

**Information Security and Privacy  
Roles, Responsibilities, and Definitions**

**Table of Contents**

**1. Purpose** .....

    Figure 1. Information Security and Privacy Rules/Policy  
    Statements Architecture.....

**2. Roles and Responsibilities** .....

    Figure 2. Information Security and Privacy Roles and  
    Responsibilities.....

        a. University Chief Information Security Officer .....

        b. University Privacy Official .....

        c. Chief Privacy Officer for the Non-UW Medicine Components  
        of the Hybrid Entity .....

        d. Chief Privacy Officer for UW Medicine .....

        e. Data Trustees .....

        f. Managerial Group for Classified Research and Contracts.....

        g. University Facility Security Officer.....

        h. Data Custodians.....

        i. Executive Heads of Major University Organizations.....

        j. Incident Manager .....

        k. Systems Owners .....

        l. System Operators .....

        m. Information Assurance Liaisons .....

        n. Workforce Members.....

**3. Definitions** .....

**4. Exemptions**.....

**5. Policy Maintenance** .....

**6. Enforcement** .....

**7. Additional Information** .....

**Appendix A. University Rules/Policy Statements on  
Information Security**.....

# Information Security and Privacy Roles, Responsibilities, and Definitions

(Approved by the Provost and Executive Vice President by authority of Executive Order No. 4; the Senior Vice President for Finance and Facilities by authority of Executive Order No. 5 and the CEO of UW Medicine, Executive Vice President for Medical Affairs, and Dean of the School of Medicine by authority of Executive Order No. 6)

## 1. Purpose

The University of Washington's (University) *Rules/Policy Statements* on information security and privacy included in the University Administrative Policy Statements (APS) establish the principles of *Confidentiality, Integrity, and Availability* for University *Institutional Information, Infrastructure Technology, or Information Systems*.

This *Rule/Policy Statement* establishes roles, responsibilities, and definitions that are used in all the University *Rules/Policy Statements* on information security and privacy as well as *Standards and Guidelines* issued pursuant to the University *Rules/Policy Statements*. Figure 1 below illustrates the University *Rules/Policy Statements* that are covered by the information in this policy. In addition, Appendix A provides a brief description of the University *Rules/Policy Statements* on information security and privacy.

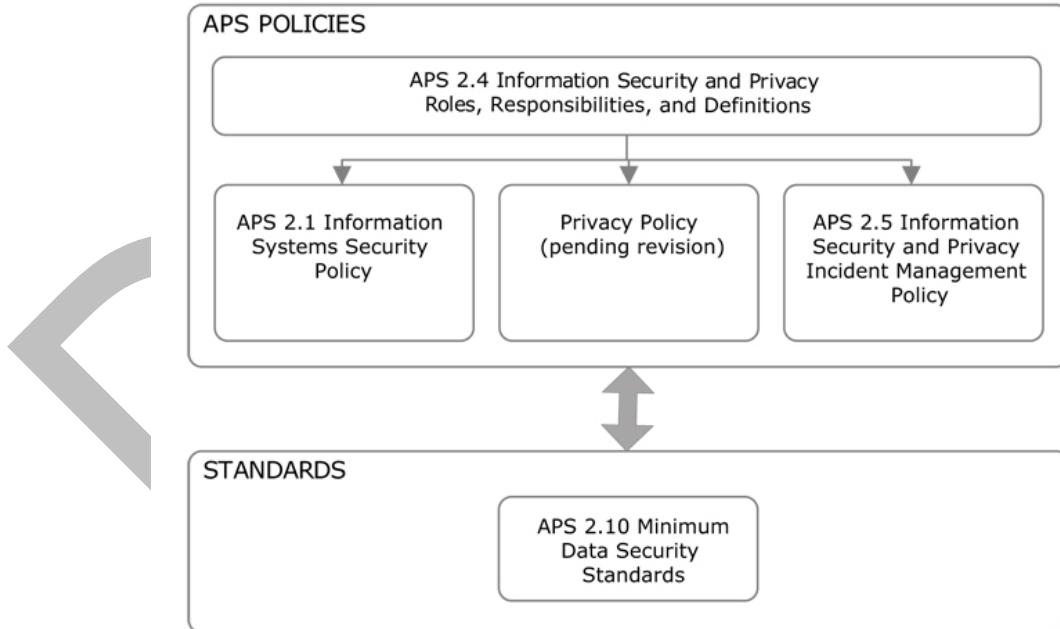


Figure 1. Information Security and Privacy Policy Statements Architecture

The capitalized and italicized terms and definitions used in this policy can be found in Sections 2 and 3.

## 2. Roles and Responsibilities

Individuals across the University have the following responsibilities for information security and privacy.

Figure 2 below illustrates the strategic, tactical, and operational relationship of the different information security and privacy roles.

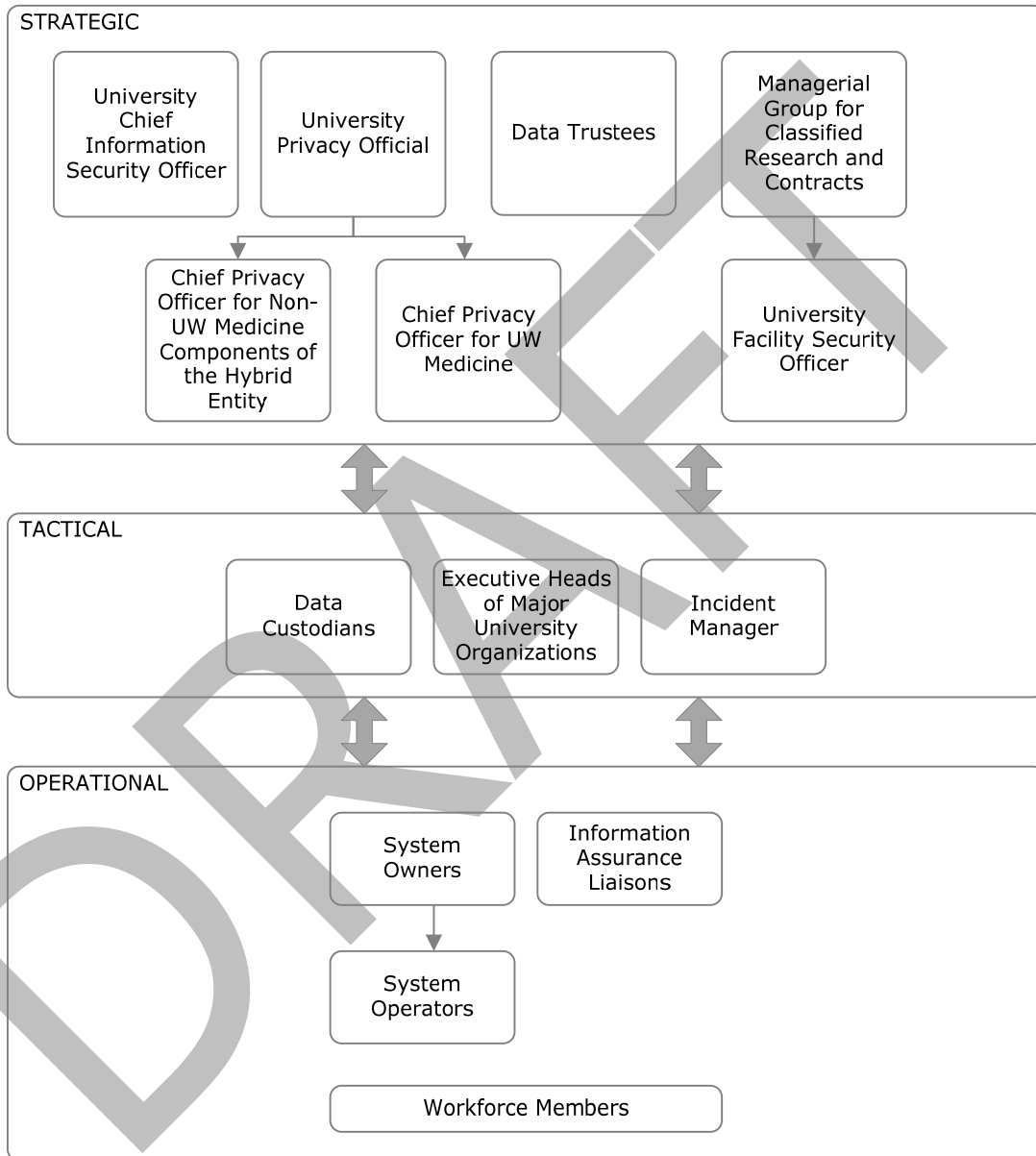


Figure 2. Information Security and Privacy Roles and Responsibilities

### a. University Chief Information Security Officer

The *University Chief Information Security Officer* is responsible for information security vision, strategy, and coordination across the University.

The responsibility of the *University Chief Information Security Officer* includes:

- Oversee the creation and maintenance of the University information security-related *Rules/Policies, Standards, and Guidelines*;
- Oversee institutional risk assessments related to the University information security practices;
- Provide support for compliance with information security related laws, regulations, standards, and contractual requirements;
- Provide oversight and direction for *Information Security and Privacy Incident* investigations including incident management and determination of notification requirements;
- Serve as the University's liaison with law enforcement, and other outside authorities who may need to be informed about an *Information Security and Privacy Incident*; and
- Collaborate with the *University Privacy Official, University Facility Security Officer*, and other individuals as appropriate to develop and maintain an authoritative list of external laws that may relate to information security and privacy at the University.

**b. University Privacy Official**

The *University Privacy Official* oversees the University *Rules/Policies*, procedures, and enforcement efforts relating to privacy.

The responsibility of the *University Privacy Official* includes:

- Coordinate and document privacy program activities among the UW Medicine and non-UW Medicine healthcare components of the University as required by the Health Insurance Portability and Accountability Act (HIPAA);
- Approve the University-wide privacy program policies and procedures;
- Oversee institutional risk assessments related to the University privacy practices;
- Work closely with senior administrators and compliance staff to enforce privacy program policies; and
- Provide oversight and direction for *Information Security and Privacy Incident* investigations including incident management and determination of notification requirements.

**c. Chief Privacy Officer for the Non-UW Medicine Components of the Hybrid Entity**

Under delegated authority from the *University Privacy Official*, provide oversight and direction for *Information Security and Privacy Incident* investigations including determination of notification requirements involving *Protected Health Information (PHI)* or other forms of *Confidential Information* at the University.

**d. Chief Privacy Officer for UW Medicine**

Under delegated authority from the *University Privacy Official*, provide oversight and direction for *Information Security and Privacy Incident* investigations including determination of notification requirements involving UW Medicine *Protected Health Information (PHI)*.

**e. Data Trustees**

*Data Trustees* are high-level employees (e.g., chancellors, vice presidents, vice provosts, and deans) that are appointed by and report to the President or Provost and Executive Vice President.

The responsibility of the *Data Trustees* includes:

- Authority over *Rules/Policies, Standards, and Guidelines* regarding business definitions of information, and the access and usage of that information, within their delegations of authority; and
- Appoint the *Data Custodians* for their *Subject Area Domains*.

**f. Managerial Group for Classified Research and Contracts**

The *Managerial Group for Classified Research and Contracts* includes the President, *Vice Provost for Research* or designee, and the *University Facility Security Officer*. The *Managerial Group Classified Research and Contracts* is responsible for the negotiation, execution, and administration of classified U.S. Government contracts at the University.

The *Managerial Group Classified Research and Contracts* provides oversight and direction for *Information Security and Privacy Incidents* involving National Security Information.

**g. University Facility Security Officer**

The *University Facility Security Officer* is responsible for directing and managing all aspects of the University's classified security program, including physical, personnel, computing, and special security. The *University Facility Security Officer* coordinates with and reports to appropriate Federal agencies regarding issues and *Incidents* related to *National Security Information* provided to or developed by the University under its classified contracts.

The responsibility of the *University Facility Security Officer* includes:

- Manage the creation and maintenance of the University *Rules/Policies, Standards, and Guidelines* related to *National Security Information*;
- Review and approve plans and procedures related to the protection of *National Security Information* at the University and at the University's organizational areas (e.g. colleges, schools, departments); and
- Serve as the University's liaison with law enforcement and other outside authorities who need to be informed about an *Information Security and Privacy Incident*.

**h. Data Custodians**

*Data Custodians* are appointed by and report to the *Data Trustees*. *Data Custodians* have knowledge of and work in accordance with numerous University *Policies* across the University, including the University *Rules/Policy Statements* on information security and privacy.

The responsibility of the *Data Custodians* includes:

- Help interpret, implement, and enforce the University's *Rules/Policies, Standards, and Guidelines* for *Institutional Information* within their purview;
- Identify *Systems of Record* containing *Institutional Information*;

- Categorize *Institutional Information* within *Systems of Record* as *Public*, *Restricted*, or *Confidential* according to the *University Rules/Policy Statements* on information security and privacy;
- Define access, quality, and usage *Standards* and *Guidelines* for *Institutional Information*; and
- Document and maintain institutional metadata.

**i. Executive Heads of Major University Organizations**

*The Executive Heads of Major University Organizations* are chancellors, vice presidents, vice provosts, deans, the Executive Director of Health Sciences Administration, and other individuals with delegated executive authority. These individuals, or their designee(s), have the following responsibilities:

- Oversee the *Confidentiality*, *Integrity*, and *Availability* of information or *Information Systems*;
- As needed, develop, implement and maintain *Rules/Policies*, *Standards*, or *Guidelines* for information security and privacy that are consistent with the *University Rules/Policy Statements* on information security and privacy and the *University Standards* and *Guidelines* issued pursuant to the *University Rules/Policy Statements*;
- Formally request exemptions to the *University Rules/Policy Statements* using the process set forth in Section 4 of this policy;
- Accountable for risks, compliance obligations, budgets, and financial costs associated with University information security and privacy, including *Information Security and Privacy Incidents* and *Information Security Breaches* within the organizational area(s) for which they are responsible;
- Follow the direction of the *University Chief Information Security Officer*, *University Privacy Official* of designee, or *University Facility Security Officer* in connection with an *Information Security and Privacy Incident* investigation, and direct others to do so; and
- Formally appoint, or have their designee(s) formally appoint, one or more *Information Assurance Liaisons* and *System Owners* for *Information System(s)* for which they are responsible.

**j. Incident Manager**

*An Incident Manager* is assigned by the *University Chief Information Security Officer*, *University Privacy Official* or designee, or *University Facility Security Officer* on a per *Incident* basis. Where required for *Incidents* involving *National Security Information*, the *Incident Manager* shall be an *Authorized Person*.

The responsibility of the *Incident Manager* includes:

- Under the direction of the designated official, manage and coordinate incident response, communication, and notification; and
- Coordinate *Incident* documentation and documentation retention activities.

**k. Systems Owners**

*System Owners* are formally appointed by and report to the *Executive Heads of Major University Organizations* or their designee(s).

The responsibility of the *System Owners* includes:

- Manage the *Confidentiality, Integrity, and Availability* of the *Information Systems* for which they are responsible. This shall include developing and implementing a process for managing access to *Information Systems* for which they are responsible, and other processes or controls in compliance with the University *Rules/Policy Statements* on information security and privacy;
- Advise *Executive Heads of Major University Organizations* on the financial resources necessary to develop and implement *Information Systems* and controls, including those specifically required by grants or contracts;
- Maintain critical *Information System* documentation; and
- Formally appoint and delegate responsibility to *System Operator(s)*.

#### **I. System Operators**

*System Operators* are formally appointed by and report to *System Owners*. Where required for *Information Systems* involving *National Security Information*, the *System Operators* shall be an *Authorized Person*.

The responsibility of the *System Operators* includes:

- Making and being accountable for operational decisions about the use and management of an *Information System*; and
- Responsibilities as delegated by *System Owners*.

#### **m. Information Assurance Liaisons**

*Information Assurance Liaisons* are formally appointed by and report to *Executive Heads of Major University Organizations* or their designee(s). Where required for *National Security Information*, the *Information Assurance Liaisons* shall be an *Authorized Person*.

The responsibility of the *Information Assurance Liaisons* includes:

- A point of contact for the University-wide information security and privacy related committees and officials as well as for the organizational area(s) for which they are responsible in matters related to information security and privacy concerns;
- Communicate with and educate *Workforce Members* regarding the *Confidentiality, Integrity, and Availability* of *Institutional Information, Information Systems*, and relevant the University *Rules/Policy Statements* as well as *Rules/Policies, Standards, and Guidelines* for the organizational area(s) for which they are responsible;
- Facilitate requests for access to *Information Systems* upon request by the *Data Custodians, System Owners*, and managers, including but not limited to, obtaining proper approval and determining appropriate access needs for staff; and
- Facilitate resolution of information security and privacy issues with the assistance of appropriate University colleges, schools, departments, or officials.

#### **n. Workforce Members**

*Workforce Members* are employees, trainees, students, volunteers, and other entities or persons who perform work for the University through employment, academic or service agreements, or contracts.

*Workforce Members* shall consult with and follow the applicable laws, regulations, and University-wide *Rules/Policy Statements*. In addition, *Workforce Members* shall consult any applicable University Guidelines.

*Workforce Members* shall only access and use University *Information Systems* and *Institutional Information* to fulfill authorized job duties or activities for the University.

### 3. Definitions

The following are definitions for terms used in the University *Rules/Policy Statements* on information security and privacy as well as *Standards* and *Guidelines* issued pursuant to the University *Rules/Policy Statements*.

**Access Control System:** Physical, administrative, or technical controls that grant and restrict individual access to *Information Systems*.

**Authentication:** A systematic method for establishing proof of individual identity when an individual accesses an *Information System*.

**Authorization:** The process to define which individuals are allowed access to an *Information System* and what privileges are allowed for each individual.

**Authorized Person:** An individual authorized to access *National Security Information* when the individual:

- Has the requisite U.S. Government security clearance, formal access approvals, and need-to-know for access *U.S. Government Classified Information*;
- Meets the conditions that define a U.S. Person (as defined in the Export Administration Regulations or International Traffic in Arms Regulations), or is covered under the terms and conditions of an export control license for access to export-controlled information; and
- A University employee for access to *Controlled Unclassified Information* that is not limited under export control regulations.

**Availability:** Information and *Information Systems* are accessible by authorized individuals.

**Computerized Devices:** A machine that includes or attaches to a computer. Examples include, but are not limited to medical devices, smart phones, or PDAs.

**Confidential Information:** Information that is very sensitive in nature and typically subject to federal or state regulations. Unauthorized disclosure of this information could seriously and adversely impact the University or the interests of individuals and organizations associated with the University.

To avoid confusion with federal Executive Order 12958 for classified *National Security Information*, confidential documents and data may be labeled "UW Confidential."

**Confidentiality:** Information or *Information Systems* are not accessed, acquired by, used, or disclosed to unauthorized parties.

**Controlled Unclassified Information (CUI):** Unclassified information that does not meet the standards for national security classification, but is pertinent to the national interests of the United States, and requires, under law or *Policy*, protection from unauthorized disclosure, special handling safeguards, or prescribed limits on exchange or dissemination. CUI includes:

- Export controlled information, whether or not it is related to a classified contract;

- Unclassified information that has been marked with U.S. Government distribution limitations, whether or not it is related to a classified contract; and
- All unclassified information related with a classified contract that has not been approved for public release.

**Guideline:** An approved and published recommendation, advice, procedure, or outline explaining how a *Rule/Policy Statement* or *Standard* may be implemented.

**Incident:** See definition for *Information Security and Privacy Incident*.

**Information System:** An assembly of electronic components that supports an operational role or accomplishes a specific objective. This may include a discrete set of information resources (e.g., network, server, computer, software, application, operating system, or storage devices) organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. These information resources may be under common management control and perform a common function.

**Information Security Breach:** Unauthorized access, acquisition, use, or disclosure, of *Confidential Information* or an *Information System* that contains *Confidential Information*.

**Information Security and Privacy Incident:** An event that adversely impacts the *Confidentiality, Integrity, or Availability* of *Institutional Information, Infrastructure Technology, or Information Systems*.

**Infrastructure Technology:** an electronic hardware device organized for the processing, maintenance, or management of an operational function (e.g. HVAC).

**Institutional Information:** All information which is created, received, maintained, or transmitted by the University. *Institutional Information* can be contained in any form, including but not limited to documents, databases, spreadsheets, email, and web sites; represented in any form, including but not limited to letters, numbers, words, pictures, sounds, symbols, or any combination thereof; communicated in any form, including but not limited to handwriting, printing, photocopying, photographing, and web publishing; and recorded upon any form, including but not limited to papers, maps, films, prints, discs, drives, memory sticks, and other *Information Systems*.

**Integrity:** Information or *Information Systems* have not been altered or corrupted by chance or by malice.

**National Security Information:** *U.S. Government Classified Information* and *Controlled Unclassified Information*.

**Policy and Rules/Policy Statements:** An approved and published set of rules. Violations of a *Rule/Policy* may result in discipline or loss of University privileges.

**Principle of Least Privilege:** Access privileges to any University *Information System* for any individual shall be limited to only what they need to have to be able to complete their assigned duties or functions.

**Principle of Separation of Duties:** Whenever practical, no one person shall 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.

**Protected Health Information (PHI):** See UW Medicine Compliance's privacy policies.

**Public Information:** Information that is published for public use or has been approved for general access by the appropriate University authority.

**Restricted Information:** Information that is circulated on a need to know basis and sensitive enough to warrant careful management and protection to safeguard its *Integrity* and *Availability*, as well as appropriate access, use, and disclosure.

**Standard:** An approved and published explanation that elaborates on a *Rule/Policy*. Violations of *Standards* may result in discipline or loss of University privileges.

**Subject Area Domains:** *Institutional Information* is classified according to specific high-level *Subject Area Domains* for the purpose of assigning accountability and responsibilities over that data. The *Subject Area Domains* are defined in the University Data Map. Examples of high-level *Subject Area Domains* are Human Resources, Academics, Financial Resources, University Advancement, etc. The University Data Map further defines specific business domains within each *Subject Area Domain*. Examples of business domains within the Academics *Subject Area Domain* are Curriculum and Courses, Financial Aid, Applications Admissions and Enrollments, Transcripts Degrees and Awards, etc.

**System of Record:** An *Information System* that is designated by the University *Data Custodians* as holding official values of *Institutional Information*. Official values are the data designated as the most accurate representation of the meaning and context of *Institutional Information* elements which are recorded as facts. Official values are not necessarily the originally entered values, and as such, a *System of Record* may not necessarily be the system where values are originally entered. When questions arise over the meaning or interpretation of data elements, or their values, the *System of Record* is used to resolve discrepancies.

**United States (U.S.) Government Classified Information:** Official information, owned by the U.S. Government or entrusted to the U.S. Government by another country, that has been determined, pursuant to U.S. Presidential Executive Order 12958 or any predecessor order, to require protection against unauthorized disclosure in the interest of national security and which has been so designated. The three levels of classification defined by Executive Order 12958 are CONFIDENTIAL, SECRET, and TOP SECRET.

**Users:** Any individual that has been granted access and privileges to *Information Systems*.

#### 4. Exemptions

A written request for an exemption to the University *Rules/Policy Statements* on information security and privacy or a *Standard* issued pursuant to the University *Rules/Policy Statements* shall be submitted for review and potential approval to the *University Privacy Official*, *University Chief Information Security Officer*, and the *Managerial Group for Classified Research and Contracts*.

#### 5. Policy Maintenance

The *University Privacy Official*, the *University Chief Information Security Officer*, and the *Managerial Group for Classified Research and Contracts* shall review and approve this policy at least every three years or more frequently as needed to respond to changes in the regulatory environment, prior to being sent for final approval by those who have been delegated executive authority. The *University Chief Information Security Officer* shall manage the review process.

#### 6. Enforcement

The individuals with responsibility to enforce the University *Rules/Policy Statements* on information security and privacy are identified herein or in a specific *Rule/Policy Statement*.

Failure by a *Workforce Member* to comply with the University *Rules/Policy Statements* on information security and privacy may result in disciplinary action up to and including termination for University employees, contract termination in the case of contractors or consultants; dismissal for interns and volunteers; or suspension or expulsion in the case of a student.

The University reserves the right to pursue appropriate legal actions to recover any financial losses suffered as the result of a violation of the University *Rules/Policy Statements* on information security and privacy.

## 7. Additional Information

For further information on this policy contact:

- University Chief Information Security Officer
- Phone: 206-685-0116
- Campus mail: Box 352820
- Email: [ciso@uw.edu](mailto:ciso@uw.edu)
- UW Medicine Chief Privacy Officer
- Phone: 206-543-3098
- Campus mail: Box 358049
- Email: [comply@uw.edu](mailto:comply@uw.edu)
- University Facility Security Officer
- Phone: 206-543-1315
- Campus mail: Box 355640
- Email: [uwfso@uw.edu](mailto:uwfso@uw.edu)

**Appendix A.**

**University Rules/Policy Statements on  
Information Security and Privacy**

<b>APS Number</b>	<b>Title</b>	<b>Brief Description</b>
2.4	Information Security and Privacy Roles, Responsibilities, and Definitions	The University <i>Rules/Policy Statements</i> on information security and privacy is a critical foundation for establishing the principles of <i>Confidentiality, Integrity, and Availability</i> for <i>Institutional Information or Information Systems</i> at the University. This policy establishes roles, responsibilities, and definitions that are used in all University <i>Rules/Policy Statements</i> on information security and privacy as well as the University <i>Standards and Guidelines</i> issued pursuant to the University <i>Rules/Policy Statements</i> .
2.1	University Information Systems Security Policy	Protective measures for <i>Information Systems</i> that collect, maintain, and use information at the University.
# TBD	Privacy Policy	Pending revision
2.5	Information Security and Privacy Incident Management Policy	Describes the process used by the University for assessing, responding to, and managing <i>Information Security and Privacy Incidents</i> .
2.10	Minimum Data Security Standards: Data Classification and Related Measures of Protection	<i>Standards</i> for classify data as confidential, restricted, or public. Includes <i>Information Systems</i> controls (that are mentioned in APS 2.1) and other protective measures based on the data classification.