.g. information on a Web server accessible via the Internet, may need to comply with laws, rules and regulations in the jurisdiction in which the system is located or where trade is taking place. There must be a formal authorization process before information is made publicly available and the integrity of such information must be protected to prevent unauthorized modification.

Software, data and other information requiring a high level of integrity, made available on a publicly available system, should be protected by appropriate mechanisms, e.g. digital signatures. Electronic publishing systems, especially those that permit feedback and direct entering of information, should be carefully controlled so that:

- information is obtained in compliance with any information protection legislation,
- information input to and processed by, the publishing system will be processed completely and accurately in a timely manner,
- sensitive information will be protected during the collection process and when stored, and
- access to the publishing system does not allow unintended access to networks to which it is connected.

9.13 Use of System Utilities

Most computer installations have one or more system utility programs that might be capable of overriding system and application controls. Use of these system utility programs must be restricted and tightly controlled. The following controls should be considered:

- use of authentication procedures for system utilities,
- segregation of system utilities from applications software,
- limitation of the use of system utilities to the minimum practical number of trusted authorized users,
- authorization for ad hoc use of systems utilities,
- limitation of the availability of system utilities, e.g. for the duration of an authorized change,
- logging of all use of system utilities,
- defining and documenting of authorization levels for system utilities, and
- removal of all unnecessary software based utilities and system software.

9.14 Monitoring Systems Access and Use

Systems should be monitored to detect deviation from access control procedures and record system events to provide evidence in case of security incidents. System monitoring allows the effectiveness of controls adopted to be checked.

Audit logs recording exceptions and other security-relevant events must be produced and kept for a period defined by the agency and within the mandate of both federal and State legislation to assist in future investigations and access control monitoring. Audit logs should also include:

- user IDs,
- dates and times for log-on and log-off,
- terminal identity or location if possible,
- records of successful and rejected system access attempts, and
- records of successful and rejected data and other resource access attempts.

Certain audit logs may be required to be archived as part of the record retention procedures or because of requirements to collect evidence.

Procedures for monitoring use of information processing facilities must be established and the result of the monitoring activities reviewed regularly. Such procedures are necessary to ensure that users are only performing activities that have been explicitly authorized. The level of monitoring required for individual facilities should be determined by a risk assessment. Areas that should be included are:

- authorized access, including detail such as:
    - the user ID,
    - the date and time of key events,
    - the types of events,
    - the files accessed, and
    - the program/utilities used.
- all privileged operations, such as:
    - use of supervisor account,
    - system start-up and stop, and
    - I/O device attachment/detachment.
- unauthorized access attempts, such as:
    - failed attempts,
    - access procedure violations and notifications for network gateways and firewalls, and
    - alerts from proprietary intrusion detection systems.
- system alerts or failures such as:
    - console alerts or messages,
    - system log exceptions, and
    - network management alarms.

The result of the monitoring activities should be reviewed regularly. The frequency of the review should depend on the risks involved. Risk factors that should be considered include:

- the criticality of the application processes,

- the value, sensitivity or criticality of the information involved,
- the past experience of system infiltration and misuse and
- the extent of system interconnection (particularly public networks).

A log review involves understanding the threats faced by the system and the manner in which these may arise. System logs often contain a large volume of information, much of which is extraneous to security monitoring. To help identify significant events for security monitoring purposes, the copying of appropriate message types automatically to a second log and/or the use of suitable system utilities or audit tools to perform file interrogation should be considered. When allocating the responsibility for log review a separation of roles should be considered between the person(s) undertaking the review and those whose activities are being monitored.

Particular attention should be given to the security of the logging facility because if tampered with it can provide a false sense of security. Controls should aim to protect against unauthorized changes and operational problems including:

- the logging facility being de-activated,
- alterations to the message types that are recorded,
- log files being edited or deleted, and
- log file media becoming exhausted and either failing to record events or overwriting itself.

9.15 Control of Operational Software

Control must be applied to the implementation of software on operational systems.
To minimize the risk of corruption of operational systems, the following controls should be considered:

- The updating of the operational program libraries should only be performed by the nominated librarian upon appropriate management authorization.
- Operational systems should only hold executable code.
- Executable code should not be implemented on an operational system until evidence of successful testing and user acceptance is obtained and the corresponding program source libraries have been updated.
- An audit log should be maintained of all updates to operational program libraries.
- Previous versions of software should be retained as a contingency measure.

Vendor supplied software used in operational systems should be maintained at a level supported by the supplier. Any decision to upgrade to a new release should take into account the security of the release, i.e. the introduction of new security functionality or the number and severity of security problems affecting this version. Software patches should be applied when they can help to remove or reduce security weaknesses.

9.16 Access Control to Source Library

In order to reduce the potential for corruption of computer programs, strict control must be maintained over access to program source libraries.

- Program source libraries should not be held in operational systems.
- A program librarian should be nominated for each application.

- IT support staff should not have unrestricted access to program source libraries.
- Programs under development or maintenance should not be held in operational program source libraries.
- The updating of program source libraries and the issuing of program sources to programmers should only be performed by the nominated librarian upon authorization from the IT support manager for the application.
- Program listings should be held in a secure environment.
- An audit log should be maintained of all accesses to program source libraries.
- Old versions of source programs should be archived, with a clear indication of the precise dates and times when they were operational, together with all supporting software, job control, data definitions and procedures.
- Maintenance and copying of program source libraries should be subject to strict change control procedures.

9.17 Change Control Procedures

The implementation of changes must be strictly controlled by the use of formal change control procedures to minimize the risk of system corruption. These formalized change controls must be enforced. They should ensure that security and control procedures are not compromised, that programmers are given access to only those units required for their work and that formal approvals are obtained. Changing application software can impact the operational environment. Whenever practical, application and operational change procedures should be integrated. These processes should include:

- maintaining a record of agreed authorization levels,
- ensuring changes are submitted by authorized personnel,
- reviewing controls and procedures to ensure they will not be compromised by the changes submitted,
- identifying all the software, databases and hardware that require change,
- obtaining formal approval before work commences,
- ensuring the changes are carried out to minimize any possible disruptions,
- ensuring the system documentation is current,
- maintaining version control on all updates,
- maintaining an audit trail of all change requests,
- ensuring that operational documentation and user procedures reflect the new environment, and
- ensuring that the changes are implemented without business disruption.

Test environments should be separated from development and production environments.

9.18 Restrictions on Changes to Software

Modification to software packages must be discouraged and essential changes controlled. Only when deemed essential, should the packages be modified. The following points should be considered:

- the possibility of controls and processes included in the base software being compromised,
- the necessity of obtaining the vendor’s consent,

- the possibility of the vendor including the changes into the base offering, and
- the impact of incorporating these changes in future releases of the base software.

9.19 Intrusion Detection Systems (IDS)

Network IDS utilize traffic analysis to compare session data against a known database of popular application attack signatures. On detection, the network IDS can react by logging the session alerting the administrator, terminating the session and even re-configuring the firewall or router to block selected traffic

Host IDS compare application / internal service log events against a known database of security violations and custom policies. If a breach of policy occurs, the host IDS can react by logging the action alerting the administrator and in some cases stopping the action prior to execution.

Application-Level IDS rely upon custom applications to log unauthorized or suspect activity and / or produce an alert. An example of an Application-Level IDS would be a Web application which maintains its own internal user / password system. Attempts to circumvent this system would not be noticed by a Network IDS, or recorded by a Host IDS.

9.20 Controls on Malicious Software

Detection and prevention controls to protect against malicious software and appropriate user awareness procedures must be implemented. Protection against malicious software should be based on security awareness appropriate system access and change management controls.
The following procedures should be implemented:

- compliance with software licenses and prohibiting the use of unauthorized software,
- protection against risks associated with obtaining files and software either from or via external networks or on any other medium, indicating what protective measures should be taken,
- installation and regular update of anti-virus detection and repair software to scan computers and media either as a precautionary control or on a routine basis,
- regular reviews of the software and information content of systems supporting critical business processes—the presence of any unapproved files or unauthorized amendments should be formally investigated,
- verification of files on electronic media of uncertain or unauthorized origin, or files received over un-trusted networks, for viruses before use,
- verification of any electronic mail attachments and downloads for malicious software before use—this check may be carried out at different places, e.g. at electronic mail servers, desk top computers or when entering the network of the organization,
- assignment of responsibilities to deal with the virus protection on systems, training in their use, reporting and recovering from virus attacks,

- appropriate business continuity plans for recovering from virus attacks, including all necessary data and software back-up and recovery arrangements,
- verification of all information relating to malicious software and ensure that warning bulletins are accurate and informative, and
- verification that qualified sources, e.g. reputable journals, reliable Internet sites or anti-virus software suppliers are used to differentiate between hoaxes and real viruses.

Staff should be made aware of the problem of hoaxes and what to do on receipt of them. These controls are especially important for network file servers supporting large numbers of workstations.

9.21 Firewalls

Firewalls' functionality must be documented and detail how they manage security policy as applied to network traffic and how they maintain internal security.

System documentation must detail the following:

- Purpose / Business rationale for the system
- Services offered, including business rationale
- Rationale for the choice of platform, operating system, components and configuration.
- Adjacent or integrated systems.
- Modifications to the default system software configuration
- Installed software
- Installed software configuration
- Installed hardware
- Installed hardware configuration
- Support contracts
- Software licenses
- Hardware lease details
- Procedures for shutdown, restart and recovery
- System maintenance schedule

9.22 External Facilities Management

The use of an external contractor to manage information processing facilities may introduce potential security exposures, such as the possibility of compromise, damage, or loss of data at the contractor's site. Prior to using external facilities management services, the risks must be identified and appropriate controls agreed with the contractor, and incorporated into the contract.

Particular issues that should be addressed include:

- identifying sensitive or critical applications better retained in-house,
- obtaining the approval of business application owners,
- implications for business continuity plans,
- security standards to be specified, and the process for measuring compliance,

- allocation of specific responsibilities and procedures to effectively monitor all relevant security activities, and
- responsibilities and procedures for reporting and handling security incidents.

10.0 Legal Requirements

All security related aspects of information processing may be subject to statutory or contractual security requirements. Each agency must be aware of their responsibilities as dictated by legislation and other legal commitments particularly as they apply to the information systems and practices required by the federal and state governments. All agencies should put in place the appropriate procedures to ensure compliance with legal considerations.

10.1 Software Copyright

Proprietary software products are usually supplied under a license agreement that limits the use of the products to specified machines and may limit copying to the creation of back-up copies only. The following controls should be implemented:

- publishing software copyright compliance procedures which define the legal use of software and information products,
- maintaining awareness of the software copyright and acquisition procedures and giving notice of the intent to take disciplinary action against staff who breach them,
- maintaining appropriate asset registers,
- maintaining proof and evidence of ownership of licenses, master disks, manuals, etc.,
- implementing controls to ensure that any maximum number of users permitted is not exceeded,
- carrying out checks that only authorized software and licensed products are installed,
- providing procedures for maintaining appropriate license conditions, and
- providing procedures for disposing or transferring software to others.

10.2 Protection of Information

Important records of an organization must be protected from loss, destruction and falsification. Some records may need to be securely retained to meet statutory or regulatory requirements as well as to support essential business activities. The time period and information content for retention may be set by federal and state laws or regulations.

Records should be categorized into record types, such as accounting records, database records, transaction logs audit logs and operational procedures, each with details of retention periods and type of storage media, e.g. paper, microfiche, magnetic, optical. Any related cryptographic keys associated with encrypted archives or digital signatures, should be kept securely and made available to authorized persons when needed.

Consideration should be given to the possibility of degradation of media used for storage of records. Storage and handling procedures should be implemented in accordance with Manufacturer’s recommendations.

Wherever electronic storage media are chosen, procedures to ensure the ability to access information (both media and format readability) throughout the retention period should be included, to safeguard against loss due to future technology change.

The system of storage and handling should ensure clear identification of records and of their statutory or regulatory retention period. It should permit appropriate destruction of records after that period if they are not needed by the organization.
To meet these obligations, the following steps should be taken within an organization:

- Guidelines should be issued on the retention, storage, handling and disposal of records and information.
- A retention schedule should be drawn up identifying essential record types and the period of time for which they should be retained.
- An inventory of sources of key information should be maintained.
- Appropriate controls should be implemented to protect essential records and information from loss, destruction and falsification.

10.3 Privacy of Personal Information

In many cases, legislation controls the processing and transmission of personal information (generally information on living individuals who can be identified from that information). Such controls impose responsibilities on those collecting, processing and disseminating personal information.
Controls must be applied to protect personal information in accordance with relevant legislation. Compliance with information protection legislation requires appropriate management structure and control. It is the responsibility of the owner of the information to ensure the information is protected and that there is awareness by all users of the information protection principles defined in the relevant legislation.

11.0 Compliance with Security Policy

Agencies must ensure that all security procedures within their area of responsibility are documented and carried out correctly. All areas within the organization may be subject to regular review to ensure compliance with security procedures and standards. These should include the following:

- information systems,
- systems providers,
- owners of information and information assets,
- hosting agencies of information and information assets, and
- users.

Both the owning and hosting agencies should support regular reviews of the compliance of their systems with the appropriate security procedures, standards and any other security requirements. All variances must be documented.

APPENDIX A: GLOSSARY

Backup: A copy of files and programs made to facilitate recovery if necessary.

Business Continuity: The predetermined set of instructions or procedures that describe how an organization's business functions will be sustained during and after a significant disruption of the normal business environment.

Business Recovery Strategy: The documentation of a predetermined set of instructions or procedures that describe how business processes will be restored after a significant disruption to the normal business environment has occurred.

Cold Site: A backup facility that has the necessary electrical and physical components of a computer facility, but does not have the computer equipment in place. The site is ready to receive the necessary replacement computer equipment in the event that the user has to move from their main computing location to an alternate site.

Contingency Plan: Management policy and procedures designed to maintain or restore business operations, including computer operations, possibly at an alternate location, in the event of emergencies, system failures or disaster.

Critical Application: An application that requires special attention to security because of the risk and magnitude of the harm resulting from the loss, misuse or unauthorized access to, or modification of, the information in the application. A breach in a critical application might comprise many individual application programs and hardware, software and telecommunications components. Critical applications can be either a major software application or a combination of hardware and software in which the only purpose of the system is to support a specific mission-related function.

Disaster Recovery Plan: An information technology plan designed to restore operability of the target system, application, telecommunication, or computer facility after a major hardware or software failure or destruction of facilities.

Disruption: An unplanned event that causes the general system or major application to be inoperable for an unacceptable length of time (e.g., minor or extended power outage, extended unavailable network, equipment or facility damage or destruction, or corruption of files by accidental or malicious intent).

Distributed System: A distributed system is an interconnected set of multiple autonomous processing units, configured to exchange and process information to complete a single business function. To the user a distributed system appears to be a single source. Distributed systems use the client-server relationship model to make the application more accessible to users in different locations.

Environmental Considerations: Those physical or tangible factors that affect the performance of, or compliance with, a given procedure or process.

Facilities: Interconnected information resources that share common functionality. They include hardware, software, information, information applications and communications.

Functional Considerations: Those process or procedure factors that affect the performance of, or compliance with, a given function.

Hosting Agency: The Hosting State Agency has physical and operational control of the hardware, software, communications and data bases (files) of the owning Agency. The Hosting Agency can also be an Owner.

Hot Site: A fully operational off-site information processing facility equipped with hardware and system software to be used in the event of a disaster.

Incident: A malicious attack against an organization's IT systems. It is normally associated with cyber attacks but includes any unauthorized violation of policies and procedures.

Information: Any data or knowledge collected, processed, stored, managed, transferred or disseminated by any method.

Intrusion Detection System: The function of an Intrusion Detection System (IDS) is to monitor and analyze captured activity data and issue alerts when unauthorized activity is detected. The functionality of the IDS must be documented as well as details on how the IDS discovers, filters and reports events based on guidelines set by security policy.

Local Area Network (LAN): A local area network (LAN) is a data communications network owned by a single organization. It can be as small as two PCs attached or can include hundreds of users and multiple servers.

Mainframe: A mainframe is a multi-user computer designed to meet the computing needs of a large organization. The term was created to describe the large central computers developed in the late 1950s and 1960s to process bulk accounting and information management functions. Mainframe systems store most, if not all data in a central location rather than dispersing data among multiple machines as with distributed systems.

Owner: The Owner of the information is the State Agency responsible for producing, collecting and maintaining the authenticity, integrity and accuracy of information.

Risk Management: Risk management is the ongoing process of assessing, controlling and mitigating the risks to information systems and technologies. Risk management should prevent or reduce the likelihood of damage to its information resources through implementation of security controls to protect a system or technologies against natural, human and environmental threats. Risk management should encompass actions to reduce or limit the consequences of risks in the event they disrupt a system or technological component.

Security Representative: An individual designated by a state agency to approve user access, communicate security policies, procedures, guidelines and best practices to agency personnel, and report on all deviations to security policies, procedures, guidelines and best practices.

Server: A server is a computer that runs software to provide access to a resource or part of the network and network resources, such as disk storage, printers and network applications. A server can be any type of computer running a network operating system. A server may be a standard PC or it can be a large computer containing multiple disk drives and a vast amount of memory that will allow the computer to process multiple, concurrent requests.

Service Level Agreement: A documented commitment on products, services or service levels to be provided. This must be agreed upon by the provider as well as the recipient and serves to manage expectations and monitor performance.

Shared Network: A network shared with third party or non-organizational users.

System: A generic term used for briefness to mean either a major application or a general support system.

Systems Access Authorization Request: Documented authorization for an individual's system access signed and approved by the requesting manager, the designated Security Representative and the Owner.

System Development Life Cycle: The scope of activities associated with a system, encompassing the system's initiation, development and acquisition, implementation, operation and maintenance and ultimately its disposal that instigates another system initiation.

Vetting: Verification of information or individuals associated with the process or task assigned.

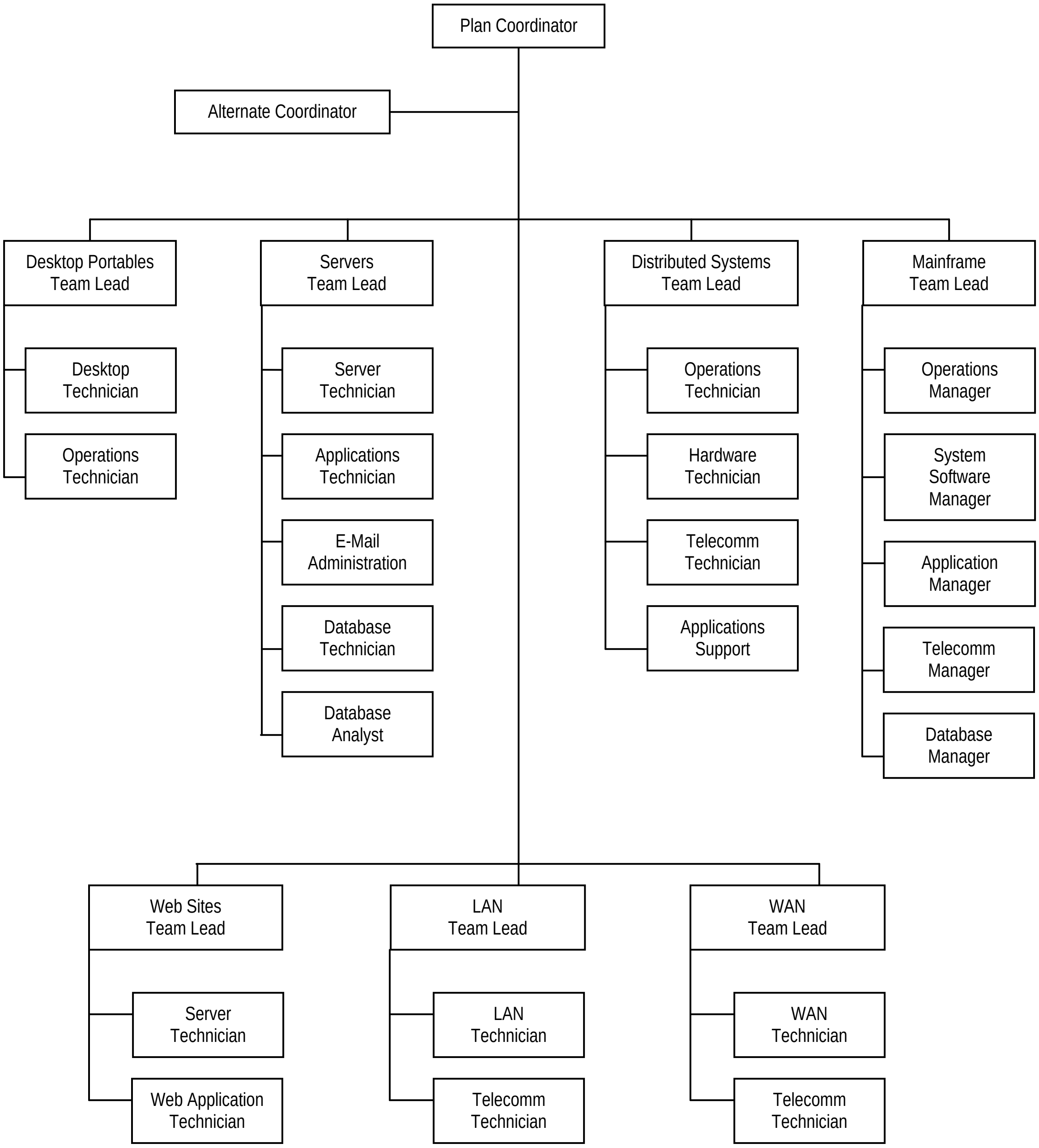
Warm Site: An environmentally conditioned workspace that is partially equipped with IT and telecommunications equipment to support relocated IT operations in the event of a significant disruption.

Web Site: A Web site is used for information dissemination on the Internet or an intranet. The Web site is created in Hypertext Markup Language (HTML) code that may be read by a Web browser on a client machine. A Web site is hosted on a computer (Web server) that serves Web pages to the requesting client browser. The Web server hosts the components of a Web site (e.g., pages, scripts, programs and multimedia files) and serves them using the Hypertext Transfer Protocol (HTTP). Web sites can present static or dynamic content. A Web site can be either internal to an organization (an intranet) or published to the public over the Internet.

Wide Area Network (WAN): A wide area network (WAN) is a data communications network that consists of two or more LANs that are dispersed over a wide geographical area. Communications links, usually provided by a public carrier, enable one LAN to interact with other LANs.

APPENDIX B: SAMPLE CRISIS TEAM ORGANIZATION

The following sample illustrates crisis team compositions insofar as skills mix required for the disaster recovery components. Alternates should be assigned for all critical skills.



APPENDIX C: RESPONSIBILITY GRID

The following grid outlines the primary responsibilities (**in bold)** for all the security considerations listed in the Policy, Procedures, and Guidelines document. In addition, the considerations are applied to the major components listed under disaster recovery. This does not preclude the fact that all State employees and agencies share in all responsibilities pertaining to information security.

Security Considerations	**Users**	**Own Agcy**	**Host Agcy**	Desktops	Servers	Web Sites	LAN	WAN	Dist. Sys.	Mainframe
Information Confidentiality	**X**	**X**	**X**	x	x	x	x	x	x	x
Information Content		**X**		x	x	x			**x**	x
Information Access		**X**	**X**	x	x	x				x
Information Security		**X**		x	x	x			x	x
Information Availability			**X**	x	x	x	x	x	x	x
Hosting Agency Security			**X**	x	x	x	x	x	x	x
Agency Security	**X**	**X**	**X**	x	x	x	x	x	x	x
Incident Management		**X**	**X**	x	x	x	x	x	x	x
Event Logging and Monitoring			**X**		x	x	x	x	x	x
Risk Assessment			**X**	x	x	x	x	x	x	x
Risk Mitigation			**X**	x	x	x	x	x	x	x
Staffing			**X**		x	x	x	x	x	x
Awareness / Training		**X**	**X**	x	x	x	x	x	x	x
Personal Computer Usage	**X**	**X**		x						
Email Usage	**X**	**X**	**X**	x			x	x		
Internet/ Intranet Security			**X**		x	x				
Support Calls			**X**		x	x	x	x	x	x
Password Resets		**X**			x				x	x
Voice Mail Security		**X**	**X**					x		
Operations Center			**X**	x	x	x	x	x		x
Operations Monitoring			**X**		x	x	x	x	x	x
Back Up of Information	**X**		**X**	x	x				x	x
Access Control			**X**	x	x	x	x	x	x	x
Network			**X**				x	x	x	
Electronic Commerce Security			**X**		x		x	x	x	x
Mobile Computing	**X**		**X**	x					x	
Remote Computing			**X**	x	x	x		x	x	
External Facilities			**X**	x	x	x	x	x	x	x
Encryption		**X**		x	x		x	x	x	x
Contingency Plan		**X**	**X**		x	x	x	x	x	x
Disaster Recovery Plan		**X**	**X**		x	x	x	x	x	x
Business Recovery Strategy		**X**	**X**		x	x	x	x	x	x

Security Considerations	**Users**	**Own Agcy**	**Host Agcy**	Desktops	Servers	Web Sites	LAN	WAN	Dist. Sys.	Mainframe
Operating Procedures			**X**		x	x	x	x	x	x
Operational Change Control			**X**		x	x	x	x	x	x
Segregation of Duties			**X**		x				x	x
Separation of Development & Operational Facilities			**X**		x				x	x
Systems Planning & Acceptance			**X**		x				x	x
Capacity Planning			**X**	x	x		x	x	x	x
Systems Acceptance			**X**		x	x	x	x	x	x
Fault Logging			**X**		x				x	x
Management of Removable Computer Media		**X**	**X**		x				x	x
Disposal of Media	**X**	**X**	**X**	x	x				x	x
Exchanges of Information & Software		**X**	**X**		x		x	x	x	x
Publicly Available Systems		**X**			x	x				x
Use of System Utilities			**X**		x				x	x
Monitoring Systems Access & Use		**X**	**X**	x	x	x	x	x	x	x
Control of Operational Software			**X**		x				x	x
Access Control to Source Library			**X**		x					x
Change Control Procedures			**X**		x				x	x
Restrictions on Changes to Software			**X**		x				x	x
Intrusion Detection Systems (IDS)			**X**		x				x	x
Controls on Malicious Software			**X**		x				x	x
Firewalls		**X**	**X**	x	x				x	x
External Facilities Management			**X**	x	x	x	x	x	x	x
Software Copyright	**X**	**X**	**X**	x	x				x	x
Protection of Information	**X**	**X**	**X**	x	x	x	x	x	x	x
Privacy of Personal Information	**X**	**X**	**X**	x	x				x	x
Compliance with Security Policy	**X**	**X**	**X**	x	x	x	x	x	x	x

APPENDIX D: CONTINGENCY PLAN CONSIDERATIONS

Considerations	**Portables**	**Servers**	**Web Sites**	**LAN**	**WAN**	**Dist. Sys**	**Mainframe**
Maintain an up to date inventory of hardware and software.	x	x				x	x
Standardize hardware, software, and peripherals.	x	x				x	x
Coordinate with security policies and procedures.	x	x	x	x	x	x	x
Backup and storage of critical information offsite.	x	x				x	x
Ensure interoperability among system components.	x	x				x	x
Implement redundancy in critical system components.	x	x		x	x	x	x
Use uninterruptible power supplies.	x	x		x	x	x	x
Document system and application configurations	x	x	x	x	x	x	x
Document environmental requirements.		x		x	x	x	x
Backup and storage of information and applications offsite.	x	x				x	x
Implement fault tolerance in critical system components.		x				x	x
Replicate information.		x				x	x
Document Web site.			x				
Code and program the Web site uniformly.			x				
Consider contingencies of supporting infrastructure.			x			x	x
Implement load balancing.			x				
Coordinate with incident response procedures.			x			x	x
Document the network.				x	x		
Coordinate with vendors.		x		x	x	x	x
Identify single points of failure.		x		x	x		
Monitor the network.				x	x		
Institute service level agreements		x		x	x		x
Consider a hot site or reciprocal agreement.		x			x	x	x

APPENDIX E: Revisions

Description	Revision Date
1. Cyber Security Incident Reporting Procedure	December 1, 2005
2. Incident Management Procedure	March 1, 2007
3. Media Sanitization Procedures	December 1, 2008

1. Computer (Cyber) Incident Reporting Procedures

Purpose: The purpose of this document is to provide a computer incident reporting and response process that the State of Oklahoma will employ in the event of an intrusion to or an attack on government computer systems. This reporting and response process provides a coordinated approach to handling incidents across all levels of government. The intention of this coordinated process is to minimize or eliminate the propagation of an event to other computers and networks. Reporting computer crimes is the only way for law enforcement to deter and apprehend violators.

Centralized reporting serves the goal of increasing awareness of vulnerabilities and threats to state government as a whole. Centralized reporting is necessary to discern patterns, identify areas of vulnerability, allocate resources, and develop statewide solutions.

Scope: This procedure applies to all agency, authority, board, department, division, commission, institution, institution of higher education, bureau, or like government entity of the executive branch of the state government.

Definitions: A computer or cyber incident is an event violating an explicit or implied computer security policy. The following types of events or activities are widely recognized as being in violation of a typical security policy. These activities include but are not necessarily limited to:

- Attempts or activities interpreted by the agency as legitimate attempts to gain unauthorized access to a system or its data;
- Unwanted disruption or denial of service;
- Unauthorized use of a system for the transmission, processing or storage of data;
- Storage and/or distribution of child pornography;
- Changes to system hardware, firmware, or software characteristics without the owner's knowledge, instruction, or consent; and

- Cyber-terrorism is the unlawful and deliberate use, modification, disruption or destruction of computing resources to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives.

The Oklahoma Computer Crimes Alliance (OCCA) is a partnership of federal, state, and local law enforcement agencies within the state of Oklahoma to aggressively address cyber threats and crime in a coordinated manner.

Procedures: It is the responsibility of all state employees to report suspected computer incidents as quickly as possible. The ultimate goals, regardless of incident, are the protection of assets, containment of damage, and restoration of service.

The reported cyber incident will be coordinated by the Oklahoma Office of Homeland Security, Information Analysis/Infrastructure Protection Division (OHS IA/IPD) and the Oklahoma State Bureau of Investigation (OSBI).

Primary support for an incident response will be at the request of the OHS IA/IPD and OSBI and be provided by the OCCA.

NOTIFICATION

Initial notification of a cyber incident should be made to the Lead Technology Position (Chief Information Officer, IT Director, Manager or Administrator) of the affected state agency or office. The affected state agency or office will make the appropriate cyber incident notification to law enforcement.

Notification of this cyber incident should be made through the OHS IA/IPD, the OSBI, and the OCCA by completing the Incident Reporting Form contained at the OCCA website (www.cybercrime.ok.gov). The OCCA website will provide notification to the Supervisory Special Agent of the Computer Intrusion Squad at the Federal Bureau of Investigation (FBI) and the Electronic Crimes Special Agent at the United States Secret Service.

The OHS IA/IPD and the OSBI will contact the OCCA to coordinate the response to the cyber incident.

A significant cyber incident (denial of service, compromise of sensitive data or information, mass viral infections) notification can be made by calling the FBI at 405-290-7770. The FBI Communications Center will contact the OHS IA/IPD, OSBI and the Electronic Crimes Special Agent at the United States Secret Service.

RESPONSE ACTIONS

Once an incident has been reported to the OHS IA/IPD, OSBI, and the OCCA, the incident specifics such as time, date, location, affected systems, and the nature and consequence of the incident will be obtained.

An initial response team consisting of the OCCA and the affected agency will respond to the incident.

The OCCA will focus on identifying the origins of the incident and apprehending those responsible. If the initial response team suspects the incident to be a cyber terrorism incident, the FBI Joint Terrorism Task Force (JTTF), and Oklahoma Office of Homeland Security will be notified. Based on continuing analysis and assessments, the initial response team will focus on remediation of mission critical information and telecommunications systems, as well as those systems whose loss would constitute an immediate threat to public health or safety.

The OCCA shall apprise the agency chief information officer, or person responsible for Information Technology, affected by the computer incident of the progress of the investigation to the extent possible.

AGENCY RESPONSIBILITIES

Employee:

- To adhere to this procedure and any other state or agency security policies and procedures.
- To report all suspected computer incidents to their supervisors and to the appropriate business or technical area manager who in turn will notify the OCCA using the OCCA website (www.cybercrime.ok.gov) or the FBI at 405-290-7770. This number is monitored 24 x 7 x 365.
- To fully cooperate with any subsequent investigation of a computer incident.

Agency:

- To communicate this procedure to all employees.
- To provide periodic security awareness training to agency employees.
- To implement procedures to ensure compliance with the initial notification procedures described in this policy.

It is the responsibility of each agency to identify procedures, whereby its IT staff will determine if a computer or cyber incident has taken place and if it should be reported using this process.

The Incident Reporting Form is attached.

INCIDENT REPORTING FORM

Note: This form is required for all suspected or actual privacy or security breaches.
This form will be sent in confidence to the state Incident Response Center.

Type of Incident (Privacy, Security, Virus, etc)		Incident Date
Individuals Providing Report (Full Name)		Report Date
Phone	Division	Supervisor / Manager

Incident Description *Complete all information known at the time of the report preparation. Supervisors and investigators will complete other items on the report as results become available.*	
Incident Description	
Information Compromised (or at risk)	
Information Systems Compromised (Hardware, software, sites): include host name(s), host IP address(es), & primary purpose of host machine(s)	
Location of the Incident or Systems: include street, city, state, zip	
Other affected hosts/sites / information (include 3rd parties, local public health, other state agencies, etc.)	
Damage or observations resulting from attack (Impact on Operations to include downtime, costs, other damages)	
Summary of Incident Investigation Results (i.e., number of hosts attacked, how access was obtained, how was attack identified, was an incident response organization contacted prior to submission of this report, etc…)	
Identify the agency or agencies which received a report concerning this incident.	

Report Completed by:

- ____
- Date:______________________

Information Reviewed by:

- ____
- Date:______________________

2. Incident Management Procedure

OVERVIEW

The Office of State Finance (OSF) monitors the State of Oklahoma network backbone, primarily focusing on the segments used by OSF and by the agencies to which OSF provides services. When abnormal and excessive traffic are revealed, further investigation is conducted. OSF will notify the agencies involved when events are observed and recorded that clearly indicate questionable activities. Examples of such activity include events indicating the possible presence of computers compromised by unknown attackers or computers actively being used to scan and perhaps exploit other cyber assets belonging to State or other entities. These activities are indicative of a serious and potentially critical intrusion and as such are considered a possible criminal act. In these cases, OSF will notify the agencies so they can open an incident report using the Oklahoma Computer Crimes Alliance (OCCA) Incident Reporting system. The agency will be given a period of time to evaluate their environment and report the results of their evaluation. If the suspected incident is not reported within 24 hours and depending on the suspected severity of the observed activity, OSF can submit a report on behalf of the agency, after notifying the agency Director. Agencies can submit, update and modify reports for their agency, regardless of who submits them.

These procedures will be used together with the Computer (Cyber) Incident Reporting Procedures, which are explained starting on page 66. In this section, a computer or cyber incident is defined as "an event violating an explicit or implied computer security policy". The goal of these procedures is to define the process for reporting and responding to "significant" incidents, whether they originate externally or internally.

When any intrusion occurs, it is the responsibility of the agency to analyze and validate each incident, documenting each step taken. When the agency believes that an incident has occurred, they shall perform an initial analysis to determine the incident's scope, such as which networks, systems, or applications are affected; who or what originated the incident; and how the incident is occurring (e.g., what tools or attack methods are being used, what vulnerabilities are being exploited). The initial analysis should provide enough information for the agency to prioritize subsequent activities, such as containment of the incident and deeper analysis of the effects of the incident. The agency shall assume the worst until thorough analysis concludes the root cause(s) of the incident and steps have been taken to mitigate or remediate the vulnerabilities and the results of any exploit(s).

Below is the list of recommended actions for the agency to follow.

Recommended Actions:

1. Report this incident to the OCCA, following the procedures provided in the current state policy—see Appendix E: Revision 1. Computer (Cyber) Incident Reporting Procedures on page 66 in the Appendix of the statewide Information Security Policy, Procedures, and Guidelines document.
2. The initial incident response activities are the responsibility of the agency experiencing the event. Whenever possible, it is imperative to preserve evidence in case of a criminal investigation. This means avoiding actions that would alter or destroy physical evidence that resides in memory and/or on the disk drives of suspected host computers.
3. Our first priority must always be to protect state assets and ensure the continuity of critical services. So the statements in #2 above must be weighed in light of the criticality, urgency and perceived risk(s) to the state. If the impact and/or risk to the state are significant, then those factors override the importance of preserving data. If the agency is able to make this decision, it must be based on the results gathered during steps #4 and #5 below.
4. Analyze the computer(s) in question to determine if any sensitive data may have been exposed, lost or damaged. House Bill 2357 defines sensitive data to include "personal information", consisting of the first name or first initial and last name of an individual in combination with any

one or more of the following data elements, when either the name or the data elements are not encrypted: a) social security number; b) driver license number; or c) account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to the financial account of an individual. This statute also specifies that if such information is reasonably believed to have been, acquired by an unauthorized person, then disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement.

5. Conduct an analysis of the network traffic flows between the compromised computer(s) and other inbound and/or outbound computer(s), including all known assets that communicate with the primary suspect devices involved in questionable activities; also, do not initiate communication with unknown assets or IP addresses of any kind, including use of the "ping command" — such activity will alert the intruder that we are aware of their presence, which may produce undesired results. If the agency is not able to perform this analysis, please notify OSF for assistance.
6. The OCCA will evaluate the reported incident and determine if a criminal investigation is needed. If not, the incident will be turned over to the agency and/or OSF to continue the response activities.
7. The remaining actions will depend on the decisions made by the agency based on the results of the analysis above that set the expectations for the overall impact of the event on critical agency assets and services.

The following describes the computer incident response team organization and roles. These procedures define the agency's roles and the roles of the state and/or other agencies where appropriate.

INCIDENT RESPONSE TEAM ORGANIZATION

Response to significant cyber incidents is guided by the agency's Incident Response Team (**IRT**). Although first responders may be general IS or IT staff and can include other agency staff with prior approval, the IRT provides overall response guidance. This team's first effort during an incident is to take control of the situation with the intent of mitigating potential damage to the agency or its customers.

It is the IRT's responsibility to:

- Manage the incident response process
- Defend against attacks and prevent further damage from occurring when an incident does occur
- Implement improvements that prevent attacks from reoccurring
- Report the outcome of any security incidents to the Information Security Officer or Cyber Security Representative, who will report the incident using established state procedures

The agency will appoint a qualified IRT with current members listed in the following table, if available.

IRT Groups	IRT Functional Members*	IRT Member Roles
State Agency	**Agency Director**	Decisions related to assets & services
	IT/IS Director	Technology decisions & alternatives
	Security Manager/Admin	Response coordinator & documentation
	Network Manager/Admin	Address network related questions/issues
	Server Manager/Admin	Address server questions/issues
	Workstation Manager/Admin	Address workstation questions/issues
	Operations Manager/Admin	Address operational questions/issues

IRT Groups	IRT Functional Members*	IRT Member Roles
	Applications Manager/Admin	Address application questions/issues
Office of State Finance	**(OSF) ISD Director**	Notify Agency Director if issues are identified Coordinate with OKOHS & OSBI to enforce the statewide minimum information security and internal control standards
	Information Security Officer	Coordinate IRT activities with agency & OCCA Coordinate IRT support for agencies requesting or requiring assistance
	Information Security Admin	Document & clarify monitored events Coordinate/support non-criminal IRT activities with agency & other group team members
	Network Manager/Admin	Coordinate/support OSF customer equipment
Oklahoma Office of Homeland Security	**(OKOHS) Agency Director**	Enforce the statewide minimum information security and internal control standards
	Information Analysis / Infrastructure Protection	Enforce the statewide minimum information security and internal control standards
Oklahoma State Bureau of Investigation	**(OSBI) Division Director**	Enforce the statewide minimum information security and internal control standards
	Computer Crimes Unit	Enforce the statewide minimum information security and internal control standards
OCCA	**Office of Homeland Security**	Assess incident reports for prosecutable value and investigate and gather evidence when necessary
	OSBI	**Assess incident reports for prosecutable value and investigate and gather evidence when necessary**
	FBI	Coordinate OCCA resources & investigations
	OSF	Maintain OCCA incident reporting system

<u>*Note</u>: It is recognized that multiple functions may be handled by the same incident response team member(s), depending on how each agency is organized. If the agency uses a third party to perform any of these functions, then that group will be responsible for providing the support necessary to identify and address the requirements or issues involved.

INCIDENT RESPONSE PROCEDURES

Each agency will develop an IRT Plan based on the FBI's National Infrastructure Protection Center guidelines, which are now part of the Office of Domestic Preparedness/Department of Homeland Security and US-CERT (United States Computer Emergency Readiness Team). These guidelines are segmented into three phases:

Phase I:	Detection, Assessment and Triage
Phase II:	Containment, Evidence Collection, Analysis and Investigation, and Mitigation
Phase III:	Remediation, Recovery and Post-Mortem

Checklists for agency incident response are provided in the following tables. The original checklists have been updated to reflect statewide policy and statute requirements.

The IRT or other staff will generally respond to incidents by following these steps in the order given. Every step, however, may not apply to each incident, and the IRT shall use discretion and experience when applying these steps to actual incidents. The checklist steps below are initiated at the point in time when a potential incident is detected and declared.

Phase I activities are designed to control risk and damage and are particularly critical to the successful response. These Phase I tasks shall be conducted by technical staff or by the IRT.

Phase I Detection, Assessment and Triage	
Step I-1	**Document all aspects of the incident.** Documentation is one of the most critical success factors for incident response. Documentation is electronic or handwritten and need not be well-organized initially. The purpose of this step is to capture everything that occurs in detail, especially names, times and events as they actually occurred. For the initial incident handler, a notebook and pen may be adequate. Screen shots and digital pictures are used when possible to capture information completely and unambiguously. Detailed documentation continues by the IRT throughout the response.
Step I-2	**Notify the IRT leader and, on a need-to-know basis only, other relevant entities.** In this step all appropriate contacts and only appropriate contacts shall be made. Incidents may have legal, human resources and public relations implications and shall not be disclosed to anyone without a specific need-to-know. Care shall be taken not to communicate at any time using potentially compromised data or voice systems.
Step I-3	**Protect evidence.** During this step, evidence is not collected but care is taken to preserve the integrity of potential evidence by guarding against: (a) destruction of evidence through established processes like re-use of backup media, system use or hard-disk wiping; and (b) destruction or tainting of evidence through incident handling actions (logging onto affected systems, etc). If deliberate destruction is considered likely (e.g., by a suspect or attacker), then more aggressive actions may be required to preserve evidence (i.e., removing systems from the network, placing evidence in safe storage, etc.)
Step I-4	**Determine if an actual incident has occurred.** Based on available data, establish whether or not an incident has occurred. This action shall consider the previous steps so that actions such as logging on to affected systems, sending out broadcast e-mails and other similar activities shall be avoided. An event is verified by reaching one of three conclusion-action pairs: 1. verified and proceed 2. undetermined and proceed 3. refuted and terminate (this conclusion must be fully documented and verified)
Step I-5	**Notify Appropriate Personnel.** Once the incident is validated (or undetermined), the appropriate internal and external personnel shall be notified immediately. These contacts follow the communication plan established by the IRT and shall include technical and management staff, human resource, public relations, legal, as well as appropriate external contacts, including the OCCA if they have not been already.
Step I-6	**Determine Incident Status.** This step determines whether the attack / incident remains active or has ceased; and if it has ceased, if it likely to resume. If this step will cause only minimal delay to communications in Step I-5, then activities in Step I-6 may actually occur prior to Step I-5.
Step I-7	**Assess Scope.** Activities in this step determine which and how many systems and data are potentially affected, including whether or not compromised system(s) are the end target or part of a more distributed attack on other systems.
Step I-8	**Assess Risk.** This activity determines agency risk based on the incident activity, scope assessment and potential impact.

Phase I Detection, Assessment and Triage	
Step I-9	**Establish Goals.** This step determines appropriate business goals to guide the response. For instance, the agency may determine that the incident has potential regulatory impact which may guide response activities. The agency realizes that accommodating all business goals may be impossible (i.e., protecting confidential data and maintaining resource availability may conflict).
Step I-10	**Evaluate response options.** Based on information gained in the previous steps, this activity identifies and evaluates appropriate options to meet the goals determined in Step I-9.
Step I-11	**Implement Triage.** Implement the agreed to strategy and option(s) identified in the previous step.
Step I-12	**Escalation and handoff.** At this point, evidence is preserved, appropriate communications made, containment activities executed, and goals identified as possible. If the IRT has not been handling the incident directly, at this point, primary incident response is transferred to the IRT.

Phase II activities are intended to: address containment; stabilization of the environment; evidence collection and analysis; evaluate impact to operations; and determine if interim mitigation actions are available and need to be implemented. These Phase II tasks shall be conducted by the OCCA, where deemed appropriate, by technical staff and/or by the IRT.

Phase II Containment, Evidence Collection, Analysis and Investigation and Mitigation (Note: The OCCA must be contacted and participate, if criminal activity is suspected.)	
Step II-1	**Containment.** Since triage actions are often executed in a crisis environment, the first step in Phase II is to validate that the containment and related triage activities are effective.
Step II-2	**Re-assess.** Once a relatively stable state is established, the scope, risk assessment and response goals are re-analyzed and re-validated. The following questions are generally addressed during this step: • How did the incident happen? When? What is the verified scope or depth of the incident? • Was there any activity after the initial incident? • Who was the source of the attack? • What are the immediate and future recommendations for response? Reestablishing the specific goals of the investigation may alter the response approach (i.e., trap and trace, disconnect systems, active or passive searching, etc.)
Step II-3	**Collect evidence.** Evidence collection involves the identification and capture of data relevant to an incident investigation. Evidence is collected in a way that the integrity of the evidence is ensured and a solid chain of custody is maintained. All evidence relevant to the investigation is captured and may include evidence from systems not actually affected by the incident (e.g., firewall logs, IDS logs, DHCP logs, mail servers, physical access logs, etc.). It's possible some evidence collection activities may involve outside entities (e.g., ISPs web hosting services, etc), legal, human resource and other agency resources are recruited as necessary to ensure proper processes are followed.
Step II-4	**Analyze Evidence.** If the OCCA determines that criminal prosecution is appropriate, the appropriate law enforcement agency will conduct a criminal investigation.
Step II-5	**Develop Hypotheses and Verify.** Previous activities formulate hypothetical answers to questions identified in Step II-2. Each hypothesis is substantiated by evidence, but answers are often not absolute requiring qualitative interpretation with reasoned conclusions. It may be

Phase II Containment, Evidence Collection, Analysis and Investigation and Mitigation (Note: The OCCA must be contacted and participate, if criminal activity is suspected.)	
	necessary to collect additional evidence to support a given conclusion.
Step II-6	**Intermediate Mitigation.** As the investigation proceeds, interim mitigation recommendations may be formulated and implemented to control risk. As resources and priorities permit, and as the criticality of the incident indicates, such interim recommendations may be implemented while the investigation continues.

Phase III activities are intended to: finalize the analysis and reporting; secure evidence; implement required remediation; recover any lost of damaged data; and document lessons learned. These Phase III tasks will typically take place after the OCCA has completed any required investigation activities and shall be conducted by the technical staff and/or by the IRT.

Phase III Remediation, Recovery, Post-Mortem	
Step III-1	**Finalize Analysis and Report.** In this step, a report is prepared to include, at a minimum: • A statement of the circumstances surrounding the incident • A summary of the incident activities and timeline • Conclusions and supporting evidence • Recommendations for short and long term mitigation
Step III-2	**Archive Evidence.** All evidence is securely archived and stored. In most cases, at least the original evidence, one back-up copy, the report and supporting documentation are maintained at least until the incident is resolved. Special circumstances may dictate that some investigation material is destroyed. If this is necessary, secure disposal processes are followed.
Step III-3	**Implement Remediation.** Short term and long term remediation activities are implemented based on a risk-justified approach. Remediation activities may include, among others, policy updates, modifications to business partner processes and upgrades to technical infrastructure.
Step III-4	**Execute Recovery.** If an incident results in the destruction or corruption of data, then a recovery is necessary. Even if temporary recoveries are executed during the incident response, after the remediation is complete a complete, reliable recovery is made.
Step III-5	**Post-Mortem Analysis.** Following the incident response, or during implementation of remediation activities, an analysis is completed to identify the strong and weak aspects of the response and to facilitate plan improvements.

3. Media Sanitization Procedures for the Destruction or Disposal of Electronic Storage Media

INTRODUCTION

House Bill No. 2332 of the 2nd Session of the 52nd Oklahoma Legislature modified Senate Bill No. 81 of the 2nd Session of the 51st Oklahoma Legislature, which now states as follows:

A. The Information Service Division of the Office of State Finance is authorized to:

   1. Develop and publish a state policy and procedures for the destruction or disposal of all electronic storage media to ensure that all confidential information stored on such electronic media devices is destroyed or disposed of in a secure and safe manner;
   2. Define the requirements for the secure destruction or disposal of electronic storage media; and
   3. Assist the Department of Central Services (DCS) in implementing the policy and procedures for the destruction or disposal of state electronic storage media.

B. The Office of State Finance shall notify all agencies, boards, commission and authorities of the policy and procedures for the secure and safe destruction or disposal of electronic storage media.

C. The Department of Central Services shall remove all data from electronic storage media from all surplus information technology and telecommunication equipment before it is sold, donated, stored or destroyed. A state agency may remove electronic storage media from their surplus information technology and telecommunication equipment prior to sending the surplus to the Department of Central Services, so long as the agency has the technical expertise for removal and that the electronic storage media is sent for destruction or disposal pursuant to this subsection.

D. The Department of Central Services shall use existing and future funds from the sale of state surplus equipment and appropriations, as necessary, to pay for the destruction of electronic storage media of equipment processed through the Department of Central Services.

POLICY

The policy for the disposal of the electronic media is included in *Section 9.10 – Disposal of Media* – in the State of Oklahoma Information Security Policy, Procedure and Guidelines at: http://www.ok.gov/OSF/documents/StateOfOklahomaInfoSecPPG_osf_12012008.pdf.

PROCEDURES

These procedures apply to all agencies, authorities, boards, commissions, and other government entities of the executive branch of the State of Oklahoma.

Electronic Equipment Destruction or Disposal Rules

1. For the purpose of this procedure, electronic storage media is defined as follows:

   a. All forms of electronic storage media, whether purchased or leased, and is used to process or store information belonging to an entity of the state of Oklahoma;

   b. Examples include, but are not limited to:

      i. Magnetic Disk Drives: from any kind of computer, whether internally or externally installed and/or accessed, including floppy disks, ATA hard drives, SCSI Drives, Reel and Cassette format magnetic tapes, Optical Disks (CDs, DVDs, WORM), Zip Disks, USB removable media (pen drives, thumb drives, flash drives, and memory sticks) with recordable, non-volatile memory capabilities;

      ii. Hand-Held Devices: including Personal Digital Assistants (i.e., Palm, PocketPC, iPAQ, BlackBerry, etc.); basically any PDA, cell phone or media player (MP3, iPod, etc.) that has been connected to a computer or computer network and/or may have received messages or data wirelessly;

2. If an asset belonging to a state entity is no longer needed and it is not in satisfactory working condition, it can be surplused to DCS pursuant to State Surplus Property administrative rules. All associated electronic media shall be destroyed by DCS, if the agency has not destroyed the electronic media.

3. If an asset belonging to a state entity is no longer needed and it is in satisfactory working condition, then it can be surplused to DCS pursuant to State Surplus Property administrative rules and DCS shall destroy all associated electronic media.

4. All “electronic media” to be “destroyed” shall be logged on the DCS Surplus Property Transfer form, by “asset and/or serial number”, as has been destroyed or released for destruction.

5. If an asset belonging to a state entity is no longer needed, is in satisfactory working condition and the agency is willing to provide the resources needed to perform the required sanitization purging process described below, a state entity can submit a written request for approval to OSF for an exemption to support the agency’s asset donation program. Prior to approval of a written request for exemption, the state entity shall demonstrate accountability and justification by implementing a formal program that includes the following:

   a. The Office of State Finance (OSF) shall review and approve the process used by the state entity to sanitize the electronic media; and OSF can designate an entity to perform random audits of sanitized media to ensure that the process is working satisfactorily;

   b. The state entity donating the surplus assets shall provide OSF and DCS with a list of the nonprofit organization(s) receiving them, including an inventory of the equipment, with serial number(s), donated to each organization;

   c. A signed agreement between the entity donating the surplus assets and the organization(s) receiving the donation(s) shall be in place; and

   d. The agreement shall specify that the organization(s) receiving the donated asset(s) accept transfer of ownership, which includes proper disposal, once the asset(s) are no longer needed, or if they stop working.

APPROVED DESTRUCTION OR DISPOSAL METHODS

Destruction or Disposal Rule #1

All electronic media shall be removed from the surplus asset and delivered to or held for pickup by a state authorized destruction agent. Such agents shall be identified by a statewide contract specifically for this purpose. All such equipment shall be destroyed using one of the approved methods described below.

There are many different types, techniques and procedures for media destruction. If destruction is decided on because of the high security categorization of the information, the media should be able to withstand a laboratory attack after its destruction (defined below in Background and Guidelines).

- *Disintegration, Pulverization, Melting and Incineration.* These sanitization methods are designed to completely destroy the media. They are typically carried out at an outsourced metal destruction or licensed incineration facility with the specific capabilities to perform these activities effectively, securely and safely.
- *Shredding.* Paper shredders can be used to destroy flexible media such as diskettes once the media are physically removed from their outer containers. The shred size of the refuse should be small enough that there is reasonable assurance in proportion to the data confidentiality that the data cannot be reconstructed.

Optical mass storage media, including compact disks (CD, CD-RW, CD-R, CD-ROM), optical disks (DVD) and MO disks, shall be destroyed by pulverizing, crosscut shredding or burning. When material is disintegrated or shredded all residues shall be reduced to nominal edge dimensions of five millimeters (5 mm) and surface area of twenty-five square millimeters (25 mm^2).

Destruction or Disposal Rule #2

All electronic media shall be destroyed using the same method(s) described in rule #1; or they may be sanitized using the following *Secure Erase* procedure, provided that an approved exemption program is in place:

Secure Erase is a set of commands embedded in most advanced technology attachment (ATA) standard drives built since 2001 (drives greater than 15 GB). Secure Erase overwrites every track on the hard drive, which includes all data on bad blocks, data left at the end of partly overwritten blocks and directories.

HDDerase is a DOS-based utility that utilizes this set of commands to securely erase, sanitize, all data on ATA hard disk drives in Intel architecture computers.

In order for the utility to work, the BIOS chip on the motherboard must support the secure erase function. Some BIOS chips prohibit the secure erase option (Freeze Lock). HDDerase will attempt to bypass the Freeze Lock, but in the event that it cannot, there are a few workarounds located in the utilities documentation.

The user must have a bootable device to use the utility. This device may be a:

- Windows boot disk
- Bootable CD (Ultimate Boot CD works well and it contains HDDerase 3.1)
- A bootable USB Device

- A *Secure Erase* Drive eRazer (which is a 3rd party hardware appliance from WiebeTech$_{TM}$)
  http://www.wiebetech.com/products/Drive_eRazer.php (Testing has shown this device to provide the most consistent results with the least amount of issues, at a cost of around $200 per appliance.)
  (***Note:*** *The bootable media must be able to run an ". Exe" file)*

HDDerase can be used as follows:

- Boot the computer in DOS using the bootable disk (CD, Floppy or USB) containing HDDerase
- Type "hdderase" at system/DOS prompt
- All ATA hard disk drives connected to the motherboard will be identified
- Select the Device you want to "sanitize"
- HDDerase will test whether the device supports this feature
- It can take from 30 to 180 minutes to complete the secure erase process.

(Note: *Ensure that the hard disk drive jumpers are* ***NOT*** *set to cable select, but rather to Master or Slave.)*

THIS PROCESS SHALL BE EXECUTED BY A TRAINED, EXPERIENCED AND AUTHORIZED INFORMATION TECHNOLOGY TECHNICIAN.

Links:

- **WiebeTech$_{TM}$** *Secure Erase* Drive eRazer - http://www.wiebetech.com/products/Drive_eRazer.php
- **Ultimate boot CD** - http://www.ultimatebootcd.com/
- **HDDerase 3.3** - http://cmrr.ucsd.edu/people/Hughes/SecureErase.shtml
- **HDDerase Documentation** - http://cmrr.ucsd.edu/people/Hughes/HDDEraseReadMe.txt

BACKGROUND AND GUIDELINES

The above procedure is based on NIST SP800-88, a standard from the National Institute of Standards and Technology (NIST) – a federal technology agency that develops and promotes measurement, standards and technology. NIST SP800-88 is the Guidelines for Media Sanitization standard developed by the Information Technology Laboratory in the Computer Security Division of NIST.

Definitions: In order for organizations to have appropriate controls on the information they are responsible for safeguarding, they must properly safeguard used media. An often rich source of illicit information collection is either through dumpster diving for improperly disposed hard copy media, acquisition of improperly sanitized electronic media or through keyboard and laboratory reconstruction of media sanitized in a manner not commensurate with the confidentiality of its information. Media flows in and out of organizational control through recycle bins in paper form, out to vendors for equipment repairs and hot swapped into other systems in response to emergencies. This potential vulnerability can be mitigated through proper understanding of where information is located, what that information is and how to protect it.

The following are some examples of electronic storage media covered by this procedure. Electronic (or soft copy) media are the bits and bytes contained in hard drives, random access memory (RAM), read-only memory (ROM), disks, memory devices, phones, mobile computing devices, networking equipment and many others. This is not a complete list. Other types can exist that may include older and newer/future versions, which are also covered by the statute and this procedure. For a complete list of media types (electronic and non-electronic) a full copy of the standard can be found at: http://csrc.nist.gov/publications/nistpubs/800-88/NISTSP800-88_rev1.pdf.

Users of these procedures should categorize the information to be disposed of, assess the nature of the medium on which it is recorded, assess the risk to confidentiality and determine the future plans for the media. Then use the information in the Sanitization Methods description(s) to decide on the appropriate method for sanitization. The selected method should be assessed as to cost, environmental impact, etc., and a decision should be made that best mitigates the risk(s) of unauthorized disclosure.

4. Removable Media — Acceptable Use Procedures

These procedures must be followed to safeguard both personal and state information. They apply to all state employees and anyone using state computer systems, including other state agency staff, contract staff and vendors. The only exception is for visitors making ad hoc use of public WiFi infrastructure. All state entities must take measures to ensure that encryption procedures (#5 below) are consistently implemented. The use of 3rd Party tools to enforce these procedures is one approved alternative; and the use of Windows technologies, such as Active Directory Group Policy and native Windows encryption utilities, is another option. The effective date of this change is July 15, 2011.

1. Mobile computing devices, including all notebooks/laptops, netbooks, tablets (iPads, Xooms, PlayBooks, Motion, etc.) and all forms of Smartphones must be encrypted if used on State infrastructure.
2. USB ports are essential for most personal computers. They are universally allowed to support the connection of keyboards and mice. They can also be used for approved peripheral devices.
3. Use of the following devices must be “state owned assets” and controlled through an authorized approval process: flash drives, external hard drives, memory sticks, audio/video devices (tablets, iPods, MP3 players or similar hybrid devices), smartphones, cell phones or cell phone hybrids, micro drives and non-standard PDAs. Exceptions may be made to authorize the use of otherwise prohibited devices, if required to perform agency activities (such as software installations or backup of existing files/systems).
4. The controls that apply to connecting devices by USB also apply to other methods of connecting these devices and will also violate this policy. Examples of other connection methods include but are not limited to: Bluetooth, Infrared, Firewire, Serial/Parallel ports, Optical (CD/DVD/Blu-ray), eSATA, or SCSI.
5. Only mobile computing devices and removable media devices from an approved list and provided through statewide contract can be used. If data resides on an unapproved removable device, it must be migrated to an approved device or an authorized designated network location.
6. All removable devices that can be used for data storage must include a data encryption algorithm and a strong password, both of which must be implemented so they cannot be removed by anyone other than an authorized administrator.
7. No personal identity information, such as social security, tax identification, bank account, credit card, personal health, or drivers’ license numbers shall be stored on these devices. Since state employee personal contact information, such as home phone numbers and addresses are considered sensitive information by state statute, storing this information is also discouraged. It will only be allowed for purposes of business continuity and disaster recovery planning and response.
8. If any of these devices are lost or stolen, the Governor’s Office must be notified within 24 hours.
9. If any of these devices are lost or misplaced for at least 48 hours, stolen or accidentally destroyed, this must be reported to your management and to the OSF Help Desk at 866-521-2444 or 405-521-2444.

10. These procedures must be enforced using "active policies", such as Microsoft Active Directory "group policies", on the Windows platforms involved (servers, desktops, directories, etc.), or an equivalent methodology on other operating systems.
11. Violations of this policy, including abuse of administrator privileges, may be cause for criminal, civil, or disciplinary action including the possibility of termination.

SOFTWARE ENCRYPTION ALTERNATIVES (MOBILE COMPUTING AND REMOVABLE MEDIA)

1. Symantec Endpoint Encryption 8.0
2. McAfee Endpoint Encryption (for Removable Media)
3. Sophos SafeGuard RemovableMedia
4. Checkpoint Media Encryption
5. LANDesk Endpoint Security (CREDANT Mobile Guardian)
6. TrueCrypt (Note: This is an open source solution that does not offer any local or remote administration software and should not be considered for medium to large organizations, unless they already have an administration tool that is or can be customized to be compatible with devices on which this product is used.)
7. BitLocker-to-Go (Note: With Windows 7, BitLocker Drive Encryption helps protect sensitive data from being accessed by unauthorized users who come into possession of lost, stolen, or improperly decommissioned computers. BitLocker-to-Go extends BitLocker data protection to USB storage devices, enabling them to be restricted with a passphrase. In addition to having control over passphrase length and complexity, IT administrators can set a (AD Global) policy that requires users to apply BitLocker protection to removable drives before being able to write to them.

HARDWARE ENCRYPTION ALTERNATIVES (MOBILE DEVICES AND USB FLASH DRIVES—OTHERS MAY BE ADDED IF APPROVED)

1. IronKey: https://www.ironkey.com/enterprise
2. Kanguru Defender: https://www.kanguru.com/index.php/flash-drives/secure-storage
3. McAfee USB Standard Encrypted Hard Drive Non-Bio
   http://www.mcafee.com/us/products/encrypted-usb.aspx (for those who already have McAfee ePolicy Orchestrator)
4. Kingston DataTraveler Locker: http://www.kingston.com/ukroot/flash/dt_Locker.asp
5. The Dell contract has provisions for ordering hardware encrypted disk drives directly from Dell. However, they are not manageable from the administrative tools provided by most software encryption vendors.

Notes:

1. There is a known flaw in the (built-in or onboard) software encryption process that impacts several major vendors of software encrypted USB flash drives (and some hardware encrypted devices). These vendors have a vulnerability flaw that can be exploited by those with knowledge of the weakness. A flaw was identified in the way the authentication works from the software to the drive itself. The worst part is that multiple vendors used the SAME KEY, and these drives actually passed low-level government certification. The vendors identified so far include:
   - Kingston
   - Verbatim
   - SanDisk

http://www.darkreading.com/insider-threat/167801100/security/encryption/222200174/index.html

2. Hardware encrypted devices are inherently more secure (for organizations that must use them for sensitive or confidential information) because hardware encryption is less vulnerable to software modifications that can be used to break or circumvent the encryption algorithms and they are designed to erase the contents after some number of failed attempts at password guessing; and they typically perform better (faster read/write times) for organizations that use them extensively or for large amounts of data storage and transfer.