

Minimum Data Security Standards (Data Classification and Related Measures of Protection)

University of Washington

September 2005 // Revised 10/24/05 // Revised 12/06/05 // Revised 1/10/06
Edits (EL) 1/20/06, Edits (KS) 3/6/06, Edits (KB) 10/11/06// Revised 02/20/07,
Edits (KB) // Edits 4/25/07 (KB, BN)

Prepared by:

Privacy Assurance and Systems Security Council (PASS Council)
Kirk Bailey, UW Chief Information Security Officer, Chair

Prepared for:

The University Technology Advisory Committee

Table of contents

1. <i>Background</i>	2
1.1. Context.....	2
1.2. Purpose.....	2
1.3. Applicability.....	2
1.4. Audience.....	2
2. <i>Data Classification and Examples</i>	3
3. <i>Controls for Protection of Data</i>	5
3.1. Records Management (Retention and Disposal of Data).....	5
3.2. System Owners and Data Custodians: Roles and Responsibilities.....	5
3.3. Access Control Principles.....	5
3.4. “Controlled” Computer.....	6
3.5. Controlled Application.....	7
4. <i>Protective Measures for Data</i>	7
4.1. Protective Measures for Public Data.....	7
4.2. Protective Measures for Restricted Data.....	7
4.3. Protective Measures for Confidential Data.....	7
4.4. Reference Matrix for Data Protection Measures.....	8
<i>Section 5. Exemptions</i>	9
<i>Section 6. Reporting</i>	9
<i>Section 7. Enforcement</i>	9
<i>Appendix A. Glossary</i>	10
<i>Appendix B. References</i>	11

Section 1. Background

1.1. Context for the Minimum Data Security Standards

The University of Washington (UW) solicits, acquires, generates, and maintains a large amount of electronic information. In addition, the UW often enters into relationships with third parties who, as an aspect of the relationship, maintain electronic information. The UW is often legally required and frequently otherwise desires for privacy reasons, to limit access to, and to the limit the distribution and disclosure of, electronic information.

This document describes standards that are specific to the protection of UW information assets in electronic form (data). The intent of these standards is to support existing UW policy and information protection objectives by defining a minimum set of security standards that also support the UW's compliance requirements.

Proper protection of data is determined by a combination of compliance requirements mandated by state and federal government statutes and regulations, accepted best practices, and institutional risk management decisions. The approach taken at the UW is to adopt a classification scheme for all data and to define measures and practices that provide appropriate protection for each class of data.

1.2. Purpose

The Minimum Data Security Standards describe the minimum standards the UW will strive to achieve, in appropriate circumstances, to limit access to, and to limit the distribution and disclosure of, electronic information. This Standard should be read and applied in conjunction with a Policy document which it serves, the [UW Information Systems Security Policy](#) and a companion Security Standard, the UW [Minimum Computer Security Standards](#). Together, these three documents strive to prevent:

- Unauthorized internal access to electronic information
- Unauthorized external access to electronic information
- Illegal or otherwise inappropriate use of UW electronic information
- Loss, corruption, or theft of UW electronic information

1.3. Applicability

This minimum data security standard applies to all data associated with UW business; to any other data caches covered by statutory or regulatory compliance requirements that are found in all UW colleges, schools, departments, and other business units; and to data caches on UW affiliates' information systems. Data associated with UW hosted research efforts that represent significant intellectual property interests also are subject to this standard, and, in addition, may be subject to other specific protective requirements.

Any questions about the applicability of this standard can be forwarded to the UW Chief Information Security Officer for review by the PASS Council.

1.4. Audience

The targeted audience for this standard includes all UW *system owners* and *designated data custodians* (see Appendix A, Glossary). It also is for all individuals who have access to and use UW information systems and data assets.

Section 2. Data Classification and Examples

The nature of the data largely determines what measures and operational practices need to be applied to protect it. To help clarify the various minimum requirements for UW data security, three categories of data have been defined. It is essential that those who are accountable for protecting the data (e.g., system owners and data custodians) understand and inventory their data assets according to these categories.

- **CONFIDENTIAL:** Data that is very sensitive in nature and typically subject to federal or state regulations. Unauthorized disclosure of this data could seriously and adversely impact the university or the interests of individuals and organizations associated with the university.
- **RESTRICTED:** Data that is generally circulated and subject to disclosure laws, yet sensitive enough to warrant careful management and protection to ensure its integrity, appropriate access, and availability.
- **PUBLIC:** Data that is published for public use or has been approved for general access by the appropriate UW authority.

In most cases, it will be obvious how to categorize data. When in doubt about how a particular data element or set of data should be classified, the safe “rule of thumb” is to default to the higher classification of the choices involved. In other words, it is better to err on the side of privacy and security protection until clarification can be obtained.

For electronic information where the integrity of the data is important, but the data itself classified as “Public” (e.g. UW financial business records), the source of the data – “the master data” (application, database, authorized data collection point, etc.) should be treated as “Restricted” and the published versions of those data (e.g. reports) can be treated as “Public” data.

Any questions about the classification of data can be forwarded to the UW Chief Information Security Officer for review by the PASS Council.

Table 1. clarifies the nature of each data category and provides criteria for determining which classification is appropriate for a particular set of data. When using this table, a positive response for the most restrictive (highest risk) category in any row is sufficient to place that set of data into that category.

Table 1. Data Classification Categories

	CONFIDENTIAL	RESTRICTED	PUBLIC
Legal Requirements	Protection of data is required by law. (See examples of specific HIPAA and FERPA data elements below.)	UW has a contractual obligation or best practice (due care) reason to protect the data.	
Risk Level	High	Medium	Low
Examples of Risk	The UW’s reputation is tarnished by public reports of its failures to protect sensitive records of employees, students, or clients.	Data is disclosed unnecessarily or in an untimely fashion, which causes harm to UW business interests or to the personal interests of an	Confusion is caused by corrupted information about enrollment and tuition that is displayed on the official UW Web site.

		individual.	
	CONFIDENTIAL	RESTRICTED	PUBLIC
Examples of Specific Data	<ul style="list-style-type: none"> • HIPAA – protected data <i>when associated with a health record</i>¹ <ul style="list-style-type: none"> - Patient names - Street address, city, county, zip code - Dates (except year) for dates related to an individual - Social Security Numbers - Health conditions and symptoms - Prescriptions - Account/Medical rec. #s - Health plan beneficiary information - Certificate and license #s - Vehicle ID and serial #s - Device ID and serial #s - Biometric identifiers - Full-face images - Any other unique identifying number, characteristic, or code - Payment guarantor's information - Telephone and fax #s - Email, URLs, and IP #s • FERPA – individual student records² <ul style="list-style-type: none"> - Grades - Courses taken - Schedule - Test scores - Advising records - Educational services received - Disciplinary actions - Student ID # - SSN - Student private email (with exceptions related to UW business) • Export Controls (e.g., EAR, ITAR)³ • Gramm-Leach-Bliley (GLB)⁴ <ul style="list-style-type: none"> - Employee financial account information - Student financial account information (aid, grants, bills) - Individual financial information - Business partner and vendor financial account information • Employee information <ul style="list-style-type: none"> - Social Security Number - Date of birth - Home address or personal contact information - Performance reviews - Specific benefit selections • Donor information • Library use records 	<ul style="list-style-type: none"> • UW NetID account information • Contact information between the UW and business partners or vendors • Employee Internet usage • Telephone billing information • Parking permits • Location of assets • Critical infrastructure blueprints or schematics • Specific physical security measures • Specific technical security measures • Proprietary research • UW employee business-related email (including student employees, but only their work-related email) 	<ul style="list-style-type: none"> • Campus promotional material • Annual reports • Press statements • Job titles • Job descriptions • Employee work phone numbers (with special exceptions) • Employee work locations (with special exceptions) • Employee email addresses (with special exceptions) • Value and nature of fringe benefits • University of Washington business records

	<ul style="list-style-type: none"> • Trade secrets, intellectual and/or proprietary research information • Information required to be protect by contract • Vendor non-disclosure agreements • Attorney/client privileged records • Restricted police records (e.g., victim information, juvenile records) • Computer account passwords • Certain affirmative action related data⁵ 		
--	--	--	--

¹For more information on HIPAA:
http://www.washington.edu/research/hsd/faq_hipaa.html

²For more information on FERPA: <http://www.washington.edu/students/reg/ferpafac.html>

³For more information on Export Controls: <http://www.washington.edu/research/osp/ecr.html>

⁴For more information on GLB: <http://www.ftc.gov/privacy/glbact/glb-faq.htm>

⁵For more information on UW Affirmative Action Policy:
http://www.washington.edu/admin/eoo/hb_Vol-IV_Non-discr.html

Section 3. Controls for Protection of Data

This section outlines the controls that are necessary to implement the protective measures outlined in Section 4, Protective Measures for Data.

3.1. Records Management (Retention and Disposal of Data)

This standards document is specific to measures and practices necessary for the protection of electronic UW data. Everyone who is accountable for the management or use of UW data must also become familiar with other university-wide and departmental policies and procedures related to records management that are published separately. These include records retention policy and procedures for the proper disposal of electronic media and paper records. For details, see the Records Retention and Confidentiality Web page:
<http://www.washington.edu/admin/hr/pol.proc/cdl/recordsReten.html>

3.2. System Owners and Data Custodians: Roles and Responsibilities

Section 6 of the *UW Information Systems Security Policy* defines the specific roles and responsibilities of groups and individuals within the university. These roles and responsibilities form the basis of accountability for and functional requirements of the protection of UW information systems. The roles of the *system owner* and *data custodian* are key to successful data protection practices. All individuals who have been designated as a *system owner* and/or *data custodian* should review their responsibilities as specified in these *Minimum Data Security Standards*, the *UW Information Systems Security Policy*, and the *Minimum Computer Security Standards*.

3.3. Access Control Principles

A required measure for protecting both confidential and restricted data is an *access control system* (see Appendix A, Glossary) that has physical, technical, and procedural elements. Any

access control measure established by a *system owner* or *data custodian* must be implemented and maintained in compliance with the *principle of least privilege* and the *principle of separation of duties* (see Appendix A, Glossary) as specified in the *UW Information Systems Security Policy*.

3.4. “Controlled” Computer

All computer systems that host confidential data or applications that use restricted data must be carefully controlled in terms of their configuration, operation, maintenance, and security measures.

It is the responsibility of the owner of the controlled computer to ensure that all management requirements are met. Controlled computers must be managed with a level of care and professional support that includes the following:

3.4.1. Controlled computers will meet all UW minimum computer security standards.

3.4.2. Controlled computers must be managed to professional standards, preferably by well-trained or certified employees or contractors with sufficient knowledge and resources to ensure that data on them are properly secured.

3.4.3. Operating systems and applications on controlled computers must be patched to and maintained at the most current level provided by their manufacturers.

3.4.4. Controlled computers should run no programs or services that are not necessary to their core purpose. For example, controlled computers that contain sensitive data should not run Web or file-sharing services, since these are frequently targeted and compromised by outsiders. Network-aware client software on controlled computers, such as Web browsers or email readers, should block the automatic execution of attachments, graphical files, or other common carriers of computer viruses, Trojans, or worms.

3.4.5. Controlled computers must prevent unauthorized users from running programs or accessing raw data. For example, there should be no "guest," shared or general-purpose accounts on controlled computers. User accounts should be limited to the minimum necessary for the operation of the computer and its core functions. Accounts with substantial system-administration privileges should be granted only to a few individuals with general management responsibility for the systems in question, and never to individuals without UW faculty or staff appointments. In general, system-administrator and similar "root" accounts should be used only when strictly required, and never when use of a less privileged account could achieve the same purpose.

3.4.6. User-authentication processes must encrypt or otherwise protect username and password exchanges from interception. In general, login or shell access to controlled computers must be restricted to the campus network and/or with secured remote access (security industry best practices) including two-factor authentication mechanisms.

3.4.7. All user passwords associated with administrative access to controlled computers should meet or exceed UW policy for complexity guidelines. In addition, users with extensive access to controlled computers should avoid using the corresponding passwords for other purposes.

3.4.8. Controlled computers must be reasonably secured against unauthorized access, including data interception and compromise. For example, controlled computers must connect to the network using technologies that are reasonably secure from sniffing, which excludes unencrypted hub or wireless connections. Controlled computers must run antivirus and anti-spyware software, updating definition files frequently. They should run host-based firewall or equivalent port-blocking software, configured to disable all ports not necessary for system functioning.

3.4.9. Controlled computers must be provided physical security measures necessary to prevent theft, tampering, or destruction.

3.4.10. Controlled computers must subscribe to a regimented backup process to ensure data integrity, system availability, and business continuity functions as required.

3.5. Controlled Application

All applications that handle confidential data must be written in a way that ensures that the data is not inadvertently exposed, either through errors in design or coding or by not implementing appropriate security measures (e.g., encryption, authorization, and authentication). In addition, Web application code must meet Open Web Application Security Project standards (see Section 4.3.2).

Section 4. Protective Measures for Data

This section outlines the specific measures that must be taken and practices that must be followed by university units and personnel in order to adequately protect data owned or managed by the university.

4.1. Protective Measures for Public Data

The UW's minimum computer security standards are required for all computer systems that host public data. In addition, public data must be protected by the specific measures identified in Section 4.4 of this document, Reference Matrix for Data Protection Measures.

4.2. Protective Measures for Restricted Data

The UW's minimum computer security standards are required for all computer systems that host restricted data. In addition, restricted data must be protected by the specific measures identified in Section 4.4 of this document, Reference Matrix for Data Protection Measures.

4.3. Protective Measures for Confidential Data

4.3.1. The UW's minimum computer security standards are required for all computer systems that host confidential data. This basic requirement, along with several other specific measures, is identified in Section 4.4 of this document, Reference Matrix for Data Protection Measures.

4.3.2. Applications that are linked to databases or data files that contain sensitive data must meet the Open Source Web Application Security Project (OWASP) standards for secure coding (<http://www.owasp.org>). Owners of such applications are required to demonstrate compliance with these standards when audited or when requested by the UW CISO (Chief Information Security Officer).

4.3.3. Loading confidential data onto laptops and other portable computing and data storage devices (e.g., USB flash drives, CDs, PDAs, BlackBerries, etc.) is discouraged and restricted to unusual operational circumstances that require such action. If it is necessary to load confidential data on to a portable computing or portable data storage device, the data must be encrypted and password protected, or an equivalent access protection measure must be taken. A laptop or other portable computing device that has confidential data stored on it must be treated as a "controlled computer." It must also have additional security features to prevent unauthorized use of the system if it is lost or stolen.

4.3.4. Strong access control and management practices are required when non-UW employees (e.g. contractors, vendors) are provided data access. UW System Owners and Data Custodians must ensure that all such granted privileges are justified, controlled and are limited to only what is absolutely necessary. If confidential data is shared or given to an outside organization as part of required business activity, a data sharing agreement (contract) specific to the data sharing activity must be implemented. It must

include appropriate risk transfer language including: specific recitals that detail the data being shared, limits of its use, and related handling; indemnification terms; terms for oversight and verification of data protection measures that are agreed to be maintained.

4.4. Reference Matrix for Data Protection Measures

At a minimum, every computer on or directly connecting to the campus network that contains UW confidential or restricted data is required to be a “controlled computer” and must meet minimum computer security standards. In addition, the data on a UW computer may need to be protected with additional security measures, which are summarized in the matrix in Table 2.

Table 2. Matrix for System Security Measures for Data Classifications

PROTECTIVE MEASURE	DATA CATEGORY		
	CONFIDENTIAL	RESTRICTED	PUBLIC
Minimum Computer Security Standards	Yes	Yes	Yes
Access Control Measures (Authorization)	Yes (documented and audited for compliance once every three years)	Yes (documented)	Yes (limited to system administrators)
Log Reviews and Alerts	Logging alerts and regular reviews	Regular reviews	Basic logging and random periodic reviews
Authentication	Yes (two-layer Minimum)	Yes (two-layer recommended)	Configure computer access to: yes for “write,” none for “read”
Firewall Protection	Yes (per controlled computer requirements)	Yes	Yes (if feasible)
Backup and Recovery Processes	Yes (per controlled computer requirements)	Yes	Yes
Physical Security	Yes	Yes	Yes
Encryption (During Transmission)	Yes	Recommended	No
Encryption (Storage/Backups)	Recommended	Optional	No
Encryption (“Data at rest” on system)	Recommended	Optional	No

Personnel Criminal Background Check	Yes (as specified by UW Human Resources)	Yes (as specified by UW Human Resources)	Yes (as specified by UW Human Resources)
Data Sharing Agreements (with business partners, vendors and others who are given UW data)	Yes	No	No
Audit of Security Measures	Yes (minimum of once every three years and more frequent audits, if possible)	Yes (random sampling)	Recommended (random sampling)

Section 5. Exemptions

While rare and unwelcome, there are situations that may require exemptions from these standards. In accordance with the *UW Information Systems Security Policy*, the PASS Council is empowered to grant exemptions. For details, see *UW Information Systems Security Policy Development, Revision, and Exemption Processes*:

<http://www.washington.edu/computing/security/pass/is.sec.pol.revision.html>

In the case of UW Medicine, exemption requests must follow UW Medicine IT Services procedures before submission to the PASS Council.

Section 6. Reporting

When a breach of security is discovered that may have caused the compromise of confidential data, including a breach of security on a controlled computer, it is required that the incident be reported as soon as possible to C&C Security Operations.

Section 7. Enforcement

Enforcement of these minimum data security standards is the responsibility of the UW Chief Information Security Officer and the PASS Council, with support from Risk Management, Internal Audit, and Computing & Communications. Failure to comply with these standards may result in disciplinary action up to and including denial of access to information systems and data, and/or termination of employment at the UW.

Appendix A. Glossary

(From UW Information Systems Security Policy, Definitions)

Access Control System: Physical, procedural and/or electronic mechanism that ensures that only those who are authorized to view, update, and/or delete data can access that data.

Authorization: The process of giving someone permission to do or have something; a system administrator defines which users are allowed access to the system and what privileges are allowed for each user.

Confidentiality: An attribute of information. Confidential information is sensitive, contractually protected, or information whose loss, corruption, or unauthorized disclosure could be harmful or prejudicial.

Data Custodians: As defined in the UW Information Systems Security Policy, individuals who have been officially designated as being accountable for protecting the confidentiality of specific data that is transmitted, used, or stored on a system or systems within a department, college, school, or administrative unit of the UW and certain affiliated organizations.

Encryption: The process of turning readable text into unreadable (cipher) text, which requires the use of a decipher key to render it readable.

Ownership: The term that signifies decision-making authority and accountability for a given scope of control.

Personally Identifiable Information: Personally identifiable information is defined as data or other information that is tied to, or which otherwise identifies, an individual or provides information about an individual in a way that is reasonably likely to enable identification of a specific person and make personal information about them known.

Personal information includes, but is not limited to, information regarding a person's home or other personal address, social security number, driver's license, marital status, financial information, credit card numbers, bank account numbers, parental status, sexual orientation, race, religion, political affiliation, personal assets, medical conditions, medical records or test results, home or other personal phone numbers, non-university address, employee number, personnel or student records, and information related to the UW [Affirmative Action Policy](#)

Principle of Least Privilege: Access privileges for any user should be limited to only what they need to have to be able to complete their assigned duties or functions, and nothing beyond these privileges.

Principle of Separation of Duties: Whenever practical, no one person should be responsible for completing or controlling a task, or set of tasks, from beginning to end when it involves the potential for fraud, abuse or other harm.

Privacy: An individual right to be left alone; to withdraw from the influences of his or her environment; to be secluded, not annoyed, and not intruded upon; to be protected against the misuse or abuse of something legally owned by an individual or normally considered by society to be his or her property.

Security: An attribute of information systems practices that includes specific policy-based, procedural, and technical mechanisms and assurances for protecting the confidentiality and

integrity of information, the availability and functionality of critical services and the confidentiality of sensitive information.

Sensitive Information: General term for any information that requires access controls and other control measures to meet legal, policy and/or ethical requirements.

System: A network, computer, software package, or other entity for which there can be security concerns.

System Owners: As defined in the UW Information Systems Security Policy, individuals within the UW community who are accountable for the budget, management, and use of one or more electronic information systems or electronic applications that support UW business, client services, educational, or research activities that are associated or hosted by the UW.

Users: Any individual that has been granted access and privileges to UW computing and network services, applications, resources, and information.

Appendix B. References

Washington State Information Services Board IT Security Policy, Standards and Guidelines (<http://isb.wa.gov/policies/security.aspx>)

[UW Information Systems Security Policy](#)

[Minimum Computer Security Standards](#)