

UW Information Systems Security

Table of Contents

1. Purpose	2
2. Applicability	2
3. Compliance	2
4. Authorities	2-8
a. State and Federal Statutes and Regulations	3-6
b. Other Primary Authorities (NCQA, JCAHO, HCFA, NAIC)	6-7
c. Common Criteria	7
d. Additional Information Sources Regarding Policy Formulation	8
5. Definitions	8-11
6. Roles and Responsibilities	11-16
a. UW Privacy Assurance and Systems Security Council (PASS Council)	11-12
b. UW Privacy Officer	12
c. Computing and Communications Security Services	12-13
d. UW Medicine IT Services Security Infrastructure Team	13
e. System Owners and Operators	14
f. Data Custodians	14-15
g. Users	16
7. Policy	16-24
a. General Statement of Policy	16-17
b. Monitoring User Accounts, Files, and Access	17
c. Electronic Data and Records Management	17-18
d. Access Controls	18-19
e. Systems and Network Security	19-20
f. Physical Security	20-22
g. Personnel Security Measures	22-24
h. Policy Enforcement	24
i. Policy Maintenance	24

*Corrected Dec 19, 2005.

UW Information Systems Security

(Approved by the President by authority of Executive Order No. 2)

1. Purpose

The University of Washington (UW) is a public institution with custodial responsibilities for a significant and diverse amount of sensitive information. The UW is also a major research center that harbors a vast amount of valuable intellectual property, is the recipient of many federal and private grants, and holds business contracts with a broad range of public and private organizations. All of these roles place significant responsibilities on the UW regarding the management and use of its information systems resources.

The purpose of this policy is to help ensure the security and availability of information technology systems and networks and the confidentiality and integrity of electronic information captured, maintained, and used by the UW. This policy provides direction for compliance with federal and state regulations, specifies appropriate practices, and defines custodial responsibilities for confidential records associated with UW operations. This policy should be used as the foundation document for all standards, procedures, and guidelines that are developed and implemented by the UW related to information systems and data security.

2. Applicability

This policy is applicable to all users (employees, faculty, students, contractors, and others) and support personnel (system administrators, network engineers, systems engineers, and others) of UW computing systems, networks, digital information, and any other electronic processing or communications related resources or services provided through the UW.

3. Compliance

Successful compliance and protection of information systems assets requires that all owners, operators, and users of UW computing and network services and systems learn, understand, and abide by this policy.

In addition, it is the responsibility of owners and operators of computer systems and applications associated with the UW to evaluate their specific compliance requirements on a regular basis as directed by UW security policy.

4. Authorities

The UW is required to comply with many state and federal laws, regulations, and promulgated rules. Beyond strict compliance requirements, the UW needs to understand and consider several additional government and industry standards and best practices that contribute to ensuring the security and availability of information

UW Information Systems Security

technology systems and networks and the confidentiality and integrity of electronic information.

This section lists the statutes, regulations, codes, and other practices that directly or indirectly affect this policy and operational guidelines reflected in this document. They are grouped under four headings, corresponding to the authorities or other bodies that make, enforce, and share them: state and federal statutes and regulations, other primary national and international authorities, national and international common criteria, and additional national and UW information sources for policy.

a. State and Federal Statutes and Regulations

Below are listed state and federal statutes and regulations that directly or indirectly affect this policy and operational guidelines and that are reflected in this document. While every owner and user of UW information systems is not expected to have read all of these documents, they are listed here for reference and to demonstrate the volume and complexity of rules that relate to the use of computers, networks, applications, and data at the UW.

1) Revised Code of Washington (RCW)

Applicable Revised Codes of Washington include the following:

- RCW 5.60.060, Who Are Disqualified—Privileged Communications (communications made to a public officer in official confidence, when the public interest would suffer by disclosure)
- Chapter 9.73 RCW—Violating Right of Privacy (Privacy Act)
- RCW 9A.48.100—Malicious Mischief—"Physical Damage" Defined
- RCW 9A.52.110, 9A.52.120, and 9A.52.130—Computer trespass
- RCW 19.190.020—Unpermitted or Misleading Electronic Mail—Prohibition (Unsolicited Electronic Mail Act)
- Chapter 40.14 RCW—Preservation and Destruction of Public Records (records management, retention, and destruction)
- RCW 42.17.020—Definitions (public records "writing" inclusive of graphics and computer records)
- RCW 42.17.260—Documents and Indexes to Be Made Public
- RCW 42.17.310—Certain Personal and Other Records Exempt (private and vital public records that are exempt from disclosure)
- RCW 42.52.050—Confidential Information—Improperly Concealed Records
- RCW 43.105.041—Powers and Duties of Board (the powers of the Information Services Board (ISB), and its authority to develop statewide or interagency technology standards and policy)

UW Information Systems Security

- RCW 43.105.200—Application to Institutions of Higher Education (ISB policy exemptions for institutions of higher education)
- Chapter 70.02 RCW—Medical Records—Health Care Information Access and Disclosure (Uniform Health Care Information Act)
- RCW 70.24.105—Disclosure of HIV Antibody Test or Testing or Treatment of Sexually Transmitted Diseases—Exchange of Medical Information
- RCW 71.05.390 through 71.05.420—Mental health records
- RCW 71.34.340—Information Concerning Treatment of Minors Confidential—Disclosure—Admissible as Evidence with Written Consent (mental health care record of juveniles)

2) Washington Administrative Code (WAC)

Applicable Washington Administrative Codes include the following:

- Chapter 478–120 WAC—Student Conduct Code for the University of Washington
- Chapter 478–124 WAC—General Conduct Code for the University of Washington
- Chapter 478–140 WAC—Rules and Regulations for the University of Washington Governing Student Education Records
- Chapter 478–276 WAC—Governing Access to Public Records
- Chapter 292–130 WAC—Agency Organization—Public Records (protection and management of public records)

3) Washington Information Services Board (ISB)

The Washington Information Services Board is Washington State's nine-member policy-making body for information technology. Applicable Washington Information Services Board publications include the following:

- Information Technology Security Policy
- Information Technology Security Standards
- Information Technology Security Guidelines

4) United States Code (U.S.C.)

Applicable United States Codes include the following:

- (5 U.S.C. Sec. 552) Freedom of Information Act (FOIA) — provisions for access to many types of records that are exempt from access under the Privacy Act, including many categories of personal information.

UW Information Systems Security

- (5 U.S.C. Sec. 552a) Privacy Act—collection, notification, disclosure, and handling requirements of personal data.
- (15 U.S.C. Sec. 6501 et seq.; 16 C.F.R. Sec. 312) Children's Online Privacy Protection Act of 1998 — requirements that a Web site directed at children less than 13 years of age obtain "verifiable parental consent" before collecting personal information from children.
- (18 U.S.C. Sec. 1029) Fraud and Related Activity in Connection with Access Devices — prohibitions and penalties associated with unauthorized possession and fraudulent use of access tokens, passwords, etc.
- (18 U.S.C. Sec. 1030) Fraud and Related Activity in Connection with Computers — related to prohibitions associated with unauthorized access and use of electronic systems.
- (18 U.S.C. Sec. 1362) Communication Lines, Stations, or Systems — prohibitions associated with malicious or willful destruction or intent to destroy or disrupt communications systems within the U.S.
- (18 U.S.C. Sec. 2510 et seq.; 47 U.S.C. Sec. 605) Wiretap Statutes — prohibitions associated with the use of eavesdropping technology and the interception of electronic mail, radio communications, data transmission, and telephone calls without consent.
- (18 U.S.C. Sec. 2701 et seq.) Electronic Communications Privacy Act — prohibitions for persons tampering with computers or accessing certain computerized records without authorization. The act also prohibits providers of electronic communications services from disclosing the contents of stored communications.
- (18 U.S.C. Sec. 2703) Requirements for Government Access — rules for government agencies for obtaining disclosure of an electronic communication from a provider of such services.
- (20 U.S.C. Sec. 1232g) Family Educational Rights and Privacy Act (FERPA) — the protection, accessibility, and disclosure of educational records and the ability to ensure their completeness and accuracy by a student or the parent of a minor student.
- (29 U.S.C. Sec. 102, et seq.) Employee Retirement Income Security Act — employer requirements to provide employees access to information about their accrued retirement benefits.
- (39 U.S.C. Sec. 3623) Mail Privacy Statute — prohibitions associated with opening mail without a search warrant or the addressee's consent.
- (42 U.S.C. Sec. 242m)—prohibitions of disclosure of data collected by the National Centers for Health Services Research and of health statistics that would identify an individual in any way.

UW Information Systems Security

- (42 U.S.C. Sec. 2000e et seq.) Equal Employment Opportunity Act — restrictions on the collection and use of information that would result in employment discrimination based on race, sex, religion, national origin, and a variety of other characteristics.
- (47 U.S.C. Sec. 1001) Communications Assistance for Law Enforcement — preserving law enforcement's ability to engage in lawful electronic surveillance in the face of new technological developments.
- (Pub. L. 104-191 Sec. 262, 264; 45 C.F.R. Sec. 160-164) Health Insurance Portability and Accountability Act — the security and privacy of individually identifiable health information that is maintained or transmitted by a covered entity. In addition, this act requires covered entities to apply many of its provisions to their business associates, researchers, employers, and others.
- (Pub. L. 107-056) Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001 — a variety of special laws specific to countering terrorist acts including expanded investigative options for law enforcement and a student monitoring program (exceptions to FERPA).

5) Federal OMB Circular NO. A-130

The UW is a recipient of federal grant money and a contracted service provider of federal Medicare and Medicaid programs through the Medical Center. Therefore, this policy also is designed to conform to best practices and planning set forth in Office of Management and Budget (OMB) policies. OMB is a federal organization that works cooperatively with grantmaking agencies and the grantee community. OMB leads development of government-wide policy to ensure that grants are managed properly and that federal dollars are spent in accordance with applicable laws and regulations.

Federal OMB Circular NO. A-130 provides uniform information resources management policies as required by many federal executive orders and acts including:

- 44 U.S.C. Sec. 35—Paperwork Reduction Act of 1980
- 5 U.S.C. Sec. 552a—Privacy Act
- 40 U.S.C. Sec. 759—Computer Security Act of 1987

b. Other Primary Authorities (NCQA, JCAHO, HCFA, NAIC)

Other primary authorities include the following groups and standards:

- National Committee for Quality Assurance (NCQA) Health Plan Employer Data and Information Set (HEDIS) compliance audit standards.

UW Information Systems Security

- NCOA advisory information system standards (based on work presented in HEDIS Volume 4: *A Roadmap for Information Systems*).
- Joint Commission on Accreditation of Healthcare Organizations (JCAHO) accreditation criteria.
- The Health Care Financing Administration (HCFA) policy bulletins.
- The National Association of Insurance Commissioners (NAIC) Health Information Privacy Model Act (1998).

c. Common Criteria

A common set of national and international criteria to guide the development and evaluation of security standards, environments, and systems has been established and maintained by the processes and oversight of the following groups:

- The Communications Security Establishment (CSE), Canada
- The Central Service for Information Systems Security (CSISS), France
- The German Information Security Agency (GISA), Germany
- The National Communications Security Agency (NCSA), Netherlands
- The Communications—Electronics Security Group (CESG), UK
- The National Institute of Standards and Technology (NIST), United States
- The National Security Agency (NSA), United States

These measures, called the "Common Criteria," support many legislated and regulatory standards at the national and international levels. UW security personnel track the activities of these groups and reflect the criteria in security policy where appropriate. Compliance with these criteria will be beneficial to the UW for technical and business reasons.

The Common Criteria (CC) are as follows:

- The Common Criteria for Information Technology Security Evaluation (CC version 2.1/aligned with ISO IS 15408) (last updated: 19 September 2000).
- Guide for Production of Protection Profiles and Security, Preliminary Draft Technical Report (PDTR) (last updated: 01 January 2000).
- CSPP—Guidance for COTS (commercial off the shelf) Security Protection Profiles, version 1.0 NISTIR 6462 (final document: 01 January 2000).
- CSPP—OS Operating System Protection Profile, draft version 0.3 (last updated: 01 April 2000).
- Role-Based Access Control (RBAC) Protection Profile, final version 1.0.
- Federal Government Firewall Protection Profiles, draft version based on CC version 2.0.
- SCPP—Smart Card Security Users Group Protection Profile, version 2.0 (last updated: 01 June 2000).

UW Information Systems Security

d. Additional Information Sources Regarding Policy Formulation

In addition to the authorities listed above, this security policy also incorporates ideas from numerous applicable sources including:

- National Institute of Standards and Technology (NIST) Engineering Principles for IT Security.
- National Research Council Report for the Record: *Protecting Electronic Health Information* (1997).
- University of Washington Strategic Goals (as established by the Board of Regents and revised March 1999).

5. Definitions

The following terms are found in this policy document or its associated guideline documents:

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

Authentication: A systematic method for establishing proof of identity.

Authorization: The process of giving someone permission to do or have something. System administrators/owners and data custodians define for their systems which users are allowed access to those systems and what privileges are assigned. A system could be an operating system, database, or application.

Availability: The assurance that a computer system is accessible by authorized users whenever needed or as pre-defined.

Common Criteria for Information Technology Security Evaluation: A comprehensive specification (aligned with the ISO IS 15408) that first defines the targeted environment and then specifies the security requirements necessary to counter threats inherent in that environment.

Computing & Communications (C&C): The UW administrative unit responsible for (among other things) central UW computing and networking.

Confidentiality: An attribute of information. Confidential information is sensitive or private information, or information whose unauthorized disclosure could be harmful or prejudicial.

Cookie: A small text file that is sent to a user's computer by the server that the user is visiting. This file can record preferences and other data about the user's visit to a particular site. Cookies often are used for long-term data collection. Short-term cookies might be used for things like authentication in "single sign-on" services.

Cost-effective: To deliver desired results in beneficial financial terms.

UW Information Systems Security

Critical Servers: Within the UW, critical servers are devices needed to support patient care or major UW administrative services, or they are devices that contain personally identifiable information that has value in and of itself.

Data Custodians: Individuals who have been officially designated as accountable for specific data that is transmitted, used, and stored on a system or systems within a department, college, school, or administrative unit of the UW.

Decryption: The process of turning unreadable cipher text into readable text.

Encryption: The process of turning readable text into unreadable cipher text.

Firewalls: Policy-based filtering systems (composed of both hardware and software) that control and restrict the flow of data between networked computer systems. Firewalls establish a physical or logical perimeter where selected types of network traffic may be blocked. Blocking policies typically are based on computer IP addresses or protocol type of application (e.g., Web access or file transfer). Types of firewalls relevant to this policy include:

- Integrated OS (operating system) firewalls, bundled with the OS (e.g., Windows, Linux).
- Dedicated firewalls protecting labs or server sanctuaries.
- Dedicated firewalls protecting individual hosts.
- Logical firewalls protecting non-co-located systems.

Forensics (Computer): The discipline of dissecting computer storage media, log analysis, and general systems to find evidence of computer crime or other violations.

Incident Response Capability: The ability to respond appropriately and completely to any incidents, situational compromises, or threats from any source.

Information Systems: The UW's electronic information systems and data assets. All computing systems, networks, digital information, and other electronic processing or communications related resources or services provided through the UW.

Integrity: Data or a system remains intact, unaltered, and reliable.

Intrusion Detection: A security management system that gathers and analyzes information from various areas within a computer or a network to identify possible security breaches, which include both intrusions (attacks from outside the organization) and misuse (attacks from within the organization).

Non-repudiation: A mutually agreed upon process, secured evidence, or other method of operation that provides proof of receipt or protection from denial of an electronic transaction or other activity.

Off Site: A location separate and distinct from the area in which something, such as a computer, is located. Frequently referred to when considering backup storage.

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

UW Information Systems Security

Perimeter Security: The ability to protect the outer limits of a network, or a physical area, or both.

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

Principle of Least Privilege: Access privileges for any user should be limited to only what is necessary to complete their assigned duties or functions, and nothing more.

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's 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.

Privacy Policy: Specific to the UW, the *UW Electronic Privacy Policy on Personally Identifiable Information*.

Privacy Statement: Sometimes referred to as a privacy policy, a privacy statement is posted on an organization's Web site to notify visitors of the types of information being collected and what will be done with the information.

Risk Management: A comprehensive methodology that strives to balance risks against benefits in a pre-defined environment.

Security: An attribute of information systems that includes specific policy-based mechanisms and assurances for protecting the confidentiality and integrity of information, the availability and functionality of critical services, and the privacy of individuals.

Security Incident: An event during which some aspect of computer security is threatened.

Server Sanctuaries: Within the UW, these are locations within computing facilities where clusters of sensitive or critical servers can be co-located and around which suitable physical and logical security measures can be implemented.

Subnet Contacts: Specific to the UW, individuals who are registered with the C&C Network Operations Center as contacts for departmental subnets.

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

System Administrators: Individuals who support the operations and integrity of computing systems and their use. Their activities might include system installation, configuration, integration, maintenance, security management, and problem analysis

UW Information Systems Security

and recovery. In addition, managing the computer network is often their responsibility in an inter-networked computing environment.

System Management: The activities performed by systems administrators.

System Operators: Individuals within the UW community who are accountable for the operational decisions about the use and management of a computing system. (See also *System Owners*.)

System Owners: Individuals within the UW community who are accountable for the budget, management, and use of one or more electronic information systems, electronic databases, or electronic applications associated with the UW. (See also *System Operators*.)

Technicians: Individuals who have technical knowledge about computers, software, hardware, operating systems, and networks (e.g., system administrators, system engineers, or network engineers).

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

UW-owned Network: A network where network components (including active elements such as routers and switches, transmission media, and network-attached computers) are owned and operated by the UW or units of the UW. A message that travels over UW-owned networks is, in general, on an open network and hence requires additional security measures to be considered secure.

UW Medicine: An affiliation of organizations including Harborview Medical Center, University of Washington Medical Center, University of Washington Physicians, and University of Washington School of Medicine.

6. Roles and Responsibilities

Responsibility for protecting UW information systems and data is shared by many entities and individuals throughout the University including the Privacy Assurance and Systems Security Council (PASS Council), the UW Privacy Officer, Computing & Communications Security Services, the UW Medicine IT Services Security Infrastructure Team, and all UW system owners, operators, data custodians, and users. The following section describes the specific roles and responsibilities of each of these groups.

a. UW Privacy Assurance and Systems Security Council (PASS Council)

The Privacy Assurance and Systems Security Council (PASS Council) is an appointed administrative authority whose role is to provide oversight and direction regarding information systems security and privacy assurance. The membership of the PASS Council is composed of senior officials and management staff representing key administrative areas of the UW's operations.

UW Information Systems Security

The responsibilities of the PASS Council include the following:

- Oversee the development, implementation, and maintenance of a University-wide strategic information systems (see Section 5, Definitions) security plan.
- Oversee the development, implementation, and enforcement of University-wide information systems security policy and related recommended guidelines, operating procedures, and technical standards.
- Oversee the process of handling requested policy exceptions.
- Advise the University administration on related risk issues and recommend appropriate actions in support of the UW's larger risk management (see Section 5, Definitions) programs.
- Ensure related compliance requirements are addressed, e.g., privacy, security, and administrative regulations associated with the Health Insurance Portability and Accountability Act (HIPAA) and other federal and state rules.
- Ensure appropriate risk mitigation and control processes for security incidents as required.

b. UW Privacy Officer

The privacy protection objectives of the UW are critical to the success of the University's mission. The UW has appointed a privacy officer as an integral component of its commitment to protect privacy and comply with all requirements for information systems protection. The role of the privacy officer is to provide strategic oversight and coordination of the University's privacy protection and compliance efforts. The privacy officer is appointed by the UW president and must be a senior member of the administration. See the *UW Electronic Privacy Policy on Personally Identifiable Information* for detailed information about the privacy officer's specific duties.

The success of the privacy officer's efforts depends on strong support from all system owners, operators, data custodians, and users throughout the UW. (For definitions of these roles, see Section 5.)

c. Computing and Communications Security Services

Computing and Communications (C&C) provides an active, key role in computer security planning, analysis, prevention, incident response, and technical education for the University community. Key groups within C&C that provide this role are Security Operations, the Security Infrastructure Team, Network Support Services, and others.

C&C's security responsibilities include the following:

- Support for UW security policy development, implementation, and enforcement.

UW Information Systems Security

- Support for UW strategic security planning and plan implementation.
- Development of security strategy in UW information systems architecture.
- Support for security and privacy awareness and education programs.
- Incident response services as needed.
- Computer forensic services as required.
- Security consulting services as needed.
- Support for the development and implementation of all appropriate standards and guidelines as necessary.

C&C coordinates its administrative activities and incident response procedures as necessary with both the privacy officer and the PASS Council. In addition, it works closely with UW Medicine Information Technology Services Security Infrastructure Team to ensure University-wide service continuity and to leverage all mutually beneficial activities and resources.

d. UW Medicine IT Services Security Infrastructure Team

The UW Medicine Information Technology Services (IT Services) Security Infrastructure Team provides a key role of centralized oversight, direction, and support for all information systems security-related services for UW Medicine. The group's responsibilities include the following:

- Support for UW Medicine security policy development, implementation, and enforcement.
- Support for UW Medicine strategic security planning and plan implementation.
- Support for security awareness and education programs.
- Incident response services as needed.
- Computer forensic services as required.
- Security consulting services as needed.
- Support for the development and implementation of all appropriate standards and guidelines as necessary with the UW Medicine community.

The UW Medicine IT Services Security Infrastructure Team works closely with C&C Security Operations to ensure University-wide service continuity and to leverage all mutually beneficial activities and resources.

The director of the UW Medicine IT Services Security Infrastructure Team has review and decision authority over requests for exceptions to information systems security policy within the UW Medicine environment, unless privacy protection issues could be involved. The latter falls under the administrative authority of the privacy officer and designated authorities specified by the UW administration or the UW Medicine administration.

UW Information Systems Security

e. System Owners and Operators

System owners and operators (see Section 5, Definitions) play a critical role in protecting UW information systems and data. Their ranks might include members of the UW professional staff, deans, department heads, faculty members, contracted employees, or students.

System owners' and operators' areas of responsibilities for systems and information security include the following:

- Comply with UW policies and statutory and regulatory requirements.
- Comply with UW guidelines related to logical and physical security (see *UW Guidelines for Implementing Systems and Data Security Practices*).
- Comply with "Guidelines for UW Computer Services Users."
- Maintain confidentiality of sensitive data, especially personally identifiable information (see Section 5, Definitions) and valuable intellectual property (see *UW Guidelines for Implementing Systems and Data Security Practices* and *UW Electronic Information Privacy Policy on Personally Identifiable Information*).
- Grant access to all users based on the principle of least privilege (see Section 5, Definitions) where required.
- Grant access to all users based on the principle of separation of duties (see Section 5, Definitions) where required.
- Submit documented reports to the appropriate authority involving incidents of security breaches with the potential to compromise personally identifiable information (see *UW Electronic Information Privacy Policy on Personally Identifiable Information*).
- Submit documented requests to the PASS Council of any desired exceptions to UW policy.
- Perform incident response activities when incidents involve their system(s).
- Specify security resources as required in University budget processes and in grant proposals.

All system owners and operators are encouraged to work closely with the PASS Council, UW privacy officer, data custodians, C&C Security Operations, and UW Medicine IT Services Security Infrastructure Team to help ensure the successful protection of UW computing resources and data.

f. Data Custodians

Data custodians are individuals who have been officially designated as accountable for specific data that is transmitted, used, and stored on a system or systems within a department, college, school, or administrative unit of the UW. The role of the data custodians is to provide direct authority and control over the management and use of specific information. These individuals might

UW Information Systems Security

be deans, department heads, managers, supervisors, or designated staff. They might serve dual roles as a system owner or operator and a data custodian.

Data custodians must follow all appropriate and related security guidelines to ensure the protection of sensitive data and intellectual property residing on systems for which they have accountability (see *UW Guidelines for Implementing Systems and Data Security Practices*).

The *UW Electronic Privacy Policy on Personally Identifiable Information* delineates the ultimate custodial authority for the various types of personally identifiable information.

Data custodians' responsibilities include the following:

- Ensure compliance with all UW policies and all statutory and regulatory requirements.
- Provide system owners and operators with requirements for access control measures to protect sensitive data.
- Ensure appropriate disposal of all media on which data is stored at the end of its use.
- Ensure appropriate security measures for transmission of data.
- Support access control of data by acting as a control point for all access requests.
- Support regular review and control procedures that ensure that all access privileges are current and appropriate.
- Submit documented reports to the appropriate authority if there is a possibility of compromise of personally identifiable information (see *UW Electronic Information Privacy Policy on Personally Identifiable Information*).
- Ensure that all access is granted based on the principle of least privilege where required (see Section 5, Definitions).
- Ensure that all access is granted based on the principle of separation of duties where required (see Section 5, Definitions).

Data custodians, in conjunction with the system owners and operators and the UW privacy officer, are responsible for documenting any requested exceptions to UW privacy protection policies. Documented exceptions must be approved in writing by the authorized University officials responsible for the electronic information to which the exception applies. Exceptions will be considered only when warranted and only to the degree necessary to achieve the mission and business needs of the University. Any and all exceptions made must be documented with the Executive Vice President.

UW Information Systems Security

g. Users

All users have a critical role in the effort to protect and maintain UW information systems and data. Users of UW computing resources and data have the following responsibilities:

- Support compliance with all federal and state statutes and regulations.
- Comply with all UW policies and guidelines (see Guidelines for UW Computer Services Users and UW Electronic Information Privacy Policy on Personally Identifiable Information).
- Protect against unauthorized access to accounts, privileges, and associated passwords.
- Maintain confidentiality of sensitive information to which they are given access privileges.
- Accept accountability for all activities associated with individual user accounts and related access privileges assigned to them.
- Restrict to authorized purposes the use of UW computers, email, computer accounts, and networks and the information accessed, stored, or used on any of these systems.
- Report all suspected security and/or policy violations to an appropriate authority (e.g., manager, supervisor, system administrator, C&C Security Operations, or UW Medicine IT Services Security Infrastructure Team).
- Report all known violations of privacy policy to the UW privacy officer.

Users are also required to follow all specific policies, guidelines, and procedures established by the UW departments, schools, colleges, or business units with which they are associated and that have provided them with access privileges.

7. Policy

The following section sets forth the UW's general policy regarding the security, availability, privacy, and integrity of its information systems, networks, and data. It stipulates specific policies for monitoring computing resources, managing electronic data and records, and controlling access to computing resources. In addition, it outlines minimum standards and practices for systems and network security.

a. General Statement of Policy

It is the policy of the UW to ensure the security, availability, privacy, and integrity (see Section 5 for definitions of each of these terms) of its information systems, networks, and data and to ensure full compliance with all applicable federal and state statutes and regulations.

UW Information Systems Security

All providers and users of UW computing services, resources, and data are required to comply with all established policies, guidelines, and procedures, including applicable federal and state statutes and regulations.

The general policy outlined in this section is the foundation for all other policy statements, guidelines, and procedures that are developed and implemented within UW computing environments.

b. Monitoring User Accounts, Files, and Access

The UW does not routinely inspect or monitor the use of computers. However, the normal operation and maintenance of UW computing and network resources require authorized UW staff to back up and cache data and communications, log activity, monitor general usage patterns, and perform other activities that are necessary for the delivery and availability of service.

Receipt of a report or discovery of inappropriate or unauthorized use of computing and network resources may trigger monitoring and investigation by authorized UW staff.

UW systems owners and operators may specifically monitor the activity of individual users including files, session logs, content of communications, and Internet access without notice, when:

- The user's activity prevents access to computing and network resources by others.
- General usage patterns indicate that unacceptable activity is occurring.
- There is reasonable cause to believe that a user has violated or is violating policy or law.
- It appears necessary to do so to protect the UW from liability.
- It is required by and consistent with law.

Evidence of misuse of computing resources will be referred to appropriate UW officials. Evidence of possible criminal activity, which could include user files, email, and/or activity logs, will be turned over to appropriate UW and law enforcement officials.

c. Electronic Data and Records Management

Much of the vast amount of electronic data generated throughout the University comprises official UW records and requires specific management and handling practices and procedures as defined by the UW and state law (see Section 4, Authorities).

All UW system owners, operators, data custodians, and users are obligated to understand the nature of the data they generate, use, or store and to ensure that they are managing that data in full compliance with all state laws and UW records management policies. All UW system owners, operators, data

UW Information Systems Security

custodians, and users are required to properly manage and protect electronic data they may be using, transmitting, and storing.

UW Records Management Services is the primary resource for information and support regarding these obligations. Specific information regarding what is defined as an official record of the UW, as well as retention, destruction, and archival requirements, is available through UW Records Management Services.

The University privacy officer and the *UW Electronic Information Privacy Policy on Personally Identifiable Information* are the primary sources for direction and information regarding personally identifiable information.

The document named *UW Guidelines for Implementing Systems and Data Security Practices* contains a table of security measures commensurate with data categories.

d. Access Controls

The UW has hundreds of different computing environments hosted on University networks, and within UW departments, schools, and business units. These environments require different security measures. Consequently, access control measures (see Section 5, Definitions) required for establishing users' access to any UW computing resources should be commensurate with the functional nature and degree of criticality of the computer systems, network resources, and data involved.

All system owners, operators, and data custodians are responsible for ensuring that their systems are properly protected with appropriate access control measures based on the criticality of their systems and the data involved. The document named *UW Guidelines for Implementing Systems and Data Security Practices* provides direction on how to define the appropriate security measures for computing systems.

In addition, all computing systems hosted on UW networks must support and comply with the following fundamental access control measures, functions, and operating principles:

- Systems are required to have an access control mechanism that allows for an appropriate level of authorization (see Section 5, Definitions) and allocation of system and data resources to individual users. Access mechanisms can be physical, transaction-based, role-based, time-based, user-based, or use any other reasonable control method appropriate for the systems' functions.
- Shared systems are required to have the capability to log basic information about user access activity and to create historical logs and access violation reports.
- System access accounts for users must be based on a unique identifier, and no shared account is allowed except as authorized by the system owner or operator and where appropriate accountability can be maintained.

UW Information Systems Security

- Users' system access must be based on the principle of least privilege (see Section 5, Definitions) and the principle of separation of duties (see Section 5, Definitions). Computer applications must be developed and integrated in a way that maintains individual user accountability and audit capability. Documented procedures should be in place for issuing, altering, and revoking access privileges on shared systems.

e. Systems and Network Security

In light of the complex and diverse nature of the different computing environments hosted on UW networks and the wide range of statutory and regulatory compliance requirements, all systems and network security measures must be based upon the functional nature and degree of criticality of the computer systems, network resources, and data involved.

All system owners and operators are responsible for ensuring that they have implemented all necessary security measures. Failure to do so risks creating security breaches or other incidents and could lead to temporary restrictions or even suspension of access to UW network resources.

The document named *UW Guidelines for Implementing Systems and Data Security Practices* provides direction on how to define the appropriate security measures for computing systems.

1) Systems Security—Minimum Measures and Practices

To protect the availability and integrity of UW computing resources, all computing systems and servers hosted on UW networks should comply with the following systems security measures and practices:

- Operating systems and applications must be maintained with the timely application of all related vendor-issued patches necessary to prevent the systems from being compromised and/or causing disruptions of network services and/or other systems.
- Externally accessible systems must install antivirus software and maintain procedures for regular signature updates.
- Shared systems are required to have a technical access control mechanism that allows authorization and allocation of system and data resources to individual users (see Section 7.d, Access Controls).
- Procedures must be maintained for regular backup of all data and system files necessary for discovery and recovery purposes. All backup media should be stored properly in a location authorized by the data owner with protections that allow access to the data by authorized personnel only. The ability to recover data from backups should be tested regularly.
- Shared systems are required to have the capability to log basic information about user access activity, system changes, and events for the possible creation of historical logs and access violation reports.

UW Information Systems Security

Logs must be monitored for intrusions or attempts at unauthorized access.

- Systems must maintain a functioning and accurate system clock, since it is a critical element for the computer forensics (see Section 5, Definitions) and system logs that are essential for successful investigations.
- Encryption capabilities (the ability to turn readable text into unreadable cipher text) must be used for systems that send or receive personally identifiable information (see Section 5, Definitions) that is transmitted over open networks like the Internet or UW-owned networks (see Section 5, Definitions).
- Critical servers (servers needed to support patient care or major UW administrative services, or devices that house personally identifiable information that has value in and of itself) must be housed in protected areas such as server sanctuaries (locations where suitable physical and logical security measures can be implemented). (See *UW Guidelines for Implementing Systems and Data Security Practices*.)

2) Network Security—Minimum Measures and Practices

To protect the security, availability, and integrity of UW network resources, all computing systems and servers hosted on UW networks should comply with the following security measures and practices:

- Support proactive vulnerability probing and reporting by UW authorized technicians to help manage system security needs.
- Use secure protocols (e.g., SSL/SSH/Kerberos) for accessing all services that require authentication (a systematic method for establishing proof of identity).
- Report all security breaches to the appropriate security entity (C&C Security Operations, UW Medicine IT Services Security Infrastructure Team, and/or the UW privacy officer).
- Display security-warning banners prior to allowing the access log-on process to be initiated on systems running applications that are accessible on the UW-owned network. These security banners must inform all users that the system or application being accessed is proprietary, that it should be accessed only by authorized users, and that system use is monitored for enforcement purposes.

f. Physical Security

Physical security measures are an important part of any effort to protect information system assets and services. As with logical security measures at the UW, the physical security measures required for protecting UW computing

UW Information Systems Security

resources must be commensurate with the nature and degree of criticality of the computer systems, network resources, and data involved.

The UW has a wide spectrum of information systems deployments. They include:

- Large data-center facilities.
- Modest-sized server rooms.
- Small sets or individual departmental servers located in all manner of office environments.
- Computer labs.
- Telecommunications closets and vaults of all shapes and sizes.
- Media storage areas.
- Desktop computer workstations and printers.
- Wireless and mobile systems.

These technology deployments require different physical security measures. These measures are especially important when sensitive information is involved. All system owners and operators are responsible for ensuring that they have implemented the appropriate physical security measures for their particular computing environment. All users are required to respect the physical security measures in place.

The following physical security measures and objectives should be implemented where applicable to protect UW computing and network assets and sensitive information:

- Physical access control measures sufficient to prevent UW assets from unnecessary and unauthorized access, use, misuse, vandalism, or theft.
- Computer rooms and telecommunications closets located away from heavy traffic patterns and not advertised.
- When appropriate, physical security measures should be in accordance with standards specified in the current edition of the National Fire Protection Association (NFPA) publication No. 75, *Protection of Electronic Computing/Data Processing Equipment*, and by Occupational Safety & Health Administration (OSHA) Safety and Health Standards. This is particularly important for data-center facilities.
- Certified smoke and fire-alarm and fire-suppression systems for data centers, server rooms, telecommunication closets, and vaults to mitigate potential damage to UW assets in the event of a fire.
- Environmental control measures (e.g., power supply, heating, ventilation, air conditioning, plumbing, and physical location) sufficient to protect UW assets from preventable service disruptions or harm. Departmental and general access labs monitored and secured when not open for use.

UW Information Systems Security

- Inventory control measures (e.g., asset tags or other identification markings) for tracking and accounting for UW assets.
- Secured off-site data/media storage and procedures that meet all archival, backup, and recovery needs for UW computing and network operations.
- Specific procedures for users of UW laptops, wireless services, and other mobile computing devices such as PDAs to prevent the theft or compromise of these devices.

Tools, systems, or procedures implemented to meet physical security requirements should be selected based on their cost-effectiveness and appropriate level of ability to protect UW assets.

g. Personnel Security Measures

This section outlines security measures and procedures that should be established and maintained when working with UW personnel throughout the employment process and when dealing with vendors, contractors, and temporary employees.

1) Measures for Hiring Employees

Comprehensive pre-employment screening is recommended for all potential candidates for key technical positions when those positions include an actual or potential wide span of systems control, and/or access to sensitive information, especially personally identifiable information or UW financial information. This screening could include checking and confirming references, background checks for criminal convictions (both federal and local, as necessary), and reviewing educational records and credit reports. All hiring officials should consider using such screening practices when hiring for key technical positions, regardless of employee type (contract, classified, professional, academic, or temporary).

All pre-employment inquiries must be conducted in full compliance with official UW guidelines established by UW Human Resources and in full compliance with state and federal laws. All hiring officials, managers, or others must work closely with UW Human Resources when engaging in any hiring process.

All UW departments, colleges, schools, and business units should have procedures in place to provide new employees with information about user responsibilities and guidelines associated with their assigned computer and network privileges and resources, including access to this document and related departmental policies, procedures, and guidelines. Appropriate supervision of new employee access to systems and data should be standard practice. New employees should be made aware that secure computing practices will be part of their performance reviews.

All physical and logical access to computing and network facilities and resources should be assigned in accordance with the principle of least

UW Information Systems Security

privilege (see Section 5, Definitions) and principle of separation of duties (see Section 5, Definitions).

2) Measures for Separating Employees

All UW departments, colleges, schools, and business units should establish and maintain processes and procedures to properly and quickly close and remove all computing system and network privileges and resources when an employee is separated, even if the employee is going to another job within the UW. These processes and procedures should include the following:

- The separated employee's immediate manager is responsible for notifying all system owners and operators, or the designated system administrator handling the computer or communications accounts, to close all related accounts and remove all access capabilities related to the separated employee.
- Separated employees may not retain, give away, or remove from UW premises any UW information (electronic or hard copy) other than personal copies of information disseminated to the public and personal copies of correspondence directly related to the terms and conditions of their employment. All other UW information in the custody of the departing employee must be turned over to the employee's immediate supervisor at the time of departure.
- At the time of separation, all UW property must be returned. This includes portable computers, printers, modems, software, cellular telephones, digital pagers, PDAs, documentation, building keys, lock combinations, encryption keys, and access cards.

3) Measures for Employees on Leave or Suspension

All UW departments, colleges, schools, and business units should establish and maintain processes and procedures to properly and quickly close and remove all computing system and network privileges and resources when an employee is suspended or is taking an extended leave of absence (including long-term illness or disability). It is important to use the same security measures for suspended employees as are used for separating employees (see Section 7.g.2). In addition, extended leaves of absence may require these measures, at the supervisor's discretion, taking into consideration such factors as level of access, nature and scope of computer applications and permissions, and duration of absence.

4) Measures for Vendors

Vendors with access to computers and networks should meet many of the same standards placed on employees. They should understand the security policies and practices. Their access should be limited to just what

UW Information Systems Security

is necessary for them to meet their contract requirements. When appropriate, vendors should be escorted into physically restricted areas. When their job is complete, they should return all access devices, and their log-on privileges should be terminated.

h. Policy Enforcement

Individuals who violate this policy may be denied access to UW computing and network resources and may be subject to other penalties and disciplinary action within and outside the UW. Departmental managers are expected to work with appropriate UW resources in investigating and addressing suspected violation of this policy. Such resources include, but are not limited to, UW Internal Audit, UW Risk Management, UW Police Department, departmental managers, UW Human Resources, and Student Affairs.

The UW may temporarily suspend, block, or restrict access to computing resources and accounts at any time when it reasonably appears necessary to do so in order to protect the integrity, security, or availability of UW computing and network resources or to protect the UW from liability. The UW will refer suspected violations of applicable law to appropriate law enforcement agencies.

In general:

- If violations of this policy are minor and unintentional, the UW will take appropriate actions to resolve the issue, and violators may be subject to disciplinary measures.
- If violations of this policy are a result of negligent or deliberate acts, the UW will take appropriate actions to resolve the issue including disciplinary measures up to and including termination of employment or expulsion.
- In addition to any other measures taken, if violations of this policy are a result of suspected illegal activities, the UW will notify appropriate University authorities and law enforcement agencies.

The UW reserves the right to pursue appropriate legal actions to recover any financial losses suffered as the result of violations of this policy.

i. Policy Maintenance

This policy and the related guidelines will be reviewed yearly. A major security compliance audit must take place every three years.