# Information Technology Security Guidelines

Adopted by the Information Services Board (ISB) on January 31, 2001

**Policy No: 402-G2**
Supersedes No: 402-G1
Effective Date: February 9, 2006
Revision Date: February 2006

Also see: 400-P, 401-S, Guideline for Reporting and Responding to Computer Crimes Definitions

## Table of Contents



## PURPOSE

The Information Services Board (ISB) has developed these guidelines to help State of Washington agencies implement, as part of their IT risk management effort, an Information Technology (IT) security program. This guide includes general direction and best practices that are consistent with the State of Washington Information Technology Security Policy and Standards.

State agencies shouldn't view these IT Security Guidelines as mandatory activities or criteria for the mandatory ISB security audit.

## STATUTORY AUTHORITY

The State of Washington Legislature established the powers and duties of the ISB, including the authority to develop statewide or interagency information services and technical policies, standards, and procedures (RCW 43.105.041).

## SCOPE

All executive and judicial branch agencies and educational institutions can use these guidelines to help operate, manage, or use IT services or equipment to support critical state business functions.

## GUIDELINES

These guidelines include two major sections. Section 1: Guidelines for agency IT security program development and maintenance, is information that will help your agency manage the structure, content, and maintenance of your IT security program. Section 2: Guidelines for IT security program components, contains information that will help your agency address the major security program components.

These guidelines include information and resources to support your agency's compliance with the Information Security Standards for security program development and maintenance. They are organized around the same numbering schema as the Information Security Standards for easy reference. Where no guidelines are provided for a specific standard it is appropriately noted.

## I. Guidelines for agency IT security program development and maintenance

The guidelines in this section will help you protect the integrity, availability, and confidentiality of agency data and safeguards agency IT resources in a manner consistent with the ISB IT Security Standards.

You can find links to IT security program development resources at http://wacirc.wa.gov/. Refer to Appendix A for a list of other resources relevant to these guidelines.

### A. Agency IT security program framework

1. Developing and documenting a general security approach

   a. Agency IT security policies and procedures

      Although your agency information assets may be specific to business functions and strategies, you may be able to organize information in broad categories such as contractual and legislative compliance, explicit access controls, virus prevention, business critical, or levels of sensitivity.

      Agency specific security policies and procedures may include:

      - Legislative and contractual compliance requirements.

- Security education, virus prevention and detection, and business continuity planning.
- Incident response requirements and processes.
- Acceptable uses and management procedures.
- Security program participant roles and responsibilities.
- Policy document and established security program maintenance processes.

The policies and procedures in your agency's IT security program should:

- Include content on purpose, scope, applicability, implementation, enforcement, roles/responsibilities, and revision history.
- Be prepared in a format that supports both hard copy and electronic storage and distribution.
- Consider existing operational procedures.
- Consider the results of the agency risk assessment process.
- Consider the results recommendations of past security audits.
- Be distributed and safeguarded in a manner consistent with the confidentiality of the content.

Consider the following when communicating about your agency IT security program:

- Inform affected parties through normal distribution channels (staff meetings, memos, email, etc.).
- Provide appropriate training to staff on roles and responsibilities in communicating Agency IT security policies and procedures.

Consider a review and update of your agency IT security program:

- As part of an agency's ongoing security program.
- When significant changes occur to an agency's IT environment.
- When significant changes occur that may pose a threat to the agency's IT security.

b. Agency authorization and authentication strategy

Develop an authorization and authentication strategy that will ensure that you maintain an adequate and appropriate level of control on all processes that involve the electronic authorization and authentication required to gain access to agency data. You can find specific

guidelines for determining appropriate approaches in Section II. E. - *Access Security Guidelines*.

c. Agency incident response

Develop a written incident response plan that will ensure appropriate interaction with both the Washington State Computer Incident Response Center (WACIRC) and the DIS Computer Security Incident Response Team (DIS CSIRT). In developing an incident response plan, consider the existing procedures put in place by both WACIRC and DIS CSIRT.

Your agency incident response plan should address the following:

- Roles and responsibilities.
- Process for internal communications (in-band and out-of-band).
- Steps to take during an incident.
- Plan testing.
- Processes for agency communication with WACIRC and DIS CSIRT.

2. Agency security IT program requirements

No applicable guidelines for this specific standard.

3. Agency IT security program contents

No applicable guidelines for this specific standard.

4. Contracting for IT resources or services

When agencies contract for IT resources or services with an entity that is not subject to the ISB standards, agencies should:

- Conduct a review of the entity's security program.
- Require specific assertions from the contracting entity.
- Arrange for an independent audit of the contracting entity.
- Use appropriate contract language for all agreements.

Actions should be commensurate with the nature of the relationship with the entity.

5. Organizations in compliance with ISB standards

   No applicable guidelines for this specific standard.

6. Assigning responsibility for agency IT security

   Consider the following when establishing the individuals and/or groups to lead and administer an agency's security functions:

   - Document roles and responsibilities.
   - Establish clear separation of duties.
   - Establish appropriate chain of command.
   - Assign functions to the appropriate entity within the organization.
   - Ensure adequate definition of the scope of duties.
   - Ensure delegation of appropriate authority.
   - Ensure support of WACIRC functions.
   - Ensure that the administration of security functions is at an organizational level sufficient to provided oversight to agency IT functions.
   - Ensure that appropriate training and certification opportunities are provided to personnel assigned to lead and administer agency security functions.

7. IT security program maintenance

   Consider the following when addressing the maintenance of your IT security program:

   - Establish a baseline based on a review of agency risk assessment results.
   - Establish organizational processes across all business units that support regular reviews.
   - Leverage the existing processes for policy development and implementation.
   - Leverage disaster recovery and business continuity efforts in establishing and reviewing critical IT infrastructure.
   - Align reviews with your agency budgeting and strategic planning processes.

8. Agency management responsibilities

   No applicable guidelines for this specific standard.

9. Sensitive IT program information

   When determining if documentation contains sensitive information about the agency's business, communications, computing operations, or employees, consider the following questions:

   - Could access to the information enable unauthorized access to systems or data?
   - Does the document itself contain information that could be considered private or sensitive?

## B. Guidelines for business impact and vulnerability, threat, and risk analysis

Effective IT security programs are primarily a risk management effort. Numerous tools and approaches are available to support a business impact and vulnerability, threat, and risk analysis. The following general guidelines are related to the business impact analysis and vulnerability, threat, and risk analysis that is required by the ISB IT Security Standards.

When conducting the risk analysis, consider the following:

1. Information asset review

   Document your agency's criteria for critical inventory items. Maintain an inventory that identifies all information technology assets that are critical to ongoing operations or which contain confidential or critical data.

2. Business impact analysis

   The initial step of the business impact analysis is to determine the priorities of senior agency management. Next, identify mission-critical business functions, which are those that are key to the continuation of the organization. If you have already documented your agency’s mission-critical business functions, reassess these functions as a part of your security program maintenance. Suggested criteria for identifying these functions include:

   - Maintenance of public health and safety.
   - Income maintenance for citizens.
   - Income maintenance for government employees.
   - Payments to vendors for goods and services.
   - Requirements for compliance or regulation.

- Effect on state government cash flow.
- Recovery costs.
- Effect on production and delivery of services.
- Volume of activity.
- Effect on public image.
- Inter-system dependency.

3. Vulnerability analysis

   For many threats, you can reduce your agency vulnerability with appropriate controls. For example, you can partially mitigate the vulnerability of data retrieval in a distributed database through
   (1) controls that verify that the receiver of each data transmission is the intended receiver and not an intruder,
   (2) prevention of intruders from intercepting messages, and
   (3) rigorous management of verification and authorization policies and procedures at distributed database sites and/or sites using the Internet or participating in e-commerce.

   Typically, areas where vulnerabilities may exist include:

   - Operating systems.
   - Communications architecture.
   - Operating procedures.
   - Access control and authentication.
   - Security procedures.
   - The competence of an agency security officer.
   - Management policies and procedures.
   - Personnel policies and procedures.
   - Inadequate audit/security mechanism.

4. Threat analysis

   Malicious threats that could render an agency vulnerable include:

   - Alteration of data.
   - Alteration of software.
   - Introduction of computer viruses and other malicious code.
   - Disclosure of confidential information.
   - Electronic emanations.
   - Employee sabotage

- External sabotage.
- Fraud.
- Hacking.
- Terrorist activity.
- Theft.
- Unauthorized use.

5. Risk analysis

   A risk analysis involves documenting the negative impacts that could result from:

   - Accidental or intentional disclosure of data to unauthorized persons.
   - Unauthorized modification, use, or destruction of data, computer, or telecommunication resources.
   - Unintended exposure to other internal or external physical or logical threats.

   Implement your risk analysis process in order to identify IT resource vulnerabilities, assign an impact (loss value) where a vulnerability is actually exposed to a known threat (causing an "event"), and determine the likelihood of occurrence for each event. You can then use this information, when taken together, to estimate an agency's overall level of risk. If you accomplish a vulnerability, threat, and risk analysis in the course of developing a disaster recovery/business resumption plan, consideration should be given to including a summary of the conclusions of your analysis. Your risk analysis typically includes the following steps:

   **Step 1** - Determine the vulnerabilities of specific IT resources and their associated threats.

   **Step 2** - Assign a cost to each potential event (instances where vulnerability is actually exposed to a known threat).

   **Step 3** - Determine the probability of occurrence of each event identified.

   Many physical threats occur regularly. Organizations such as the Federal Emergency Management Agency (FEMA), the Federal Communications Commission (FCC), and the U.S. Fire Administration maintain records of recurring threats, historical occurrences, and statistical probabilities. Local, state, and Federal agencies usually provide statistics on naturally occurring disasters, burglaries, power outages, fires and storms.

**Step 4** - Estimate the loss potential of an agency program or service area, either by quantitative or qualitative means:

Quantitative Approach: The qualitative approach allows you to use numeric values to determine potential loss. The impact of an event is the amount of damage it could cause. The frequency of occurrence of that event is the number of times it could happen. If these two numbers are precisely known, the product of the two would be a statement of potential loss, where Loss = (Impact of Event) x (Frequency of Occurrence). Because the exact impact and frequency cannot usually be specified, it is possible to approximate the loss with an annual loss exposure (ALE). The ALE is the product of estimated impact and estimated frequency of occurrence per year.

Qualitative Approach: In this method, you create scenarios that outline the potential threats to the business and a ranking of these threats according to their seriousness (i.e.; qualitative terms such as low, medium, or high). The procedure usually includes writing scenarios for the major risks, estimating the effects of the occurrences, and evaluating the use of countermeasures and safeguards. You can then rank scenarios according to the seriousness of threats and the sensitivity or financial losses associated with them.

**Step 5** - Identifying and documenting risks

Identify and document those risks that could result in accidental or intentional disclosure of data to unauthorized persons, unauthorized modifications, and/or use or destruction of data, computer, or telecommunications resources.

## II. Guidelines for agency IT security program components

Primarily, your IT security program should protect your data, the systems it resides on, and the network it travels through. The generally accepted information security model used for information security is referred to as the "C.I.A. Triangle." This model emphasis the preservation of three key data attributes: confidentiality, integrity, and availability.

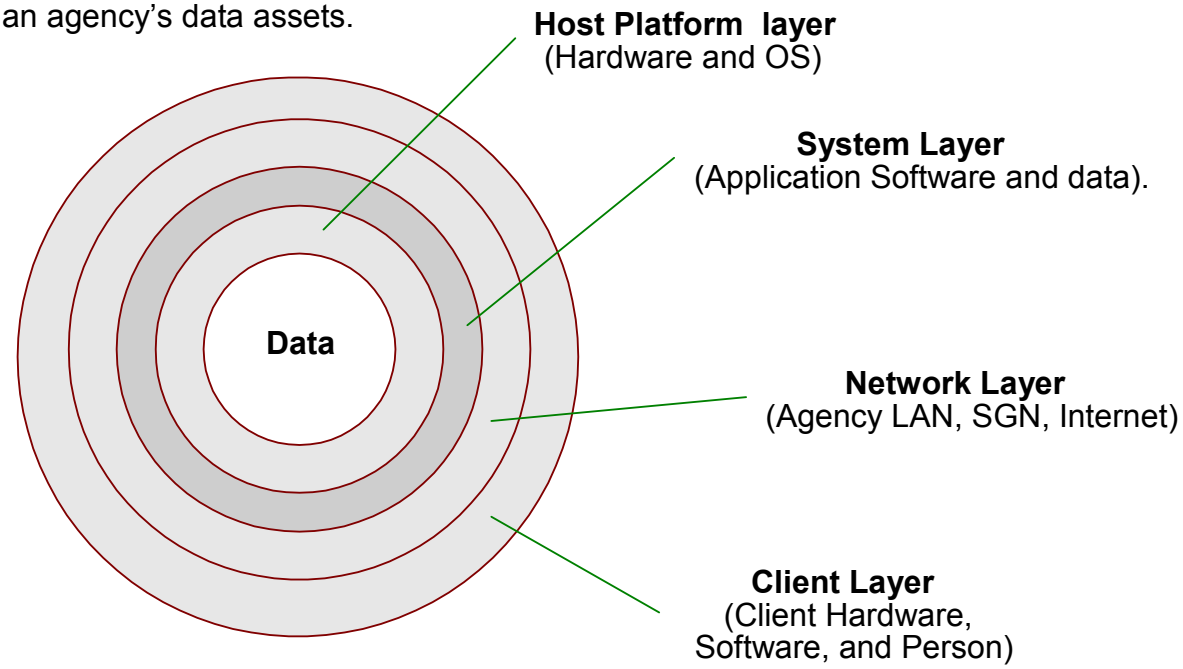
- **Confidentiality** Ensures that only those people and systems with the rights and privileges to access information are able to do so.
- **Integrity** Ensures that Information is whole, complete, and uncorrupted.

- **Availability** Ensures that those people and systems with the rights and privileges to access information can do so without interference or obstruction, and receive it in the required format at the desired time.

To ensure effective protection of your agency's data, you will need to consider the following:

- **Physical security** Taking the actions necessary to protect the physical items, objects, or areas of your agency from unauthorized access or misuse.
- **Personal security** Taking the actions necessary to protect authorized individuals or groups of individuals who access the agency's operational areas.
- **Data security** Taking the actions necessary to protect the agency's access and disclosure of data.
- **Network Security** Taking the actions necessary to protect the data and communications networking components, connections, and contents.

IT Security professionals refer to the concept of "defense in depth" when devising effective security environments. The defense in depth approach "layers" the key security elements, identified above, to create a cohesive defense strategy. The following drawing depicts a typical view of how this layered approach can protect an agency's data assets.



To ensure effective IT security, you must carefully design, implement, and manage appropriate IT security controls for each layer of this model. IT security controls are safeguards and counter-measures that you put in place to mitigate risks to the confidentiality, integrity, and availability of your agency's data and information. These controls address the people, process, and technology risks associated with each layer.

Consider these concepts as you formulate your agency IT security program.

## A. Personnel security guidelines

The following guidelines will help you develop, document, and implement the personnel security aspects of your IT security program.

1. Reference checks and background investigations

   When your agency is hiring or assigning personnel to positions which may impact the availability, integrity, or confidentiality of data and/or systems, your human resource office should conduct appropriate reference checks and background investigations.

2. Security awareness training

   Develop a formal security orientation and training program for all employees. The program should be current and comprehensive, and address the following:

   - Applicable laws and/or rules.
   - Applicable state policies and standards.
   - Agency security policies, plans, and procedures.
   - Emerging IT security issues relating to new technologies such as e-government initiatives.
   - General IT security awareness.

3. IT security support staff technical training

   If your agency employs dedicated security support staff, consider the following when developing a training strategy:

   - Document the aims, training activities, and schedule for security personnel training.
   - Encourage participation and membership in security organizations and working groups.

- Provide access to training tools and programs specifically related to your agency's operating environment.
- Support your staff's pursuit of security certification.

4. Sanctions for security violations

   Your agency should have a defined set of sanctions for security violations. Your human resource and legal personnel should consult with IT security personnel to develop these sanctions. Document these sanctions in the agency security program and clearly define them in related agency policies (acceptable use, etc.).

5. Employee/contractor separation of service

   When implementing procedures for outgoing or transferring employees and contractors, consider the following:

   - The removal of access privileges, computer accounts, authentication tokens.
   - Debriefing the outgoing employee or contractor on the continuing responsibilities for confidentiality and privacy.
   - Ensuring the return of property related to IT use.
   - Ensuring the continued availability of data related to the employee's or contractor's work responsibilities.
   - Implementing procedures for unfriendly termination, including the prompt removal of system access and in some cases, the physical removal or personnel from facilities.

6. Vendor contracts

   When contracting for IT services, consider the following when developing procurement documents and establishing contracts:

   - Whether contractors will be working on-site or off-site.
   - Physical access control procedures, including termination of access.
   - Use of State resources.
   - Need for remote access by contractors.
   - Use of non-disclosure agreements.
   - Requirement for access to confidential information.

   Agency security personnel should work with their agency contract office to establish standard and consistent language in all IT service contracts.

The ISB Model Contracts on the portfolio website at http://isb.wa.gov/modelcontracts/Default.aspx contain sample clauses for personnel security.

## B. Physical security guidelines

The following guidelines will help you develop, document, and implement the physical security aspects of an IT security program.

1. Location and layout of the facility

   - If applicable, locate large (mainframe) computer equipment and/or servers in a secure, environmentally controlled facility.
   - If a computer facility is located in a multi-floor facility, consider the risk of damage from plumbing failures, equipment, or occupants of upper floors.
   - Locate the computer facility inconspicuously, away from exterior walls if possible, with no references or direction signs.
   - Locate computer rooms within an overall facility away from heavy traffic patterns.
   - Use asset tags or other identification markings for all computer equipment.
   - Compare inventory records of computer equipment and the actual physical equipment on an annual basis.

2. Physical security attributes for computer or telecommunications rooms

   - Use locking mechanisms to limit computer room access to authorized individuals.
   - Ensure that the placement of computer room walls and windows limits access by unauthorized individuals.
   - Ensure that the general structure of interior walls is secure and are constructed from the floor to the true, not false, ceiling.
   - Use appropriate devices to control access to sensitive data.
   - Ensure perimeter security for surrounding areas.

3. Facility access control

   - Identify critical areas and designate specific personnel who require access to these areas. Limit access to the fewest number of personnel possible.
   - Limit access to the computer operations facility to authorized persons.

- Arrange for positive identification using pass, key lock, badge system, cipher lock, or other controls for employees, suppliers, and visitors to access the computer room. Make sure you can audit access if possible and review access logs regularly when available..
- Change locks or lock combinations to the computer room on a periodic basis.
- Establish a control system to ensure identification of the individuals who possess keys, cards, and badges at any given time.
- Review, on a frequent basis, the list of assigned key cards or access rights and verify that all persons on the list are still authorized employees.
- Use logs or special badges to identify visitors to the computer room. Provide escorts for visitors, vendors, and contractors when they are in monitored areas.
- Control maintenance and other facilities personnel access to the computer room.
- Require managers to frequently visit the computer room facility on an unannounced basis during a non-prime shift and determine that access control procedures are being followed.
- Establish a system to control individuals bringing or taking packages or containers to and from the restricted area.
- When your agency terminates an employee, immediately escort the terminated employee from the computer room and cancel that employee's access rights.
- Equip any supplementary doors within the computer room facility with exit-only locks and audible alarms.
- Provide for prompt reporting of any actual or suspected hostile act to the appropriate security or law enforcement agency.
- Use locking devices to secure critical freestanding mini/microcomputer systems.
- Use locks to secure the chassis of critical mini/microcomputer system from improper removal of boards and from unauthorized operation, whether or not the system is attached to its work platform.
- Ensure that critical mini/microcomputer workstations are properly locked, that work areas are clear of programs and diskettes, and that locking keys are properly secured during off-shift hours.

4. Physical data storage and telecommunications controls

   - Establish access, fire, and other controls for the prime data storage facility that is appropriate and consistent with procedures used in the main computer room facility.

- Establish procedures for logging data in and out of the media library.
- Establish access, fire, and other controls for the telecommunications control area, which are appropriate and consistent with other computer room procedures.
- Shield or obscure from view cabling of telephone or local network lines from remote devices to the telecommunications facility.

5. Off-site media storage

   - Ensure that media storage meets needs for archival and/or rotational access.
   - Ensure allowance for storage of paper media, magnetic media, or both.
   - Ensure that media storage area meets agency needs for common vaulting, safe-deposit boxes, and/or electronic vaulting.
   - Ensure that storage security needs will be satisfied through use of guards, TV monitors, third-party surveillance, and/or automated security systems.
   - Ensure that storage-building environment provides adequate protection from fire, electrical problems, civil disturbance, and natural disasters.

6. Physical security controls for mobile/remote computing

   a. Laptops and Personal Digital Assistants

      - Ensure that the use of laptops and mobile computing devices such as personal digital assistants (PDA) are properly controlled. Employ appropriate encryption solutions to prevent the compromise of data.
      - Ensure that employees are aware of the risks of stolen or compromised remote computing devices.

   b. Portable data storage devices

      Secure at all times – including in storage, in transit, and during backup creation – removable, or portable storage media containing data the agency has identified as sensitive or critical (such as system backup media).

## C. Data security guidelines

The following guidelines will help you develop, document, and implement the data security aspects of an IT security program.

1. Developing, documenting and implementing policies and procedures

   a. Data classification

      Categorize data according to the risk associated with unauthorized disclosure. Security personnel should work with their legal office when establishing appropriate classifications for their agency.

      Potential categories include:

      *i. Public information*

      Public information is information that your agency can release to the public. It is information for which there is no exemption by state or Federal law allowing nondisclosure to the public. Public information does not need protection from unauthorized disclosure, but does need protection from unauthorized changes that alters the information.

      *ii. Confidential information*

      Confidential information is information that your agency cannot release to the public. It is information that is specifically protected by either state or Federal law, exempting it from disclosure. Confidential information generally includes:

      - Personal information about persons or individual clients, regardless of how your agency obtains that information.
      - Information concerning employee payroll and personnel records not in the Department of Personnel (DOP) system.
      - IT security information that, if released, could jeopardize the integrity of data or result in fraud or unauthorized disclosure or modification of information.

      *iii. Information requiring special handling*

      Information requiring special handling is information that your agency cannot release to the public and for which additional protections need to be in place. This information includes:

      - Information for which either state or Federal laws or regulations require protection or dictate particular handling requirements, for example Health Information Portability and Accountability Act (HIPAA), Executive Order, etc.

- Information that is covered by a contract or agreement in which specific and strict handling requirements are set forth.
- Information for which serious consequences can arise from unauthorized disclosure ranging from life threatening action to legal sanctions.

b. Application development processes

Consider the following actions during the application development process:

*i. Version control and accuracy*

- Establish version control policies and procedures for development and maintenance.
- Track and maintain a log of all software changes.
- Use appropriate automated version control toolkits.

*ii. System security requirements assessment and testing during the development life cycle*

The following guidance regards security testing of agency designed and implemented software:

- Consider the use of threat modeling practices that:
  - Identify the valuable assets that the systems must protect.
  - Create an architecture overview by using simple diagrams and tables to document the architecture of the application, including subsystems, trust boundaries, and data flow.
  - Decompose the architecture of the application, including the underlying network and host infrastructure design, to create a security profile for the application.
  - Identify the threats that could affect the application.
  - Document each threat using a common threat template that defines a core set of attributes to capture for each threat.
  - Rate the threats to prioritize and address the most significant threats first.

- Consider the following design vulnerabilities:
  - Input overflows, buffer overruns, and no bounds checking.
  - Use of external programs via command interpreters.
  - Unnecessary functionality, such as access to Visual Basic for running programs.
  - Inclusion of executable content without a good reason.
- Consider the following steps during the course of the application development process:
  - Conduct an independent protection audit before release.
  - Use an independent team if necessary.
  - Exercise good change control in the software update process.
  - Provide a secure manufacturing and distribution mechanism.
  - Provide a beta-testing process that helps find flaws.
  - Build a repeatable testing capability.
  - Use constant quality improvement to enhance security.

2. Data sharing

   *Appendix B* of these guidelines contains a sample *Interagency Data Sharing Agreement*.

   Your agency should use data sharing agreements to document when you exchange data outside your agency's managed environment.

   Data sharing agreements record the business arrangements between one or more entities concerning the exchange of data. This exchange could be occasional or frequent. The scope should include decisions made related to data classification, data use and purpose, methods of passing the data between the agencies or entities, constraints or obligations imposed by the agency or entity that owns the data on the agency or entity receiving the data, and roles and responsibilities for properly handling the data. Consult appropriate legal counsel when preparing a data sharing agreement.

   a. Data sharing agreements document the exchange of data for business purposes. Typically, data sharing agreements should include:

i. Definition or description of the data being shared or exchanged.

ii. Explanation of the intended use of the data, the justification for sharing the data, and the reasons that the data is being shared.

iii. Documentation of the level of "due care" needed to protect the integrity and confidentiality of the data.

iv. Documentation of any required constraints imposed by the data owner on the use and handling of the data.

v. Documentation of expectations regarding non-disclosure of the data.

vi. Documentation of expectations regarding confidentiality and privacy of the data.

vii. Identification of actions that should be taken at the time of termination (e.g. what happens to the data that is in the possession of the receiving agency?).

b. Data sharing agreements should include a description of the data, and whenever possible, identify the data classification of the data being shared using the guidelines found in Section II.C.1.a – Data Classification. You can then use this data classification as a way to articulate appropriate data security controls for each classification.

c. Data sharing agreements should identify how the entities will access or share data.

d. Data sharing agreements should be very explicit about who has authorization, from the data owner, to access the data.

e. Data sharing agreements should document the data protection standards imposed by the data owner on the data receiver.

i. If legal or statutory requirements impose data protection standards, include the appropriate citations. A good example is data that is subject to the Federal HIPAA laws.

ii. Identify data access controls that the receiving entity is required to implement to protect the data. This may include user identification and authentication requirements.

iii. Disclose the names of everyone who can access the data though not specifically authorized in the agreement (e.g. network administrators).

iv. Identify data transmission controls required to protect the data. This may include use of secure protocol or non-repudiation requirements.

v. Identify data storage controls required to protect the data. This may include possible constraints on where data can be stored, possible data encryption requirements (e.g. is encryption required, what level of encryption is required, what encryption technologies are acceptable, what validation methods are required, etc.), or requirements to use specific ACL parameters on folders where the data may be stored.

*vi.* Identify any compliance monitoring or audit requirements.

f. Data sharing agreements should include an agreed upon process for the disposal of the data after it has been used by the receiving agency. When agencies lose or poorly manage operational control of confidential data, the data owner and data receiver can face substantial risk.

3. Data and program back-up

Based on associated risk, address the following as part of your data and program back-up security planning:

a. Data archival and rotational requirements

When determining the data your agency will archive, specify:

- Data and programs that require no back-up.
- Data and programs that require a secure on-site back-up.
- Data and programs that require both on-site and off-site back-up.
- Frequency of back-ups and the reuse of back-up media.

- Storage of back-up copies of critical files, documentation, and forms in a secure, off-site location.

b. Data restoration

Determine what records will be needed to restore service for various levels of system failure and establish procedures for the creation, maintenance, verification, and emergency use of back-up data. Consider the following categories of data:

- Data files that include magnetic tape master files, disk dumps, and transaction files.
- Application programs.
- Job-control language.
- Systems software, including custom software.
- Program and systems documentation.
- Operational documentation.
- Security, back-up, and recovery procedures.
- Audit records.

c. Securing backup media

Categorize each data file in accordance with the sensitivity and importance of the information it contains. Periodically, select several key applications and ensure that key versions of data files and documentation and special forms are stored in the off-site location. Establish an inventory listing of all items in the off-site location and keep it current.

4. Secure management of information and data encryption

This guideline will help you develop an encryption strategy. The standard content represents a minimum set of core information that should be included in the encryption component of your agency IT security program.

a. Risk assessment

During the risk assessment process, consider the following when determining secure data management and encryption needs:

- Document, in your agency IT security program, the circumstances under which it is appropriate to encrypt and not encrypt.

- At a minimum, use encryption when required by Federal or state regulations or if there is confidential information with a high risk of unauthorized disclosure. Make the decision on whether to encrypt, or not, at project inception. Base your decision on a risk assessment of data sensitivity, how the data is accessed, and who is accessing the data, not solely on whether the data will be accessed through an organization's internal network, the State Government Network (SGN), the Inter-Governmental Network (IGN), or the Internet. Finally, make the decision to encrypt irrespective of the physical distance between the machines involved in the transfer.

- Perform an assessment on the confidentiality level of data, regardless of use. Confidentiality of data is based on many factors, such as operational requirements, regulatory issues, policy and data sensitivity. The confidentiality rating of the data dictates the appropriate level of protection needed.

If, based on the assessment, you decide to encrypt data, you will need to account for three types of data to which encryption might apply (one, two, or all three might apply):

- Data at rest (data stored on device).
- Data in movement (data in transit over a network).
- Data being viewed or used during an interactive session.

State and Federal regulations are an important consideration in determining when to encrypt. Some regulations are very specific as to when you must encrypt confidential information. State and Federal regulations governing mental health, alcohol and substance abuse have stringent safeguard requirements, which you can potentially enforce through encryption.

Encrypt confidential data that you:

- Transmit over unsecured telecommunications lines.
- Store in an electronic file that resides on a computer mainframe, Local Area Network (LAN) client server, or PC hard drive that is readily accessible by individuals who are not authorized to access the information.

You may not need to encrypt confidential information that you don't transmit over unsecured telecommunication lines. For example,

confidential data stored on a mainframe computer may not require encryption when:

- The database is not accessible to the general public.
- The data are reasonably protected from access by agency employees who do not have a need to know.

You will find guidelines on data classification in Section II.C.1.a - Data Classification.

b. Encryption methods, guidelines, and product criteria

Encryption methods

Depending on the type of data to be encrypted, and the nature of the data transport mechanism, consider several encryption methodologies:

- Secure Sockets Layer (SSL) protocol.

  The SSL protocol is an accepted method for providing a secure channel between Web clients and Web servers by riding on top of the TCP/IP layer of the network protocol stack. SSL provides secure communications, authentication of the server, and data integrity of the message packet. When deemed appropriate by your agency, invoke SSL to provide these services for Web-based applications.

- Hypertext Transfer Protocol Secure (HTTPS or S-HTTP).

  HTTPS is also an accepted method for providing a secure channel between Web clients and Web servers and protect the TCP/IP layer of the network protocol stack. HTTPS provides secure communications, authentication of the server, and data integrity of the message packet. When deemed appropriate by your agency, invoke HTTPS to provide these services for Web-based applications.

- Secure/Multipurpose Internet Mail Extensions (S/MIME)

  S/MIME is a standard for secure electronic mail. You can use S/MIME for authentication (using digital signatures) and privacy (using encryption).

S/MIME melds proven cryptographic constructs with standard E-mail practices. It will also support interoperability between E-mail packages that support the protocol.

If your agency needs secure E-mail services, document, in your security program, how your agency will use S/MIME or some equivalent standard.

Technical guidelines for encryption

Use encryption for all storage and transmission of sensitive data or as required by law, using the following minimum attributes:

- Recommend 128-bit key encryption or the highest encryption level possible, subject to constraints such as legacy user population, that meets the agency's requirements.
- Generate keys securely.
- Use public key exchange algorithms.
- Distribute keys securely, not by e-mail.
- Use SSL, HTTPS, Virtual Private Networks (VPN); or other secure connection methods that utilize PKI (digital certificate) technology and Internet-based standards for secure network sessions.

Encryption products criteria

Many products may help you comply with the encryption requirements stated in the Information Technology Security Standards. For example, you may satisfy the secure e-mail requirements by either a secure e-mail package that requires a customer client; or usage of secure messaging where the e-mail is stored on a secure server and must be "picked up" by the recipient.

Consider these suggested criteria when choosing data products:

i. Secure file transfer

The products you use to provide secure exchange of information from one application or user should:

- Be compatible with all entities (government-to-government, government-to-business, government-to-customer).
- Conform to industry-wide standards.
- Support a wide range of platforms.
- Be easily automated with current technologies.

- Support multiple encryption algorithms and key lengths.
- Use transaction logging to provide audit capability.

ii. Secure e-mail

The products you use to secure the delivery of a message from a sender to a receiver should:

- Be compatible with all entities (government-to-government, government-to-business, government-to-customer).
- Conform to industry-wide standards.
- Support a wide range of e-mail clients.
- Integrate with existing e-mail systems.
- Support multiple encryption algorithms and key lengths.
- Meet agency audit requirements.

iii. Secure data storage

The encryption products you use to protect data content and changes in data state from its original storage on electronic media should:

- Be compatible with all entities (government-to-government, government-to-business, government-to-customer).
- Conform to industry-wide standards.
- Support a wide range of platforms.
- Be easily automated with current technologies.
- Support multiple encryption algorithms and key lengths.
- Meet agency audit requirements.

5. Web server data security

No applicable guidelines for this specific standard.

## D. Network security guidelines

1. Secure network operations

The following guidelines will help you develop, document, and implement the network aspects of your IT security program.

a. Infrastructure management processes

Create a management function that has the authority to establish network policies and procedures for such areas as:

- Approving equipment types, such as workstations (terminals, microcomputers, mini-computers), which you may introduce to your network.
- Authorizing the introducing of new equipment to your network.
- Scheduling and authorizing the introduction of communication lines, network addresses, and workstations outside normal operating hours.
- Determining an appropriate level of management approval for changes to the telecommunications network.
- Communicating the network management policies and procedures to users of the network.
- Documenting appropriate use of secure network sessions.
- Documenting appropriate use of VPN.

b. Change management processes

Document your agency's controls for network equipment inventories and equipment changes. Include all network equipment, e.g., modems, controllers, workstations, communication lines, and related devices.

- Ensure that only authorized workstations are connected to the network.
- Physically verify inventory information by checking the actual workstation installations.
- Use network diagrams to document both physical and logical connections between network and other data processing equipment.
- Verify items of network equipment, wherever located, and trace them to inventory records and to network diagrams to determine that records are accurate.
- Store network diagrams in a location protected from unauthorized access.
- Establish procedures for such matters as adding a new workstation or changing a port assignment.
- Establish a formal testing procedure covering the introduction of any new equipment or changes to any network.
- Verify that you have followed formal testing procedures.

c. Network breach detection and incident response

The following general guidelines will help you develop breach detection and response procedures.

i. Breach detection

Your agency should support the following processes:

- Operating system and application software logging.
- Maintaining alarm and alert functions.
- Reviewing, on a daily basis, audit logs from access control mechanisms.
- Reporting anomalies.
- Using supplemental intrusion detection software on critical servers.
- Reviewing, on a weekly basis, audit logs on internal protected servers.
- Using redundant intrusion detection on highly critical servers.
- Using tools to monitor traffic patterns at known concentration points.
- Preventing unauthorized modifications of the firewall configuration to assure integrity.

Typically, you can make and save, on protected media, checksums, cyclic redundancy checks, or cryptographic hashes from the runtime image. Each time an authorized individual, usually the firewall administrator, modifies the firewall configuration, you must update the system integrity online database and save it onto a file system on the network or removable media. If the system integrity check shows that the firewall configuration files have been modified, you will know that the system has been compromised.

Update the firewall's system integrity database each time you configure or modify the firewall. Store system integrity files on read-only media or off-line storage. On a regular basis, check the system integrity on the firewall so that your administrator can generate a listing of all files that may have been modified, replaced, or deleted.

Include, in your agency security program a description of how you:

- Document your firewall configuration to log all reports on a daily, weekly, and monthly basis. This will help you analyze network activity when needed.
- Establish procedures to periodically examine your firewall logs to determine if attacks have been detected.
- Record security-related events on the firewall's audit trail logs.
- Include, at a minimum, hardware and disk media errors, login/logout activity, connect time, use of system administrator privileges, inbound and outbound E-mail traffic, TCP network connect attempts, in-bound and out-bound proxy traffic type.
- Document configuration of the firewall to:

  - Reject any kind of probing or scanning tool that is directed to it so that the firewall does not leak protected information.
  - Block all software types that are known to present security risks.
  - Notify the firewall administrator, at any time, of any security alarm.

Processing audit trails

The frequency and nature of your audit trail reviews should be commensurate with agency size and risk assessment results.

Have processes in place to review audit trails for the following:

- Data entry authorization.
- Operator logging.
- Processing control and balance reports.
- Transaction log files.
- Output distribution logs.

System access violations

Have processes in place for:

- Monitoring system access violations for subsequent action and ensuring that controls exist to limit such access attempts.
- Determining if terminal access codes, menu screens, and personal passwords are changed on a periodic basis.

- Determining that computer system access rights are changed or canceled for individuals who have either terminated employment or changed job responsibilities.
- Assigning responsibility and follow-up for unauthorized access attempts.
- Documenting reports of unauthorized entry, unauthorized attempts to enter, or other breaches of the security areas listed above.

ii. Incident response

The three major components of an effective computer incident response procedure are reporting, handling, and post mortem response.

- Incident reporting is formal acknowledgement that a computer incident occurred.
- Incident handling is the actions taken to resolve the incident.
- Incident post mortem is the analysis of how the incident happened and how to handle the situation so that it does not reoccur.

Your agency incident response plans should be consistent with, and whenever possible, follow the WACIRC Incident Response Procedures, which you can find at http://wacirc.wa.gov/incidentreporting.htm

If you suspect a computer crime, contact the Washington State Patrol Computer Crimes Unit. WACIRC has established guidelines to develop a consistent process for all state agencies to use when responding to a potential computer crime. You can review WACIRC guidelines, link to the Law Enforcement Guidelines for Reporting and Responding to Computer Crimes at http://isb.wa.gov/policies/WACIRCGuidelines.pdf .

2. Wireless devices

The following items should be considered in agency security programs regarding the use of wireless LANs:

- Use an industry standard, such as VPN, for authentication and encryption for all wireless traffic to prevent unauthorized access.
- Use private (non-Internet-routable) IP addresses for wireless devices.

- Change the wireless access point (AP) name Service Set Identifier (SSID) from the default setting to one that is non-descriptive.
- Disable beaconing on the device to discourage opportunist hackers.
- Define how you will determine that no rogue access points exist.

3. Patch management

   Consider the following patch management items for your agency security programs:

   - When you apply patches to new or reconfigured devices, consider the likelihood of infection when attaching to the network. An alternative may be to apply patches offline, such as from a manually produced CD.
   - If your agency uses Microsoft products, replace or eliminate computers that are running unsupported versions of Microsoft products. Unsupported versions do not receive critical or security updates for known vulnerabilities.
   - Your agency should adopt a formal patch management procedure that uses an automated tool and follows industry best practices. Include processes that assess, test, and implement patches. You can find information about automated tools currently used by state agencies at http://wacirc.wa.gov .
   - Your agency should work with Microsoft, CERT, SANS, and other vendors and organizations that offer alert services.
   - Your agency should automatically apply missing patches to workstations when employees connect or when they are denied access to the network.
   - For devices where automatic update is problematic (e.g. remote computers or devices connected with slow connection speeds) agency's should consider alternative methods of patch distribution such as:

     - Mail CDs with appropriate patches to remote users with a deadline for application of the patches.
     - Direct remote users to use Vendors' online update service with a deadline for application of specific patches.
     - Direct remote users to bring the computer used for remote access back into the agency's environment and apply needed patches.

   - Administrators should make sure that they use patches released from appropriate trusted sources.

- Use patch testing procedures to assess the following:

  - Did the patch correct the intended vulnerability?
  - Did the patch open new and/or old vulnerabilities?
  - Did the patch impact your system reliability and/or performance?
  - Did the patch have an impact on your applications?
  - Did you use a scanning tool to verify the patch results?

4. Anti-virus protection

   Your Agency should establish procedures for virus prevention, detection, and removal.

   Consider the following when implementing anti-virus protection:

   - Include appropriate content in your agency security training program to help employees reduce the threat of viruses.
   - Use off-the-shelf scanning tools on servers and desktops with appropriate scanning intervals (at least once a week).
   - Implement appropriate response mechanisms to alert others to the discovery of found viruses, including communication to a security administrator and other users who may be at risk.
   - Develop a plan to deal with detected viruses that you cannot delete, including disconnection from the network and cleansing of hard disks.
   - Scan files at the server or firewall level for viruses.
   - Review virus scanning logs by system administrators.

5. Secure SGN connectivity

   No applicable guidelines for this specific standard. If your agency is interested in establishing a connection to the State Government Network, submit a request to net-change@dis.wa.gov.

6. Web browser and e-mail client security

   Establish procedures to control interactive Internet technologies such as ActiveX and Java scripts:

   - Include appropriate content in your agency security training program addressing the potential risks of downloading applets.
   - Configure browsers to accept applets from only trusted servers.

7. Web server security

   No applicable guidelines for this specific standard.

## E. Access security guidelines

The following guidelines will help you develop, document, and implement the access security aspects of an IT security program.

1. General access security

   Put in place appropriate access controls and technologies to control end-user access to agency applications. When allowing access from the Internet, consider using encryption protocols, such as Secure Sockets Layer (SSL), to provide authenticated, encrypted communication between the end-user and the application.

   Consider the following logon and password controls for your agency security program for site access control:

   - Control all system access by using security software that validates passwords and authorization codes.
   - Require written requests for Logon IDs.
   - Do not allow the use of shared Logon IDs, except for authorized and approved business justification or when shared Logon IDs are the only practical solution.
   - Do not allow concurrent use of Logon IDs.
   - Cancel workstation access authorizations when a workstation has been inactive for a specified length of time.
   - Assign Logon IDs to specific individuals rather than functions or groups of individuals.
   - Require individuals to change passwords as soon as they expire with a limit of one grace logon. Where not supportable by Operating System functionality, address this in policy.
   - Allow owner of Logon ID to change his/her own password.
   - Require the user at his/her first logon to change all passwords. Where not supportable by Operating System functionality this should be addressed in policy.
   - Prevent users from displaying or sharing their passwords.
   - Exclude passwords from batch files.
   - Prevent users from reusing passwords for a minimum of five iterations.

- Cancel or deactivate Logon IDs when an individual leaves the organization or has a change in responsibilities.
- Delete or deactivate Logon IDs that have been inactive for more than six months.
- Review personnel reports of former employees and verify that you have deleted their workstation access rights.

When your Internet authentication risk level assessment (see Section II. E. 3. - *Internet Access*) indicates that authentication processes and mechanisms stronger than those provided by user ID and passwords be used, you should consider authentication tools such as digital certificates. Digital certificates used should be issued by a licensed Washington state certification authority according to the terms of the Washington State Certificate Policy.

2. Remote access

Remote access is end-user access to agency computing resources through a non-state controlled network, device, or medium.

Proper configuration of end-user access devices is the first line of defense in securing remote system access. In order to ensure the protection and integrity of the systems and data being accesses, your agency should:

- Require virus detection software with current signatures on all remote access devices.
- Establish methods of maintaining current patches for the operating system and all applications installed on the user access device.
- Require a hardware firewall on all broadband connections used by a remote access device.
- Require the user of personal firewall software on remote PCs and laptops.
- Consider using encrypted file systems, especially on mobile devices such as laptops.

Allow connection of employee-owned equipment to agency resources only through “indirect” (proxy type) technologies, including properly configured Citrix or Outlook Web Access, as opposed to technologies that allow the client to become a “remote node” on the network (i.e. dial-up connections).

a. Use of dial-up lines

Consider the following dial-up line usage issues in agency security programs:

- Control the use of dial-up connections to the computer systems and workstations to prevent unauthorized access attempts.
- Identify the dial-up connections that are available within the telecommunications network. Determine whether the existing dial-up connections are necessary and have been approved by management.
- Prevent unauthorized access attempts, when the sensitivity of data is of great importance, by installing "call back" or "see through" security devices or logical network security passwords on all dial-up connections.
- Prevent, whenever possible, accidental line detection, assign dial-up access numbers to a three-digit exchange number that is different from the organization's main telephone exchange.
- Establish procedures to authorize user access to the dial-up system and screen all users prior to authorization.
- Change dial-up access telephone numbers on a periodic basis when possible and cost-effective.

b. Maintaining logs of remote connections

Ensure that the security system logs all unsuccessful password or authorization code access attempts.

c. Monitoring remote access by vendors

Consider the following issues in agency security programs regarding the use of manufacturer, software vendor, and third-party access lines:

- Monitor the use of manufacturer, software vendor, and third party dial-up access lines to the computer system.
- Change access numbers and access codes frequently.
- Establish procedures for reporting unauthorized entry or attempts to the appropriate security function.

d. Policies and procedures for Virtual Private Network (VPN) services

Document how your agency plans to support the following processes regarding the use of VPN:

- Document requirements for a VPN and how you plan to review them.
- Manage your security policy equivalency between networks through regular reviews and updates.
- Provide backup connections for high impact applications in the event of an ISP outage or denial of service.

The security risk of implementing a VPN solution without a centralized authentication and validation service is identical to consenting to an agency having dual connections to the internet, one being inside the state firewall and the other outside.

3. Internet access

The following guidelines will help you determine the level of risk associated with your agency's Internet-based application. Once you have conducted a data classification analysis, (see Section II. C. 1. - *Data Classification*), and intend to make information available or conduct transactions with internal users, customers, business partners, or the general public via the Internet, consider and document your agency risk assessment process based on the following:

**Step 1**- Determine mandated requirements

Before completing an assessment of the appropriate authentication risk level, consider the following questions:

Do any transactions involved in the application in question require a legally binding signature? If the answer is yes, under the Washington Electronic Authentication Act (Chapter 19.34 RCW) you must use a digital certificate issued by a licensed Certificate Authority.

Is the data or transaction subject to legal or policy-based restrictions outside the scope of the State of Washington Information Technology Security Policy? If the answer is yes, before initiating Step 2 of the assessment process, determine if the laws or policies mandate specific authentication mechanisms.

Does the application involve the processing of high dollar value transactions? If the answer is yes, consider using a high-level authentication mechanism.

**Step 2** - Quantify potential impacts

In order to determine the appropriate identification and authentication practice and authentication mechanism, consider the following questions and issues and quantify your risk assessment of the issues based on the provided guidelines.

## Authentication Risk Level Determination Chart

| Question/Issue | Impact Quantification Guidelines (0-5)<br>0 - No impact 1 - Minimal impact<br>3 - Some impact 5 - High impact | | | Total Score by Issue |
|---|---|---|---|---|
| | Fiscal | Operational | Customer | |
| What is the potential impact of unauthorized viewing of the data by outside intruders? | | | | |
| What is the potential impact of unauthorized viewing of the data by legitimate users? | | | | |
| What is the potential impact of the use of the information assets for other than authorized purposes? | | | | |
| What is the potential impact of unauthorized deletion, modification, or disclosure of information? | | | | |
| What is the potential operational impact if the service becomes unavailable (denial of service attacks)? | | | | |
| What is the potential cost impact if the services provided by the system become unavailable (denial of service attacks)? | | | | |
| What is the potential public confidence impact if the services or data provided by the system are compromised? | | | | |
| How important is non-repudiation (inability of a user to deny the initiation of a transaction) to the transactions supported by the system? | | | | |
| | | | Overall Score: | |

**Step 3** - Document conditions and assumptions

Prepare a brief narrative, which documents the conditions and assumptions used in completing the impact quantification in Step 1.

If your agency must use encryption processes and/or mechanisms to support your Internet application – other than those supported by the Washington State Digital Government framework – document the processes and/or mechanism.

**Step 4** - Determine level of risk

After quantifying the impact of potential security and operational issues and documenting conditions and assumptions, use the table below as a guide for determining the appropriate risk level. After determining the appropriate risk level, select an authentication mechanism that addresses the associated risk.

| Impact score | Level of risk |
|---|---|
| 0-10 | No or little risk |
| 10-20 | Low risk |
| 20-30 | Moderate risk |
| 30-40 | High risk |

The table above is a guideline to help agencies determine the appropriate authentication and protection mechanism based on the level of risk. Other non-security risk factors, such as cost or user impact, may cause an agency to select a higher or lower assurance level. In such cases, document these factors in the narrative completed in Step 3.

4. Secure access mechanisms

   Ensure that you have put in place appropriate access controls and technologies to control end-user access to agency applications. When allowing access from the Internet, consider the use of encryption protocols, such as Secure Sockets Layer (SSL), to provide authenticated, encrypted communication between the end-user and the application.

   When your data classification analysis (see Section II. C. 1. - *Data Classification*) and Internet authentication risk level assessment (see Section II. E. 3. - *Internet Access*), indicate that authentication processes

and mechanisms stronger than those provided by user ID and passwords be used, consider using strong authentication mechanisms.

Strong authentication is a process that determines the authenticity of the user's identity on the basis of at least two of the three following factors:

- Something you know — (e.g. the user name and password).
- Something you have – (e.g. secure ID token or digital certificate).
- Something you are – (e.g. fingerprints or specific physical traits).

When you require a user to present "something they have" (e.g. one time password generated by a secure ID token or digital certificate), ensure that the token is securely issued to prevent someone, other than the intended user, from gaining access to the token. If you use digital certificates, they should be issued by a licensed Washington State Certificate Authority, consistent with the terms set forth in the Washington State Certificate Policy.

### III. Guidelines for digital government (Internet) application submittal

No applicable guidelines for this specific standard.

## MAINTENANCE

Periodically, we will need to revise policies, standards, and guidelines due to technology advances and changes in the business requirements of agencies. The Department of Information Services is responsible for routine maintenance of these policies, standards, and guidelines to keep them current. Major policy changes will require the approval of the ISB.

## APPENDIX A - IT SECURITY PROGRAM DEVELOPMENT RESOURCES

There are many sources of information on the Internet that your agency can use to formulate effective IT security programs. These include:

wacirc.wa.gov
www.cert.org
www.sans.org
www.microsoft.com/security
www.gocsi.org
www.us-cert.gov
www.ciac.org/ciac/related_sites.html
www.first.org
www.nsi.org/compsec.html

# APPENDIX B – SAMPLE INTERAGENCY DATA SHARING AGREEMENT

(Consult with appropriate legal counsel prior to executing a data sharing agreement)

NOTE: **Use this template when developing a Data Sharing Agreement (DSA) between <AGENCY> and other state agencies** WHEN <AGENCY> IS SENDING/PROVIDING DATA TO THEM. **The model includes many terms commonly used in DSAs, but you will need to customize each DSA you develop. Not all the terms that are included in this model will apply to some DSAs, or you may need to add terms that are not included in this template. Items in italics are notes explaining and/or providing optional terms for your consideration. Pay particular attention to the items marked *"Optional" or "Include as Applicable"* and determine appropriateness for your specific DSA.**

**This template is available in electronic format from the <AGENCY> Contract Office. The <AGENCY> Contract Office and the <AGENCY> Data Security Administrator must review all draft DSAs.**

## INTERAGENCY DATA SHARING AGREEMENT
## between
## the
## STATE OF WASHINGTON
## Department of_____
## and the
## <AGENCY>

This Interagency Data Sharing Agreement (DSA) is entered into by and between _____, hereinafter referred to as "____", and the <Agency>, hereinafter referred to as "<AGENCY>", pursuant to the authority granted by Chapter 39.34 RCW.

***AGENCY PROVIDING DATA: <AGENCY>***

| | | |
|---|---|---|
| **Agency Name** | | |
| Contact Name(s): | Agreement Administrator: | Technical Administrator: |
| Title: | | |
| Division: | | |
| Address: | | |
| Phone: | | |
| E-mail: | | |

***AGENCY RECEIVING DATA: (Referenced in this document as Receiving Party (XXX) for example purposes only. The correct name or initials of the agency, and whichever role is appropriate for <AGENCY>, will be used in the final document.)***

| | | |
|---|---|---|
| **Agency Name** | | |
| Contact Name(s): | Agreement Administrator: | Technical Administrator: |
| Title: | | |
| Division: | | |
| Address: | | |

Phone:
E-mail:

This DSA has been reviewed by the authorized IT Data Security Administrator in each agency, as applicable.

## 1. PURPOSE OF THE DSA

The purpose of this DSA is to provide the XXX . . .

## 2. DEFINITIONS

"Agreement" means this Interagency Data Sharing Agreement, including all documents attached or incorporated by reference.

"Data Access" refers to rights granted to XXX employees to directly connect to <AGENCY> systems, networks and /or applications via the State Governmental Network (SGN) combined with required information needed to implement these rights.

"Data Transmission" refers to the methods and technologies to be used to move a copy of the data between APD systems and XXX systems, networks and/or employee workstations.

"Data Storage" refers to the state data is in when at rest. Data can be stored on off-line devices such as CD's or on-line on XXX servers or XXX employee workstations.

"Data Encryption" refers to ciphers, algorithms or other encoding mechanisms that will encode data to protect its confidentiality. Data encryption can be required during data transmission or data storage depending on the level of protection required for this data.

"Personal Information" means information identifiable to any person, including, but not limited to, information that relates to a person's name, health, finances, education, business, use or receipt of governmental services or other activities, addresses, telephone numbers, social security numbers, drivers license numbers, credit card numbers, any other identifying numbers, and any financial identifiers.

## 3. PERIOD OF AGREEMENT

**This Agreement shall begin on _____, or date of execution, whichever is later, and end on _____, unless terminated sooner or extended as provided herein.**

## 4. JUSTIFICATION FOR DATA SHARING

Data is needed to . . .

## 5. DESCRIPTION OF DATA TO BE SHARED

*(**NOTE:** Include a description of the data that is requested, including data elements, time frames and format of the data, as necessary. Specify if the data provided can be linked to other data and under what conditions, as necessary. For example: Data shared will include the data contained in the agency's internal database that is described in this Agreement and will be updated through an automated process that runs daily on a server operated at . . . .).*

Data to be shared includes . . . .

## 6. DATA ACCESS

***Example:*** *Data access will be via terminal emulation software to be loaded on the appropriate XXX staff workstations. <AGENCY> will grant access permissions required to access the data defined above.*

## 7. DATA TRANSMISSION

*Example****: Data transmission will be via anonymous FTP using the State Governmental Network (SGN) – The FTP site will be server ABC123, e-mail attachment, sneaker net, floppy disk, CD, etc. (pick one).***

## 8. DATA STORAGE AND HANDLING REQUIREMENTS

***NOTE****: <AGENCY> needs to identify and include any constraints on XXX's handling of the data once in XXX's possession. Below paragraph is an example only.*

***Example:*** *All data provided by <AGENCY> will be stored in an encrypted form on a server with access limited to the least number of XXX staff needed to complete the purpose of this DSA.*

## 9. DATA ENCRYPTION *(If applicable)*

***Example:*** *<AGENCY> and XXX have agreed to use a software tool to encrypt data prior to transmission. The tool is _____ (Example: PKZIP PRO; the encryption algorithm to be use is Password + 3DES). The password will be transmitted separately from any data transmission event.*

## 10. INTENDED USE OF DATA

***Example****: The data described above shall be used for analysis purposes only to prepare required annual business summaries published by XXX.*

## 11. CONSTRAINTS ON USE OF DATA

This Agreement does not constitute a release of the data for the *XXX*'s discretionary use, but may be accessed only to carry out the responsibilities specified in RCW . . . . and for the purposes described herein. Any ad hoc analyses or other use of the data, not specified in this Agreement, is not permitted without the prior written agreement of <AGENCY>.

*If Applicable* - The raw data and analysis generated will not identify personal information by name, and will be used for summary reporting purposes only. Any and all reports utilizing the data shall be subject to review by _____ prior to publication or presentation.

The *XXX* is not authorized to update or change any data in the _____ system, and any updates or changes will be cause for immediate termination of this Agreement.

## 12. SECURITY OF DATA

A. Data Protection

XXX shall take due care and take reasonable precautions to protect <AGENCY>'s data from unauthorized physical and electronic access. XXX will strive to meet or exceed the requirements of the Information Services Board (ISB) policies and standards for data security and access controls to ensure the confidentiality, availability and integrity of all data shared.

B. Data Security Technology Standards

<AGENCY> will be responsible for providing data security technology standards that will ensure acceptable levels of data security to XXX. These data security technology standards will include clear definitions outlining when and where data should be encrypted and by what technologies.

***Example:*** *<AGENCY> requires XXX to use the DIS Secure FTP service. <AGENCY> will cover all costs associated with this service.*

C. IT Data Security Administration

<AGENCY> and XXX IT Data Security Administrators will exchange documentation that outlines the data security program components supporting this Agreement. This documentation will define all data security methods and technology for each individual data exchange to ensure <AGENCY> and XXX are in compliance with all appropriate ISB security standards.

This documentation will serve to satisfy any potential requirement each agency may have under ISB Security Standards to document the management of secure information.

## 13. NON-DISCLOSURE OF DATA

Before receiving the data identified above, the XXX shall notify all staff who will have access to the data of the following requirements. This notification shall include all IT support staff as well as staff who will use the data. A copy of this notification shall be provided to <AGENCY> at the same time it is provided to relevant XXX staff.

A. Non-Disclosure of Data

1. XXX staff shall not disclose, in whole or in part, the data provided by <AGENCY> to any individual or agency, unless this Agreement specifically authorizes the disclosure. Data may be disclosed only to persons and entities that have the need to use the data to achieve the stated purposes of this Agreement.

2. XXX shall not access or use the data for any commercial or personal purpose.

3. Any exceptions to these limitations must be approved in writing by <AGENCY>.

B. Penalties for Unauthorized Disclosure of Information

In the event the XXX fails to comply with any terms of this Agreement, <AGENCY> shall have the right to take such action as it deems appropriate. The exercise of remedies pursuant to this paragraph shall be in addition to all sanctions provided by law, and to legal remedies available to parties injured by unauthorized disclosure.

The XXX accepts full responsibility and liability for any violations of the Agreement.

C. Employee Awareness of Use/Non-Disclosure Requirements

The XXX shall ensure that all staff with access to the data described in this Agreement are aware of the use and disclosure requirements of this Agreement and will advise new staff of the provisions of this Agreement.

XXX will provide an annual reminder to staff of these requirements. ***(Optional)***

## 14. DATA CONFIDENTIALITY

**(*NOTE*:** *Include these terms if the data is confidential. If the data being accessed by the XXX includes protected health information, as defined in the Health Insurance Portability and Accountability Act (HIPAA) of 1996, refer to Exhibit B and include HIPAA terms in the document as applicable.)*

A. Regulations Governing Confidentiality of Data

1. The *XXX* acknowledges the confidential nature of the information and agrees that *XXX* personnel with access shall comply with all laws, regulations and policies that apply to protection of the confidentiality of the data.

2. This data is confidential under state (NOTE: include if applicable: and Federal law), access and use of this information will be limited only to persons whose staff function requires such access.

B. Limited Access to Data (Use as Applicable)

Individuals will access data only for the purpose of this Agreement. Each individual with data access shall read and sign Exhibit A, "Statement of Confidentiality and Non-Disclosure," prior to access to the data.

**15. OVERSIGHT**

The XXX agrees that <AGENCY> will have the right, at any time, to monitor, audit, and review activities and methods in implementing this Agreement in order to assure compliance therewith, within the limits of RP's technical capabilities.

**16. AMENDMENTS AND ALTERATIONS TO THIS AGREEMENT**

With mutual consent, <AGENCY> and the XXX may amend this Agreement at any time, provided that the amendment is in writing and signed by authorized staff.

**17. TERMINATION**

Either party may terminate this Agreement with *(15, 20, 30)* days' written notice to the other party's Agreement Administrator named on Page 1. However, once data is accessed by the XXX, this Agreement is binding as to the confidentiality, use of the data, and disposition of all data received as a result of access, unless otherwise amended by the mutual agreement of both parties.

**18. DISPUTE RESOLUTION**

In the event that a dispute arises under this Agreement, a Dispute Board shall determine resolution in the following manner. Each party to this Agreement shall appoint one member to the Dispute Board. The members so appointed shall jointly appoint an additional member to the Dispute Board. The Dispute Board shall review the facts, contract terms, and applicable statutes and rules and make a determination of the dispute.

**19. GOVERNANCE**

A. The provisions of this Interagency Data Sharing Agreement are severable. If any provision of this Agreement is held invalid by any court that invalidity shall not affect the other provisions of this Interagency Data Sharing Agreement and the invalid provision shall be considered modified to conform to the existing law.

B. In the event of a lawsuit involving this Interagency Data Sharing Agreement, venue shall be proper only in Thurston County, Washington.

## 20. SIGNATURES

The signatures below indicate agreement between the parties.

**<AGENCY>**

_____ _____
SIGNATURE DATE

*TITLE:* _____

**DEPARTMENT OF_____**

_____
SIGNATURE DATE

*TITLE:* _____

**EXHIBIT A**

***NOTE: Use this document if <AGENCY> is sending confidential data to another agency. Agency staff who will have access to the data must each sign this document and return it to <AGENCY>, per the terms of Section 11, Paragraph A, "Limited Access to Data".***

## STATEMENT OF CONFIDENTIALITY AND NON-DISCLOSURE

between the
State of Washington

**<AGENCY>**
and the

_____

**<AGENCY> DSA No. _____**

As an employee of the Washington State _____, I have access to information contained in the _____ of the State of Washington, <Agency> (<AGENCY>). This information is confidential, and I understand that I am responsible for maintaining this confidentiality. I understand that the information may be used solely for the purposes of work under <AGENCY> DSA No. _____.

Before you are allowed access to the information in the data, you are required to sign the following statement:

- I have been informed and understand that all information in the <AGENCY> ____ is confidential and may not be disclosed to unauthorized persons. I agree not to divulge, transfer, sell, or otherwise make known to unauthorized persons any information contained in this system.

- I also understand that I am not to access or use this information for my own personal information but only to the extent necessary and for the purpose of performing my assigned duties as an employee of _____ under this Agreement. I understand that a breach of this confidentiality will be grounds for disciplinary action which may also include termination of my employment and other legal action.

- I agree to abide by all Federal and state laws and regulations regarding confidentiality and disclosure of the information in the ___.

_____
Signature of Employee

_____
Printed Name of Employee

_____
Date

**EXHIBIT B** (Reference name for the purposes of this template only.)

**HIPAA PROVISIONS: If <AGENCY> will be receiving data that includes protected health information about individuals from a "Covered Entity", as defined below, then <AGENCY> will be defined as a Business Associate in the Data Sharing Agreement (DSA) in accordance with the Health Insurance Portability and Accountability Act of 1996. The following definitions and terms would be included in the DSA.**

**A. DEFINITIONS**

"Covered Entity" means _____, a Covered Entity as defined in 45 CFR 160.103. *(NOTE: For example, DSHS is a Covered Entity based on this law.)*

"Business Associate" means <AGENCY>, who performs or assists in the performance of an activity for or on behalf of the Covered Entity that involves the use or disclosure of protected health information (PHI). Any reference to Business Associate under this Data Sharing Agreement includes all <AGENCY> staff.

"Designated Record Set" means a group of records maintained by or for the Covered Entity that is the medical and billing records about individual or the enrollment, payment, claims adjudication, and case or medical management records, used in whole or in part by or for the Covered Entity to make decisions about individuals.

"HIPAA" means the Health Insurance Portability and Accountability Act of 1996, as codified at 42 USCA 1320d-d8.

"Individual" means the person who is subject of PHI and includes a person who qualifies as a personal representative in accordance with 45 CFR 164.502(g).

"PHI" means protected health information and is information created or received by Business Associate from or on behalf of Covered Entity that relates to the provision of health care to an individual; the past, present, or future physical or mental health or condition of an individual; or past, present, or future payment for provision of health care to an individual. 45 CFR 160 and 164. PHI includes demographic information that identifies the individual or about which there is reasonable basis to believe, can be used to identify the individual. 45 CRR 160.103. PHI is information transmitted, maintained, or stored in any form or medium. 45 CFR 164.501. PHI does not include education records covered by the Family Educational Right and Privacy Act, as amended, 20 USCA 1232g(a)(4)(B)(iv).

**B. COMPLIANCE**

Business Associate shall perform all Agreement duties, activities and tasks in compliance with HIPAA and regulations enacted pursuant to its provisions, successor law and/or regulation. Pursuant to 45 CFR 164.502(e), Business Associate shall implement policies and procedures to safeguard and maintain PHI in accordance with

the requirements of state and Federal law. In the event of a conflict of interpretation of Agreement terms relevant to HIPAA, the language and intent of this Agreement shall control.

**C. USE AND DISCLOSURE OF PHI**

Business Associate is limited to the following permitted and required uses or disclosures of the PHI:

1. Business Associate shall only use or disclose PHI as required to perform the services specified in this Agreement or as required by law, and shall not use or disclosure such PHI in any manner inconsistent with the use and disclosure restrictions placed on the Covered Entity by HIPAA, or the resulting policies and procedures of the Covered Entity.

2. Business Associate shall protect PHI from, and shall establish appropriate safeguards to prevent, the unauthorized disclosure of PHI in accordance with the terms and conditions of this Agreement and state and Federal law, including any regulations governing the security of PHI and the transmission, storage or maintenance of electronic data that contains PHI for as long as the PHI is within its possession and control, even after the termination or expiration of this Agreement.

**D. REPORT OF UNAUTHORIZED USE OR DISCLOSURES OF PROTECTED HEALTH INFORMATION**

Business Associate shall report in writing all unauthorized uses or disclosures of PHI to the Covered Entity within five (5) working days of becoming aware of the unauthorized use or disclosure of the PHI.

**E. THIRD PARTY AGREEMENTS**

If subcontracting is permitted under the terms of this Agreement, then Business Associate shall enter into a written agreement with any agent, subcontractor, independent contractor, volunteer, or any other third party with access to PHI, that contains the same terms, restrictions, and conditions as this Agreement.

**F. CONSENT TO AUDIT**

Business Associate shall give reasonable access to PHI, records, books, documents, electronic data and/or all other business information received from, or created or received by Business Associate on behalf of Covered Entity, to the Secretary of the U.S. Department of Health and Human Services or designee and/or to the Covered Entity for use in determining Covered Entity's compliance with HIPAA privacy requirements.

**G. RETURN OF INFORMATION**

Business Associate shall, within ten (10) working days of termination or expiration of this Agreement, in accordance with Contract Termination and Expiration Procedures, and at the discretion of Covered Entity, either return or destroy all PHI, including PHI in possession of third parties under contract to Business Associate.

**H. ACCOUNTING OF DISCLOSURES**

Business Associate shall document all disclosures of PHI and information related to such disclosures. Within ten (10) working days of a request from Covered Entity, Business Associate shall provide Covered Entity with an accounting of those disclosures of PHI, as required by 45 CFR 164.504 and 164.528.

**I. PHI AMENDMENT**

Business Associate shall, within ten (10) working days of a request from Covered Entity, provide Covered Entity with information regarding amendment of PHI contained in a Designated Record Set. Business Associate will, as directed by Covered Entity, thereafter incorporate any amendments to the PHI in the Designated Record Set. 45 CFR 164.526.

**J. PHI ACCESS**

Business Associate shall provide Covered Entity with reasonable access to PHI in a Designated Record Set. Or as directed by Covered Entity, Business Associate shall provide an individual with reasonable access to such PHI. 45 CFR 164.524.

**K. INDIVIDUAL'S ACCESS TO INFORMATION**

If any individual asks Business Associate for an accounting of disclosure of PHI, or for access to or amendment of PHI in a Designated Record Set, Business Associate shall within two (2) working days forward the request to the Covered Entity for response.