

Exhibit I

**Information Technology
Security Standards**

Adopted by the Information Services Board (ISB) on November 20, 2000

Policy No: 401-S3

Also see: 400-P2, 402-G1

Supersedes No: 401-S2

Auditor's Audit Standards

Effective Date: November 20, 2000

OFM Guidelines for Economic Feasibility

Revision Date: January 10, 2008

Definitions

Table of Contents

INTRODUCTION 1
INTERIM ADDENDUM..... 2
STATUTORY AUTHORITY 2
SCOPE 2
EXEMPTIONS 3
I. Standards for Agency IT Security Program Development and Maintenance 3
 A. Agency IT Security Program Framework 3
 B. Business Impact and Vulnerability, Threat and Risk Analysis 6
II. Standards for Agency IT Security Program Components 7
 A. Personnel Security Standards 8
 B. Physical Security Standards 8
 C. Data Security Standards 9
 D. Network Security Standards 12
 E. Access Security Standards 15
III. Standards for Digital Government (Internet) Application Submittal 17
 A. General Requirements 17
 B. Internet Application Design Packet Submittal Contents 18
MAINTENANCE 19
APPENDIX: CROSS-REFERENCE OF IT SECURITY POLICY AND STANDARDS 20
INFORMATION TECHNOLOGY SECURITY STANDARDS INTERIM ADDENDUM 22

Introduction

To implement the Information Technology (IT) Security Policy, to protect IT resources, and to enable security audits of those resources, it is required that agencies adhere to common IT security standards. Common standards will help ensure that all agencies have an effective and secure environment for IT processing.

The protection of computer systems and related data in the State of Washington requires an approach that results in implementation of a balanced, cost-effective application of security disciplines and techniques required by these standards.

Information Technology Security Standards

Prepared by the Washington State Department of Information Services

Security standards define the processes, procedures, and practices necessary for implementing an agency-specific IT security program. These standards apply to all IT activities, whether they are operated by or for an agency. They include specific steps that shall be taken to ensure that a secure IT environment is maintained and all agency systems provide for privacy and security of confidential information.

At the core of these standards is the concept of a shared, trusted environment for interaction between agencies as well as agency to customer transactions. This shared, trusted environment is defined as the Washington State Digital Government Framework. This framework includes the State Government Network (SGN).

These standards are based on a set of key principles intended to protect this trusted environment, which include:

- Sound risk assessment that results in an adequate level of security.
- Security levels that are commensurate with the shared risk to the state enterprise.
- Implementation of security with a customer-centric focus.
- Security programs that support industry standards where applicable.
- Focus on a least-privilege approach to access control.

Agencies that operate some or all of their information systems outside of this environment shall still adhere to the security principles contained in these standards by creating equivalent environments.

This document contains the following IT security standards:

- I. Standards for Agency IT Security Program Development and Maintenance
- II. Standards for Security Program Components
- III. Standards for Digital Government (Internet) Applications

Interim Addendum

The requirements contained in the Information Technology Security Standards Interim Addendum, located at the end of this document, also apply to all IT activities. The addendum contains interim standards adopted in conjunction with the revision of Policy No. 400-P1 Securing Information Technology Assets effective January 10, 2008. These items, which had previously been included in the policy revision dated April 2002, will be reviewed in full and incorporated as appropriate into the body of these standards during the next revision.

Statutory Authority

The provisions of RCW 43.105.041 detail the powers and duties of the Information Services Board (ISB), including the authority to develop statewide or interagency information services and technical policies, standards, and procedures.

Scope

Information Technology Security Standards

Prepared by the Washington State Department of Information Services

These standards apply to all executive and judicial branch agencies and educational institutions, as provided by law, that operate, manage, or use IT services or equipment to support critical state business functions.

Exemptions

These standards apply to Institutions of Higher Education, except, pursuant to RCW 43.105.200, when they develop security standards in lieu of the standards below that are: a) appropriate to their respective environments, and b) consistent with the intent of the ISB. Such higher education security standards shall address:

Appropriate levels of security and integrity for data exchange and business transactions;
Effective authentication processes, security architecture(s), and trust fabric(s); and
Compliance, testing, and audit provisions.

Standards

I. Standards for Agency IT Security Program Development and Maintenance

These standards provide instructions to facilitate the development and maintenance of an agency IT security program needed to protect the integrity, availability, and confidentiality of agency data and safeguard agency IT resources.

A. Agency IT Security Program Framework

The purpose and focus of developing an IT security program is to mitigate the risks associated with operating in a shared, enterprise environment. This shall be accomplished by defining the level of protection that will be accorded agency information assets based on the results of a risk analysis process. In addressing their IT security programs, agencies shall document the processes that the organization has developed and adopted to protect its data and IT assets.

The amount of detail included in an agency program should be commensurate with the size, complexity, and potential business exposure based on the agency's *Business Impact and Vulnerability, Threat and Risk Analysis* (Section I.B). Most importantly, it shall recognize the importance of an enterprise approach to IT security.

Information Technology Security Standards

Prepared by the Washington State Department of Information Services

1. Agencies shall document the general security approach of the agency, at a minimum addressing how the agency has complied with the following:

- a. Agency IT Security Policies and Procedures.

All agency IT security policies and procedures shall be documented, communicated, and updated on a regular basis. They shall be specific enough to reduce ambiguity but flexible enough to address all agency environments.

- b. Agency Authorization and Authentication Strategy.

Agencies shall have a strategic approach to authentication and authorization that is consistent with the concept of shared risk, specifically when operating on the SGN.

- c. Agency Incident Response.

Agencies shall have a basic incident response plan as part of their security program. The incident response plan shall include an exercise approach to ensure the effectiveness of the plan.

2. An agency's security program shall address all applicable standards outlined in this document. If it is determined by a thorough risk assessment that a component of this standard does not apply to an agency's environment, the security program shall clearly document the reasons these elements are not applicable.

3. An Agency IT security program shall contain enough information to:

- a. Enable agency management to assure the agency's ability to protect the integrity, availability, and confidentiality of agency information.
- b. Protect its IT assets from unauthorized use or modification and from accidental or intentional damage or destruction.
- c. Ensure the protection of the SGN.

4. When an agency contracts for IT resources or services with an entity not subject to the ISB Standards, the contracting agency shall ensure the entity's security practices are in compliance with these standards.

Information Technology Security Standards

Prepared by the Washington State Department of Information Services

5. Organizations in compliance with the ISB Standards are considered trusted. Contracts between trusted organizations do not need to document compliance with the contracting agency's standards. If the contracting agency determines the need for higher security assertions, then a service level agreement or similar contract shall be established detailing the security requirements.
6. Agencies shall assign responsibility for IT security to an individual or group with the appropriate training and background to administer those functions. Agencies shall ensure that the individual or group has proper authority to install, monitor, and enforce security standards and procedures.
7. Agencies shall have a plan to maintain their IT security program that addresses the following:
 - a. The IT security program shall be reviewed, evaluated, and updated annually or whenever significant changes occur to an agency's IT environment.
 - b. Documentation of the following maintenance components:
 - i. Procedures used for making changes to security processes, procedures, and practices.
 - ii. Procedures for distributing initial and updated IT security policies, standards, and guidelines.
8. Agency management has the following responsibilities regarding the IT Security Program in accordance with the ISB Information Technology Security Policy:
 - a. Pursuant to RCW 43.105.017(3), agency heads are responsible for the oversight of their respective agency's IT security and shall confirm in writing that the agency is in compliance with these standards. The annual security verification letter shall be included in the agency IT portfolio and submitted to the ISB. The verification indicates review and acceptance of agency security processes, procedures, and practices as well as updates to them since the last approval. The head of each agency shall provide annual certification to the ISB by August 31 of each year that an IT Security Program has been developed and implemented.

Information Technology Security Standards

Prepared by the Washington State Department of Information Services

- b. Agencies shall have an audit performed once every three years for compliance with IT Security Policy and Standards. This audit shall be performed by parties independent of the agency's IT organization. Each agency will be required to maintain documentation showing the results of its audit and plans for correcting material deficiencies that the audit identifies.
 - c. All IT security program documentation shall be written in a clear, compelling, non-technical manner.
9. Some IT security program documentation may contain sensitive information about the agency's business, communications, and computing operations or employees. Such information is to be shared only with personnel who have a need to know. Security program documentation, as prescribed in RCW 42.17.310(1)(ww) and (ddd), should be clearly labeled as "Computer Security Information".

B. Business Impact and Vulnerability, Threat and Risk Analysis

A risk analysis is a systematic examination of assets, threats, and vulnerabilities that provides the foundation for the development of an appropriate IT Security Program. Adequate risk analysis is the key to determining the level of protection required for all computing assets such as networks, applications, systems, facilities and other enterprise assets. A risk analysis will:

- Identify dependence on existing IT assets.
- Identify vulnerabilities of existing IT assets.
- Assess the probabilities of threats occurring to existing IT assets.
- Determine the impact of losses if they do occur.
- Identify the value of safeguards or countermeasures designed to reduce the threats and vulnerabilities to an acceptable level.

The goal of the risk analysis process is to determine an acceptable level of risk that considers agency security, the security of shared resources (especially related to operation on the SGN), agency business strategy and the overall cost of countermeasures. Conducting an adequate risk analysis will aid agency efforts to better apply available resources to their security program.

Agencies shall conduct a risk analysis when introducing significant new systems or when major changes are made to an agency's existing computing environment. To conduct a risk analysis, agencies shall complete the following steps:

1. Information Asset Review

Information Technology Security Standards

Prepared by the Washington State Department of Information Services

An information asset review shall be performed to identify, at a minimum, those information assets that are critical to ongoing operations or which contain confidential or critical data. The criteria for this inventory assessment shall be documented.

2. Business Impact Analysis

A business impact analysis shall be performed for all information assets identified in the Information Asset Review. The purpose of the business impact analysis is to document the potential impact of loss of the assets. Consideration shall be given to operational, financial, and legal impacts.

3. Vulnerability Analysis

A vulnerability analysis is used to identify vulnerabilities associated with information assets. The vulnerability analysis shall identify specific vulnerabilities related to information assets identified in the information asset review, as well as where those vulnerabilities exist.

4. Threat Analysis

A threat analysis shall be conducted to identify threats that could result in the intentional or accidental destruction, modification or release of data, computer, or telecommunication resources.

5. Risk Analysis

A risk analysis is a collective review of the vulnerabilities and threats to all identified assets to determine the likelihood and impact. This analysis forms the foundation for security program planning.

While no specific format is required for the risk analysis, instructions and suggested formats, as well as links to risk analysis resources, can be found in the Information Technology Security Guidelines. Organizations may also consider leveraging disaster recovery reviews, specifically relating to critical assets and business impact, when completing IT security risk assessments.

II. Standards for Agency IT Security Program Components

Agency security programs shall document policies and procedures for the functional areas outlined below.

Information Technology Security Standards

Prepared by the Washington State Department of Information Services

A. Personnel Security Standards

Agencies shall develop, document, and implement policies and procedures for the selection, orientation, and supervision of employees and contractors who have access to agency IT resources. The objective is to ensure that a high level of integrity and satisfactory staff conduct is achieved and maintained, and to promote an awareness of security matters. The following are to be included:

1. Reference checks and background investigations where appropriate.
2. Security awareness training, at hire and annually.
3. IT Security support staff technical training.
4. Sanctions for security violations.
5. Processes for employees or contractors when separating from service.
6. Appropriate language in all vendor contracts regarding security requirements.

B. Physical Security Standards

Agencies are responsible for assuring that adequate physical security protections are implemented to maintain the availability, confidentiality and integrity of the agency's computer systems. Investments in physical security shall be commensurate with the risks, threats, and vulnerabilities unique to each individual site and location.

Agencies shall develop, document, and implement policies and procedures for the following:

1. Location and layout of the facility.
2. Physical security attributes for computer or telecommunications rooms (if applicable).
3. Facility access control.
4. Physical data storage and telecommunications controls.
5. Off-site media storage.

Information Technology Security Standards

Prepared by the Washington State Department of Information Services

6. Physical security controls for mobile/remote computing.
 - a. Laptops and Personal Digital Assistants (PDAs).
 - b. Portable data storage devices (e.g., tape drives, zip drives, removable hard drives, USB data storage devices).

C. Data Security Standards

The purpose of the data security component of the IT security program is to reduce the risk associated with the unauthorized access, disclosure, or destruction of agency-controlled data. Content shall include data classification standards and rules for the access, storage, and dissemination of data.

1. Agencies shall develop, document, and implement policies and procedures for:
 - a. Classification of data based on the agency's risk analysis. At a minimum classify data as sensitive/confidential versus public information.
 - b. Application development processes:
 - i. Ensure version control and currency.
 - ii. Ensure system security requirements assessment and testing during the development life cycle.
2. When sharing data with an external entity (whether data sharing is covered as part of a larger contract, a service level agreement (SLA), or as a dedicated data sharing agreement), the following shall be addressed:
 - a. The data that is to be shared.
 - b. The classification of the data (reference ISB IT Security Guidelines).
 - c. How the data will be accessed or shared.
 - d. Who will have access to the data.
 - e. How the data will be protected.
 - f. What will be done with the data when it is no longer needed for the contract.

Information Technology Security Standards

Prepared by the Washington State Department of Information Services

3. Data and program back up.
 - a. Agencies shall address data archival and rotational requirements for backup media based on the results of their risk analysis. This shall include media used in the backup of host and workstation data.
 - b. Agencies shall establish procedures for periodic tests to restore agency data from backup media.
 - c. Agencies shall establish methods to secure their backup media.
4. Secure management of information and data encryption standards.
 - a. An agency's risk assessment shall identify which data is confidential and when that data needs to be encrypted (secured).
 - b. If encryption is required, the agency security program shall include methodology to ensure the elements in the following areas related to secure file transfer, secure e-mail, and secure data storage are met.

- i. Secure File Transfer

Secure exchange of information from one application or user to another requires that:

All manipulations of data during the exchange are secure.

If intercepted during transmission, data cannot be understood.

The intended recipient is the only one who can understand the transmitted information.

Confirmation is received that the intended recipient received the data.

Confidential information subject to exposure shall be encrypted.

It is assumed that the exchange of information occurs only between secure endpoints.

- ii. Secure E-mail

Secure delivery of a message from a sender to a receiver requires that:

E-mail, and any attachments, containing confidential information shall be encrypted from the sending device to the receiving device.

Chain-of-custody shall be preserved from sending device to receiving device.

Information Technology Security Standards

Prepared by the Washington State Department of Information Services

Ability to un-encrypt sender's message through authorized process; sending organization must be able to un-encrypt and retrieve originating version of sent message.

All manipulations of data during the transfer from sending device to receiving device are secure.

If intercepted between sending device and receiving device, data cannot be understood.

Only the selected receiver can view the data in its original, unencrypted state.

If technically feasible, confirmation shall be issued to indicate that the intended receiver received the data.

The sending organization shall determine what information requires the need for secure e-mail and ensure that the encrypted e-mail message is retrievable within a pre-defined archival period.

iii. Secure Data Storage

Secure data storage is defined as the protection of data content and changes in data state from its original storage on electronic media by using encryption processes. Secure data storage requires that:

An organization has the ability to un-encrypt stored data through an authorized process.

An organization has the ability to un-encrypt stored data through a pre-defined recovery period identified by the organization.

An organization protects the encryption and decryption method (key and algorithm).

If the data is accessed by unauthorized entity, it cannot be understood.

An organization has the ability to detect alteration of intended content.

5. Web Server Data Security

If a Web server is used for access to confidential or sensitive data, agencies shall ensure that the appropriate security and server and database configuration is put in place and documented to maintain the confidentiality and integrity of the data.

Information Technology Security Standards

Prepared by the Washington State Department of Information Services

D. Network Security Standards

1. Agencies shall develop, document, and implement policies and procedures to ensure secure operation of their applications, secure network sessions within the Washington State Digital Government Framework, and appropriate layered protection to address shared risk. These policies and procedures shall include:
 - a. Infrastructure management processes.
 - b. Change management processes.
 - c. Appropriate network breach detection and incident response processes that leverage statewide incident response capabilities such as the Washington computer Incident Response Center (WACIRC) and the Department of Information Services Computer Security Incident Response Team (DIS CSIRT).
2. Agencies shall develop document, and implement policies and procedures to effectively secure wireless devices that extend their Local Area Networks (LANs). Agencies shall:
 - a. Develop, document, and implement wireless access security practices within the agency.
 - b. Firewall all wireless access point connections from the agency network and the SGN. Equivalent solutions shall be approved by the agency's Washington State Department of Information Services (DIS) Senior Technology Management Consultant and documented in the agency security program.
 - c. Use industry standard authentication and encryption methods.
 - d. Perform a self-audit on a regular basis to locate any unauthorized wireless devices.
3. Agencies shall develop, document, and implement policies and procedures for Patch Management.
 - a. All computers systems shall have all critical updates and security updates applied in a timely manner.

Information Technology Security Standards

Prepared by the Washington State Department of Information Services

- b. Agencies shall develop, document, and implement policies and procedures that require any remotely attached device, either employee owned, or agency owned, to have current patches. Agencies may choose to disable or block access for any device that is not in compliance with this requirement.
 - c. Agencies shall develop, document, and implement policies and procedures that require devices attached to agency networks (either on agency local area networks, or wireless networks) to have current patches.
4. Agencies shall develop, document, and implement policies and procedures for Anti-Virus Protection.
- a. Agencies shall develop, document, and implement policies and procedures that address virus prevention, detection and removal processes, including signature currency. Agencies shall ensure that all file transfers, e-mail of all types, and web browser based traffic are examined for known viruses. File transfer, e-mail or web browser-based traffic that cannot be examined for viruses should be disallowed.
 - b. Agencies shall develop, document, and implement virus incident response procedures that are integrated with the WACIRC incident reporting processes.
5. Agencies with devices connected to the SGN shall ensure:
- a. The devices are not connected to external networks either directly or through an extranet/VPN connection. External networks are defined as any networks not part of the SGN and not protected by the DIS-managed security layer, OR;
 - b. The devices are connected to external networks only through a DIS-managed or approved security layer. The DIS-managed security layer is defined as firewalls, proxy servers and security gateways, OR;
 - c. The agency network is only connected to the SGN through a DIS managed or approved security layer.

Information Technology Security Standards

Prepared by the Washington State Department of Information Services

6. Agencies shall develop, document, and implement policies and procedures for Web Browser and E-mail Client security.
 - a. All software used to access or transmit through the Internet shall be approved by an authorized agency authority and shall incorporate all provided security patches that are appropriate to the environment in which it is operating in accordance with the patch management standards.
 - b. Agencies shall ensure that all files received from the Internet are checked for viruses in accordance with the virus prevention standards.
 - c. Agencies shall develop, document, and implement clear acceptable use policies for the use of web browsers and e-mail.

7. Agencies shall develop, document, and implement policies and procedures for Web server security.
 - a. Information placed on a Web site is subject to the same privacy restrictions as non-electronic information. Accordingly, before information is placed on the Internet, it shall be reviewed and approved for release in the same manner as other official memos, reports, or other official non-electronic information. Agencies shall conform to the ISB Public Records Privacy Protection Policy that implements Executive Order 00-03, Public Records Privacy Protections, for its Web site information.
 - b. Web server software shall not be downloaded, installed, or run without prior approval by an agency-authorized system administrator.
 - c. Remote control of Web servers (i.e. administrator operations, including supervisor-level logon) shall be done from the console or via properly secured sessions. The authentication processes and mechanisms used shall be commensurate with the level of risk associated with the nature of the remote environment (i.e. within the SGN or externally over the Internet).
 - d. Patches for Web server software and underlying operating system software shall be installed in accordance with the patch management standards found in section II. D. 3 of this document.

E. Access Security Standards

1. General Access Security

- a. Agencies shall develop, document, and implement policies and procedures that address access security controls for mainframe, client/server, wireless LANs, and stand-alone workstation-based systems that are consistent with the agency's classification of the data processed.
- b. Hardened passwords shall be used and enforced whenever technically and operationally feasible. For those systems for which it would be technically infeasible or which would require modification to meet this requirement as defined below, agencies shall document what other measures are to be taken to secure user access.
- c. Agencies shall develop, document, and implement policies and procedures that address appropriate user training on the use, construction of, and maintenance of hardened passwords.

Hardened Passwords shall meet the following criteria:

- i. Passwords shall be a minimum of eight characters long and contain at least one special character and two of the following three character classes: upper case letters, lower case letters, and numerals.
- ii. Shall not contain the user's name or any part of their full name.
- iii. Passwords shall be changed a minimum of every 120 days.
- iv. After a maximum of five incorrect login attempts, accounts will be locked for a specified period of time, or until administrator reset.
- v. Password administration rules shall be systematically enforced. Any exception shall be documented in the agency's security program.

Information Technology Security Standards

Prepared by the Washington State Department of Information Services

2. Remote Access

Agencies shall develop, document, and implement policies and procedures for remote access that mitigate the threat or risk posed by all users or devices authorized to connect remotely to or through the SGN. Mitigation must not be susceptible to end user modification. Technologies include, but are not limited to, dial-up, wireless, and Virtual Private Networks (VPN).

- a. Agencies shall control the use of dial-up lines.
 - i. Dial-in ports may be used only if there is no other way to satisfy a business need.
 - ii. If dial-in is used, all security features (dial back, etc.) appropriate to the operating environment shall be used.
- b. Agencies shall maintain and review a log of remote connections.
- c. Agencies shall monitor remote access by vendors.
- d. Agencies that use VPN services shall develop, document, and implement policies and procedures and that, at a minimum, address the following:
 - i. VPN solutions shall use industry standard protocols.
 - ii. An agency that operates a VPN solution through a firewall configuration other than the SGN perimeter gateways (e.g. routers, VPN, etc.) or DIS-managed security gateways (e.g. Secure Access Washington, Transact Washington, etc.), shall use an equivalent solution and shall include documentation of the configuration in the agency IT security program.
 - iii. An agency that operates a VPN solution that involves token-based technology such as smart cards shall use the mechanisms supported by the Washington State Digital Government Framework or an equivalent solution approved by the agency's DIS Senior Technology Management Consultant. Equivalent solutions shall be documented in the agency security program.

Information Technology Security Standards

Prepared by the Washington State Department of Information Services

3. Internet Access

The use of the Internet as an access alternative to applications and data imposes new risks regarding the verification of an end user's identity. The standards set forth in this section respond to the issues that shall be addressed by agencies concerned with authentication and access of Internet-based systems.

Internet-based applications shall involve the use of authentication processes and mechanisms that provide a level of identity confidence (level of confidence) that is commensurate with the risk associated with unintended access and/or disclosure of data. "Level of Confidence" can be determined by assessing the processes, controls, mechanisms and technologies used in the authentication process to provide the following:

- a. Identification and Authentication: To initially establish and confirm the identity of an individual or entity and ensure that an authentication mechanism (e.g. digital certificate, password, etc.) used to authenticate an individual or entity has been securely issued.
- b. Authentication Integrity: To ensure that the authentication mechanism used to authenticate an individual or entity is responsibly managed and properly protected to prevent unintended use or compromise.
- c. Authentication Validation: To confirm and validate the identity of an individual or entity upon presentment of the authentication mechanism to an Internet-based system.
- d. Application Security: To ensure that an Internet-based application is properly insulated from direct access from the Internet, and that only individuals or entities whose identities have been positively validated are eligible to access the application.

III. Standards for Digital Government (Internet) Application Submittal

A. General Requirements

This section describes the IT security related content that shall be included in the submittals for Internet-based application design packets. The agency's DIS Senior Technology Management Consultant will use available internal and external resources to review design features relating to Internet security. The Consultant will provide developers pro-active access to the security infrastructure and provide development teams (particularly those agencies with no Internet-based application security personnel) with suggestions or advice on how to best utilize the security infrastructure and existing capabilities of the Washington State Digital Government Framework.

Information Technology Security Standards

Prepared by the Washington State Department of Information Services

Internet-based applications that are designed to provide anonymous access to public information (no specific application level security requirements) are not subject to this submittal requirement.

If a new application or data source is to be integrated into a previously submitted and approved environment, no subsequent submittal is required.

B. Internet Application Design Packet Submittal Contents

1. The agency's security program shall address how the agency will ensure all new Internet-based applications will be reviewed with the agency's DIS Senior Technology Management Consultant.
2. The security program shall address how submitted information will include, at a minimum, the following IT security related information:
 - a. Application description.

Provide a general description of the purpose of the application and the nature of the information involved.
 - b. Application services.

Describe the nature of the services to be provided to the user of the application (static data, interactive queries, data entry, electronic payments).
 - c. Authentication requirements (high, medium, low level of confidence).

Describe the level of confidence required for user authentication and provide a summary of the analysis completed to determine this level.
 - d. Certificate Authority integration (if required).

If the proposed authentication mechanism involves the use of digital certificates, describe any known application integration issues.
 - e. Application access control mechanisms.
 - i. If the project involves providing access to an existing application, describe the nature of the application's access control mechanisms (user ID, password, etc.).
 - ii. If it is the intent of the agency to re-authenticate a user at the application level after the users have been authenticated by a centralized mechanism and processes (such as SGN perimeter gateways (e.g. routers, VPN, etc.) or DIS-managed security gateways (e.g. Secure Access

Information Technology Security Standards

Prepared by the Washington State Department of Information Services

Washington, Transact Washington, etc.), describe the justification for not accepting the initial authentication.

f. Encryption requirements.

Describe any specific encryption requirements for data transmission and/or storage.

g. Proposed development tools.

If known, describe the proposed development tools to be used in the creation or modification of the application for use via the Internet.

h. Proposed Web server platform.

If known, provide information regarding the hardware, operating system, and services provided by the Web server platform.

Maintenance

Technological advances and changes in the business requirements of agencies will necessitate periodic revisions to policies, standards, and guidelines. The Department of Information Services is responsible for routine maintenance of these to keep them current. Major policy changes will require the approval of the ISB.

Information Technology Security Standards

Prepared by the Washington State Department of Information Services

Appendix: Cross-reference of IT Security Policy and Standards

Table 1 provides a cross-reference of the IT Security Policy to the relevant sections in the IT Security Standards.

Table 1

Policy	Relevant Standard Section
1. Each agency must operate in a manner consistent with the maintenance of a shared, trusted environment.	Standards for IT Security Program Development and Maintenance (Section I) Network Security Standards (Section II, D.)
2. Each agency must establish its networks and secure applications within the Washington State Digital Government Framework. This requires that all parties interact with agencies through a common security architecture and authentication process.	Network Security Standards (Section II, D) Access Security Standards (Section II, E.)
3. Each agency that operates its applications and networks within the Washington State Digital Government Framework must subscribe to the principles of shared security	Standards for IT Security Program Development and Maintenance (Section I) Network Security Standards (Section II, D) Access Security Standards (Section II, E.)
4. Each agency must address the effect of using the Internet to conduct transactions for state business with other public entities, citizens, and businesses	Network Security Standards (Section II, D) Access Security Standards (Section II, E.)
5. Each agency must ensure staff is appropriately trained in IT security procedures	Personnel Security Standards (Section II, A.)

Information Technology Security Standards

Prepared by the Washington State Department of Information Services

6. Each agency must review its IT security processes, procedures, and practices at least annually and make appropriate updates after any significant change to its business, computing, or telecommunications environment	Standards for IT Security Program Development and Maintenance (Section I)
7. Each agency must conduct an IT Security Policy and Standards Compliance Audit once every three years. It must be performed by parties independent of the agency's IT organization	Standards for IT Security Program Development and Maintenance (Section I)
8. Pursuant to RCW 43.105.017(3), agency heads will confirm in writing that the agency is in compliance with this policy	Standards for IT Security Program Development and Maintenance (Section I)
9. The State Auditor may audit agency IT security processes, procedures, and practices	Standards for IT Security Program Development and Maintenance (Section I)

Information Technology Security Standards

Prepared by the Washington State Department of Information Services

Information Technology Security Standards Interim Addendum

Adopted by the Information Services Board (ISB) on January 10, 2008

Policy No: 401-S3

Effective Date: January 10, 2008

This addendum contains interim standards adopted in conjunction with the revision of Policy No. 400-P1 Securing Information Technology Assets effective January 10, 2008. These items, which had previously been included in the policy revision dated April 2002, will be reviewed in full and incorporated as appropriate into the body of the standards during the next revision.

Additional Interim Standards

1. *Previous location in policy: Purpose*

The purpose of the Information Technology (IT) Security Policy is to create an environment within State of Washington agencies that maintains system security, data integrity and privacy by preventing unauthorized access to data and by preventing misuse of, damage to, or loss of data. The state's transition from multiple proprietary network connections over dedicated leased networks to the Internet for conducting vital public business has highlighted the following security concerns:

- Information Integrity - Unauthorized deletion, modification or disclosure of information;
- Misuse - The use of information assets for other than authorized purposes by either internal or external users;
- Information Browsing - Unauthorized viewing of sensitive information by intruders or legitimate users;
- Penetration - Attacks by unauthorized persons or systems that may result in denial of service or significant increases in incident handling costs;
- Computer Viruses – Attacks using viral code that reproduces itself by modifying other programs, spreading across multiple programs, data files or devices on a system or through multiple systems in a network, that may result in the destruction of data or the erosion of system performance;
- Fraud - Attempts to masquerade as a legitimate user to steal services or information, or to initiate transactions that result in financial loss or embarrassment to the organization; and
- Component Failure - Failure due to design flaws or hardware/software faults can lead to denial of service or security compromises through the malfunction of a system component.

Information Technology Security Standards

Prepared by the Washington State Department of Information Services

Because information technology security planning is primarily a risk management issue, the policy, these standards and the associated guidelines focus on the creation of a shared and trusted environment, with particular attention to:

- Common approaches to end-user authentication;
- Consistent and adequate network, server, and data management;
- Appropriate uses of secure network connections; and
- Closing unauthorized pathways into the network and into the data pursuant to RCW 43.105.017(2).

Such an environment is made possible through an enterprise approach to security in state government that:

- Promotes an enterprise view among separate agencies;
- Requires adherence to a common security architecture and its related procedures;
- Recognizes an interdependent relationship among agencies, such that strengthening security for one strengthens all and, conversely, weakening one weakens all; and
- Assumes mutual distrust until proven friendly, including relationships within government, with trading partners, and with anonymous users.

In response to these threats and to assist state agencies in mitigating associated risks, the Information Services Board (ISB) requires that agencies take steps necessary to initiate an enterprise-wide approach to:

- Ensure secure interactions between and among governmental agencies take place within a shared and trusted environment;
- Ensure secure interactions between and among business partners, external parties and state agencies utilize a common authentication process, security architecture, and point of entry;
- Prevent misuse of, damage to, or loss of IT hardware and software facilities;
- Ensure employee accountability for protection of IT assets; and
- Prevent unauthorized use or reproduction of copyrighted material by public entities.

Accordingly, the ISB directs state agencies to:

- Operate in a manner consistent with the Information Technology (IT) Security Policy of the State of Washington;
- Develop, implement, maintain, and test security processes, procedures, and practices to protect and safeguard voice, video, and computer data computing and telecommunications facilities -- including telephones, hardware, software, and personnel -- against security breaches;
- Train staff to follow security procedures and standards;
- Apply appropriate security measures when developing transactional Internet-based applications, including but not limited to electronic commerce (e-commerce); and
- Ensure and oversee compliance with the policy and standards.

Information Technology Security Standards

Prepared by the Washington State Department of Information Services

2. Previous location in policy: Statement 1.

Agencies may establish certain autonomous applications, including those hosted by an Applications Service Provider or other third party, outside of the shared, trusted environment, PROVIDED the establishment and operation of such applications does not jeopardize the enterprise security environment, specifically:

- The security protocols (including means of authentication and authorization) relied upon by others; and,
- The integrity, reliability, and predictability of the state backbone network.

3. Previous location in policy: Statement 3.

Furthermore, each agency that operates its applications and networks within the Washington State Digital Government framework must subscribe to the following principles of shared security:

- Agencies shall follow security standards established for selecting appropriate assurance levels for specific application or data access and implement the protections and controls specified by the appropriate assurance levels;
- Agencies shall recognize and support the state's standard means of authenticating external parties needing access to sensitive information and applications;
- Agencies shall follow security standards established for securing servers and data associated with the secure application; and
- Agencies shall follow security standards established for creating secure sessions for application access.

4. Previous location in policy: Statement 4.

Each agency must address the effect of using the Internet to conduct transactions for state business with other public entities, citizens, and businesses. Plans for Internet-based transactional applications, including but not limited to e-commerce, must be prepared and incorporated into the agency's portfolio and submitted for security validation.

5. Previous location in policy: Statement 5.

Agencies are encouraged to participate in appropriate security alert response organizations at the state and regional levels.

- All Internet applications should be included and managed within the agency portfolio. As required by the IT Security Standards, a detailed security design packet for transactional, non-anonymous applications (including but not limited to those using a

Information Technology Security Standards

Prepared by the Washington State Department of Information Services

security mechanism for access control) is submitted for review by DIS but the security related information need not be included in the portfolio.

Examples of security mechanism for access control include, but are not limited to, Public Key Infrastructure, User ID and passwords, or biometrics.

6. Previous location in policy: Statement 6.

Examples of changes that require review and appropriate updates to the agency security program include modifications to physical facility, computer hardware or software, telecommunications hardware or software, telecommunications networks, application systems, organization, or budget. Practices will include appropriate mechanisms for receiving, documenting, and responding to security issues identified by third parties.

7. Previous location in policy: Statement 7

Each agency must maintain documentation showing the results of its review or audit and the plan for correcting material deficiencies revealed by the review or audit.