

**Minimum Data Security Standards:  
Data Classification and Related Measures of Protection**

**Table of Contents**

- 1. Background** ..... 2
  - a. Context for the Minimum Data Security Standards ..... 2
  - b. Purpose ..... 2
  - c. Applicability ..... 3
  - d. Audience ..... 3
- 2. Data Classification and Examples** ..... 3
- 3. Controls for Protection of Data** ..... 7
  - a. Records Management (Retention and Disposal of Data) ..... 7
  - b. System Owners and Data Custodians: Roles and Responsibilities ..... 7
  - c. Access Control Principles ..... 7
  - d. "Controlled" Computer ..... 8
  - e. Controlled Application ..... 9
- 4. Protective Measures for Data** ..... 9
  - a. Protective Measures for Public Data ..... 9
  - b. Protective Measures for Restricted Data ..... 9
  - c. Protective Measures for Confidential Data ..... 10
  - d. Reference Matrix for Data Protection Measures ..... 10
- 5. Exemptions** ..... 12
- 6. Reporting** ..... 12
- 7. Enforcement** ..... 12
- 8. Additional Information** ..... 12

## Minimum Data Security Standards: Data Classification and Related Measures of Protection

(Approved by the Provost and Executive Vice President by authority of Executive Order No. 4, Senior Vice President for Finance and Facilities by authority of Executive Order No. 5, and the Vice President of UW Technology by authority of Executive Order No. 63)

### 1. Background

#### a. 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 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.

#### b. Purpose

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 the policy statement it serves, APS 2.1, "UW Information Systems Security," and a companion Security Standard, the "UW Minimum Computer Security Standards" [<http://www.washington.edu/computing/security/pass/MinCompSec.html>]. 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.

---

## Minimum Data Security Standards: Data Classification and Related Measures of Protection

### c. 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 (CISO) for review by the Privacy Assurance and Systems Security (PASS) Council [<http://www.washington.edu/computing/security/pass>].

### d. Audience

The targeted audience for this standard includes all UW system owners and designated data custodians (see Definitions from APS 2.1, "UW Information Systems Security"). It is also for all individuals who have access to and use UW information systems and data assets.

## 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 UW or the interests of individuals and organizations associated with the UW. To avoid confusion with federal Executive Order 12958 for classified national security information, confidential documents and data may be labeled "UW Confidential."
- **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.

### Minimum Data Security Standards: Data Classification and Related Measures of Protection

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 is 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 CISO for review by the PASS Council.

The table below 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.

	Confidential	Restricted	Public
<b>Legal Requirements</b>	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.	
<b>Risk Level</b>	High	Medium	Low
<b>Examples of Risk</b>	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 individual.	Confusion is caused by corrupted information about enrollment and tuition that is displayed on the official UW Web site.
<b>Examples of Specific Data</b>	<ul style="list-style-type: none"> <li>• HIPAA — protected data <i>when associated with a health record</i><sup>1</sup></li> <li>- Patient names</li> <li>- Street address, city, county, zip code</li> <li>- Dates (except year) for dates related to an individual</li> <li>- Social Security numbers</li> </ul>	<ul style="list-style-type: none"> <li>• UW NetID account information</li> <li>• Contact information between the UW and business partners or vendors</li> <li>• Employee Internet usage</li> </ul>	<ul style="list-style-type: none"> <li>• Campus promotional material</li> <li>• Annual reports</li> <li>• Press statements</li> <li>• Job titles</li> <li>• Job descriptions</li> </ul>

## Minimum Data Security Standards: Data Classification and Related Measures of Protection

	Confidential	Restricted	Public
<b>Examples of Specific Data</b> <i>(continued)</i>	<ul style="list-style-type: none"> <li>- Health conditions and symptoms</li> <li>- Prescriptions</li> <li>- Account/Medical record numbers</li> <li>- Health plan beneficiary information</li> <li>- Certificate and license numbers</li> <li>- Vehicle identification and serial numbers</li> <li>- Device identification and serial numbers</li> <li>- Biometric identifiers</li> <li>- Full-face images</li> <li>- Any other unique identifying number, characteristic, or code</li> <li>- Payment guarantor's information</li> <li>- Telephone and fax numbers</li> <li>- Email, URLs, and IP numbers</li> <li>• FERPA — individual student records<sup>2</sup> <ul style="list-style-type: none"> <li>- Grades</li> <li>- Courses taken</li> <li>- Schedule</li> <li>- Test scores</li> <li>- Advising records</li> <li>- Educational services received</li> <li>- Disciplinary actions</li> <li>- Student identification number</li> <li>- Social Security number</li> <li>- Student private email (with exceptions related to UW business)</li> </ul> </li> <li>• Export Controls (e.g., EAR, ITAR)<sup>3</sup></li> </ul>	<ul style="list-style-type: none"> <li>• Telephone billing information</li> <li>• Parking permits</li> <li>• Location of assets</li> <li>• Critical infrastructure blueprints or schematics</li> <li>• Specific physical security measures</li> <li>• Specific technical security measures</li> <li>• Proprietary research</li> <li>• UW employee business-related email (including student employees, but only their work-related email)</li> </ul>	<ul style="list-style-type: none"> <li>• Employee work phone numbers (with special exceptions)</li> <li>• Employee work locations (with special exceptions)</li> <li>• Employee email addresses (with special exceptions)</li> <li>• Value and nature of fringe benefits</li> <li>• University of Washington business records</li> </ul>

**Minimum Data Security Standards:  
Data Classification and Related Measures of Protection**

	Confidential	Restricted	Public
<p><b>Examples of Specific Data</b> <i>(continued)</i></p>	<ul style="list-style-type: none"> <li>• Gramm-Leach-Bliley (GLB)<sup>4</sup> <ul style="list-style-type: none"> <li>- Employee financial account information</li> <li>- Student financial account information (aid, grants, bills)</li> <li>- Individual financial information</li> <li>- Business partner and vendor financial account information</li> </ul> </li> <li>• Employee information                             <ul style="list-style-type: none"> <li>- Social Security number</li> <li>- Date of birth</li> <li>- Home address or personal contact information</li> <li>- Performance reviews</li> <li>- Specific benefit selections</li> </ul> </li> <li>• Donor information</li> <li>• Library use records</li> <li>• Trade secrets, intellectual and/or proprietary research information</li> <li>• Information required to be protected by contract</li> <li>• Vendor non-disclosure agreements</li> <li>• Attorney/client privileged records</li> <li>• Restricted police records (e.g., victim information, juvenile records)</li> <li>• Computer account passwords</li> <li>• Certain affirmative action related data<sup>5</sup></li> </ul>		

<sup>1</sup>For more information on the Health Insurance Portability and Accountability Act (HIPAA) for Human Subject Data: [http://www.washington.edu/research/hsd/faq\\_hipaa.html](http://www.washington.edu/research/hsd/faq_hipaa.html) and for UW Medicine: <http://depts.washington.edu/comply/>

<sup>2</sup>For more information on the Family Educational Rights and Privacy Act (FERPA): <http://www.washington.edu/students/reg/ferpafac.html>

## Minimum Data Security Standards: Data Classification and Related Measures of Protection

<sup>3</sup>For more information on Export Administration Regulations (EAR) and International Traffic in Arms Regulations (ITAR): <http://www.washington.edu/research/osp/ecr.html>

<sup>4</sup>For more information on the Gramm-Leach-Bliley Financial Services Modernization Act (GLB): <http://www.ftc.gov/privacy/glbact/glb-faq.htm>

<sup>5</sup>For more information on UW Affirmative Action Data Collection: <http://www.washington.edu/provost/ap/eoaa/index.html#aadf>

### 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.

#### a. 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 more information, see the General Records Retention Schedules [<http://www.washington.edu/admin/recmgt/retention.schedule.title.html>].

#### b. System Owners and Data Custodians: Roles and Responsibilities

Section 6 of APS 2.1, "UW Information Systems Security," 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 this set of standards, APS 2.1, "UW Information Systems Security," and the Minimum Computer Security Standards.

#### c. Access Control Principles

A required measure for protecting both confidential and restricted data is an **access control system** 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 Section 5, Definitions, in APS 2.1, UW Information Systems Security).

## Minimum Data Security Standards: Data Classification and Related Measures of Protection

### d. "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:

- #1 Controlled computers will meet the UW Minimum Computer Security Standards.
- #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 Operating systems and applications on controlled computers must be patched to and maintained at the most current level provided by their manufacturers.
- #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.
- #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.
- #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.

---

## **Minimum Data Security Standards: Data Classification and Related Measures of Protection**

- #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.
- #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.
- #9** Controlled computers must be provided physical security measures necessary to prevent theft, tampering, or destruction.
- #10** Controlled computers must subscribe to a regimented backup process to ensure data integrity, system availability, and business continuity functions as required.

### **e. 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.c, Item #2).

## **4. Protective Measures for Data**

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

### **a. 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.d of this document, Reference Matrix for Data Protection Measures.

### **b. 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

## Minimum Data Security Standards: Data Classification and Related Measures of Protection

protected by the specific measures identified in Section 4.d of this document, Reference Matrix for Data Protection Measures.

### c. Protective Measures for Confidential Data

- #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.d of this document, Reference Matrix for Data Protection Measures.
- #2 Applications that are linked to databases or data files that contain confidential data must meet the Open 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.
- #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 comply with the encryption security measures in the table below and be 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 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.

### d. 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 UW Minimum Computer Security Standards (<http://www.washington.edu/computing/security/pass/>)

## Minimum Data Security Standards: Data Classification and Related Measures of Protection

MinCompSec.html). In addition, the data on a UW computer may need to be protected with additional security measures, which are summarized in the matrix in the table below.

Protective Measures	Data Category		
	Confidential	Restricted	Public
<b>Minimum Computer Security Standards</b>	Yes	Yes	Yes
<b>Access Control Measures (Authorization)</b>	Yes (documented and audited for compliance once every three years)	Yes (documented)	Yes (limited to system administrators)
<b>Log Reviews and Alerts</b>	Logging alerts and regular reviews	Regular reviews	Basic logging and random periodic reviews
<b>Authentication</b>	Yes (two-layer minimum)	Yes (two-layer recommended)	Configure computer access to: yes for "write," none for "read"
<b>Firewall Protection</b>	Yes (per controlled computer requirements)	Yes	Yes (if feasible)
<b>Backup and Recovery Processes</b>	Yes (per controlled computer requirements)	Yes	Yes
<b>Physical Security</b>	Yes	Yes	Yes
<b>Encryption (During Transmission)</b>	Yes	Recommended	No
<b>Encryption (Storage/Backups)</b>	Recommended	Optional	No
<b>Encryption ("Data at Rest" on System)</b>	Recommended	Optional	No
<b>Personnel Criminal Background Check</b>	Yes (as specified by UW Human Resources)	Yes (as specified by UW Human Resources)	Yes (as specified by UW Human Resources)
<b>Data Sharing Agreements (with Business Partners, Vendors and Others Who Are Given UW Data)</b>	Yes	No	No

**Minimum Data Security Standards:  
Data Classification and Related Measures of Protection**

Protective Measures	Data Category		
	Confidential	Restricted	Public
<b>Audit of Security Measures</b>	Yes (minimum of once every three years and more frequent audits, if possible)	Yes (random sampling)	Recommended (random sampling)

**5. Exemptions**

While rare and unwelcome, there are situations that may require exemptions from these standards. In accordance with the policy statement APS 2.1, "UW Information Systems Security," 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.

**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 UW Technology Security Operations.

**7. Enforcement**

Enforcement of these minimum data security standards is the responsibility of the UW CISO and the PASS Council, with support from the Risk Management, Internal Audit, and UW Technology units. 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.

**8. Additional Information**

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

UW Information Systems Security Policy: <http://www.washington.edu/admin/rules/APS/02.01.7.html>

Minimum Computer Security Standards: <http://www.washington.edu/computing/security/pass/MinCompSec.html>