University Data Policies

BACKGROUND

Data are valuable institutional assets of Washington State University. Data policies are needed to ensure that these resources are carefully managed, maintained, protected, and used appropriately.

Five areas have been identified which require data policy statements:

Data Administration—Management accountability for administering institutional data;
Data Authorization and Access—Authorization and access to institutional data;
Data Usage—Appropriate use and release of institutional data;
Data Maintenance—Upkeep of institutional data; and
Data Security—Protection of institutional information assets.

SCOPE

These policies apply to all institutional business units, workforce members, and institutional information systems that collect, store, share, process, or transmit institutional data.

DEFINITIONS

See supporting section *BPPM* 87.01 for definitions applicable to this policy.

ENFORCEMENT

The Office of the Chief Information Officer (CIO) is responsible and has the authority for enforcing compliance with this policy.

VIOLATIONS

Persons determined to have violated this policy are subject to sanctions imposed using the procedures set forth in applicable University policies and handbooks (e.g., the WSU *Faculty Manual*, the *Administrative Professional Handbook*, *WAC* 357-40 (civil service employees), applicable collective bargaining agreements, and the WSU Standards of Conduct for Students, *WAC* 504-26).

MAINTENANCE

The Office of the CIO is to review this policy every three years or on an as-needed basis due to changes to technology environments, business operations, legal, or regulatory requirements.

EXCEPTIONS

Exceptions to this policy must be approved by the Office of the CIO, under the guidance of the appropriate information owner(s) and the University Chief Information Security Officer.

The Office of the CIO must document and maintain all policy exceptions in writing for the life of the exceptions. Approvals for policy exceptions are effective for a specified period of time and must be reviewed by the Office of the CIO on a periodic basis.

University Data Policies

Data Administration Policy

PURPOSE

Data are valuable institutional resources and must be carefully managed and maintained to ensure the availability, integrity, confidentiality, and privacy of institutional data. This data administration policy is intended to ensure that all institutional data are managed as institutional assets for fulfilling the University's mission of instruction, research, outreach, and engagement. This policy also defines institutional roles and responsibilities that are essential to the appropriate oversight and execution of these University data policies.

DATA ADMINISTRATION POLICY STATEMENT

Institutional data must be properly administered, managed, and maintained throughout its entire life-cycle. Information owners are accountable for the security and privacy of institutional data under their care.

ROLES AND RESPONSIBILITIES

Information Owner

Responsibilities of the information owner include the following:

- Assigning appropriate classifications to institutional information (i.e., public, internal, confidential, or regulated);
- Ensuring that the appropriate technical, administrative, and physical controls and processes are implemented for safeguarding the confidentiality, privacy, integrity, and availability of institutional data based on the classification of the information;
- Establishing appropriate use and data handling processes and procedures for operational and administrative management of institutional data;
- Establishing and approving appropriate authorization processes for granting access to institutional data based on the appropriate level of access, need-to-know, and applicable legal or regulatory requirements; and
- Accepting the information security and privacy risk to the University and individuals from business unit operations.

Data Custodian

Responsibilities of the data custodian include the following:

- Identifying and documenting systems containing institutional data within their specific area of responsibility;
- Categorizing institutional information within their specific area of responsibility according to University information security and privacy policies, standards, procedures, and guidelines;

University Data Policies

Data Administration Policy (cont.)

Data Custodian (cont.)

- Understanding and documenting how institutional data is generated, collected, stored, processed, transmitted, accessed, released, maintained, and disposed of in the systems of record for which they are responsible;
- Implementing the appropriate administrative, physical, and technical safeguards to ensure the confidentiality, privacy, integrity, and availability of institutional data;
- Reviewing and approving requests for access to institutional data within their area of responsibility; and
- Ensuring that business unit policies and procedures are consistent with University policies, standards, and procedures.

Data User

Institutional and personal responsibilities of data users include the following:

- Following the appropriate policies, standards, procedures, and guidelines governing the usage, security, and privacy of institutional data; and
- Reporting suspected or actual vulnerabilities pertaining to the confidentiality, integrity, or availability of institutional data.

University Data Policies

Data Authorization and Access Policy

PURPOSE

Access to institutional data in its many forms is vital to the successful operation of the University. Faculty, staff, students, and authorized University affiliates and third parties need appropriate access to University data in support of University business functions. In turn, all users authorized to access institutional data are obligated to appropriately use and effectively protect institutional data. This policy defines classifications for WSU data and provides some guidance for classifying WSU information. These classifications provide guidance for determining institution-wide data protection standards, and the information security and privacy risks associated with collecting, accessing, sharing, storing, processing, and transmitting institutional data.

The policy is intended to supplement, not override, the definition of access to data under Washington Public Records Act, *RCW* 42.56, and the Preservation of Public Records law, *RCW* 40.14.

DATA AUTHORIZATION AND ACCESS POLICY STATEMENT

Access to institutional data must be provided to authorized individuals in support of University business functions. Authorization to access institutional data is to be granted by the appropriate information owner or their designee to only those with a legitimate need. Information owners or their designees are to define, for their areas of responsibility, the workforce members who are authorized to access institutional data and to ensure that only authorized workforce members have access to such data. Authorization to access institutional systems and data must support the principles of least privilege and separation of duties. (See *BPPM* 87.01 for definitions of these principles.)

An individual's access to his/her own student or employment information, however, is governed by law and is not constrained by these categories.

Institutional information must be categorized according to the following:

Information Classifications

Public—Information in this classification does not need protection from unauthorized access or disclosure; however, there may be requirements to protect the integrity and availability of data in this classification. See also *BPPM* 87.01.

Internal—This information may be made available to authorized University personnel in support of the performance of their assigned roles/duties, and may be released to authorized University affiliates or third parties with approval from the appropriate information owner, or as required by law. Unauthorized access, disclosure, or loss of integrity or availability of this classification of information could result in some harm to the University or to individuals. See also *BPPM* 87.01.

University Data Policies

Data Authorization and Access Policy (cont.)

Information Classifications (cont.)

Confidential—Access may be granted to this classification of information by the appropriate information owner to only authorized personnel with a strict need-to-know. Confidential information may be released to authorized University affiliates or third parties only with explicit approval from the appropriate information owner, or as required by contract or law. Unauthorized access, disclosure, or loss of integrity or availability of this information could cause significant harm to the University and its operations, assets, or to individuals, and may include significant reputational, legal, and financial consequences. See also *BPPM* 87.01.

Regulated—Access may be granted to this classification of information by the appropriate information owner to only authorized personnel with a strict need-to-know. This information may be released to affiliates or groups outside of the University community only with explicit approval from the appropriate information owner, or as required by contract or law. Unauthorized access, disclosure, or loss of integrity or availability of this information could cause significant or serious harm to the University and its operations, assets, or to individuals, and may include significant or serious reputational, legal and financial consequences, including civil and criminal penalties. See also *BPPM* 87.01.

University Data Policies

Data Usage Policy

PURPOSE

Authorization to access institutional data carries with it the responsibility to use the data for its intended purposes and not for personal gain or other inappropriate purposes. This data usage policy is intended to ensure that institutional data are used appropriately and in support of fulfilling University mission and business objectives.

DATA USAGE POLICY STATEMENT

Institutional internal, confidential, and regulated information must be used only in the performance of assigned roles/duties within the University unless an approved agreement allows release to a third party as provided for under "Release of Institutional Data" below, or as permitted by law.

DATA USAGE RESPONSIBILITY

Individuals are responsible for using institutional data and any information derived from them appropriately. Institutional data must not be used to promote or condone discrimination on the basis of race/ethnicity, color, creed, religion, national origin, gender, gender identity or expression, sexual orientation, age, marital status, the presence of any sensory, mental, or physical disability, or whether a disabled or Vietnam veteran. Institutional data must not be used to promote or condone any type of harassment, copyright infringement, political activity, personal business interests, or any activity that is unlawful and/or precluded by University policies.

Willful misuse of institutional data, violation of state ethics laws and rules with regard to institutional data, or other breaches of this policy, can result in termination of access privileges, University disciplinary action which may include termination of employment, student discipline in accordance with WSU policy, and/or civil and criminal penalties. (See Ethics in Public Service, *RCW* 42.52, or http://ethics.wa.gov/. For information on appropriate use, see EP4: Electronic Communication Policy.)

RELEASE OF INSTITUTIONAL DATA

The release of institutional data must be in compliance with University policies, and federal and state laws and regulations, and must be approved by the appropriate information owner or their designee.

Use of any cloud or third-party system which will be used to collect, store, process, share, or transmit institutional data, must be authorized by the appropriate information owner or their designee, prior to use in accordance with institutional policies, standards, and procedures. Such a use must be documented by a written contract or agreement between the University and the third party, unless required by law. If there are financial considerations, the appropriate Finance and Administration personnel must review and approve the contract. (See *BPPM* 10.11 for contract procedures.)

(NOTE: The above requirement does not apply to release of data under the Public Records Act, *RCW* 42.56. See *BPPM* 90.05.)

University Data Policies

Data Usage Policy (cont.)

RELEASE OF INSTITUTIONAL DATA (cont.)

Information that is considered to be public and is to be published on a publicly accessible information system, must be authorized by the appropriate information owner or their designee. The information owner must periodically review information that has been made publicly available on institutional information systems for non-public information. If institutional internal, confidential, or regulated information has been discovered to have been made available to the general public, it must be promptly removed by the appropriate business unit.

The sharing or release of institutional confidential or regulated information to a service provider or other third party requires that the responsible institutional business unit request a written statement of information security risk from the Office of the CIO. The responsible business unit is accountable and responsible for accepting the information security and privacy risk of institutional data that are released to third parties.

Information systems that store and process institutional confidential and regulated data must reside in the U.S., to include such data stored in backup systems and systems for disaster recovery and business continuity purposes.

University Data Policies

Data Maintenance Policy

PURPOSE

Institutional data are managed as institutional assets for use by the University community. The usefulness and effectiveness of institutional data depend on these data being available, accurate, and complete. This data maintenance policy is intended to ensure the availability and integrity of institutional data.

DATA MAINTENANCE POLICY STATEMENT

Institutional data must be maintained by authorized individuals on behalf of the University throughout its entire life-cycle.

DATA AVAILABILITY AND INTEGRITY

Every effort must be made to ensure the availability, accuracy, and completeness of institutional data. Access to data for management and maintenance purposes must be authorized by the appropriate information owner or their designee.

It is the responsibility of each business unit that creates, collects, stores, processes, shares, and transmits institutional data to ensure the application of uniformly high standards in data management and maintenance, to include the availability and integrity of the institutional data under their care throughout its entire life-cycle. See the Data Security Policy section of this document for University policy on retention and disposition of institutional data.

University Data Policies

Data Security Policy

PURPOSE

The purpose of this policy is to establish University requirements to ensure the confidentiality and privacy of institutional data.

DATA SECURITY POLICY STATEMENT

Institutional business units must maintain an up-to-date inventory of all institutional confidential and regulated information under their purview, to include information collected, stored, processed, shared, or transmitted by cloud providers or other third parties.

Institutional information that is categorized as confidential or regulated, and is stored, processed, shared, or transmitted on University or third-party information systems, must be encrypted. This is to include all production, development, test, and back-up information systems.

Mobile devices, portable storage media, and all electronic media containing institutional confidential and regulated data must be encrypted and stored in physically secure locations.

Electronic transmission of institutional confidential and regulated data must be encrypted during transmission to and from institutional information systems, to include affiliates and third parties.

Encryption methods must use industry-standard encryption technologies that have been validated by an established standards body such as the National Institute of Standards and Technology (NIST). Acceptable industry standard cryptographic key management practices must be appropriately managed and maintained to safeguard the cryptographic keys and to protect the integrity of the encryption processes.

All institutional data covered by federal or state standards, laws, regulations, or contractual agreements are to meet the information security and privacy requirements defined by those standards, laws, regulations, or contracts.

DATA RETENTION AND DISPOSITION

A current copy of institutional data must be preserved to ensure the restorability of data lost to disaster or destruction. Procedures to recover lost data must be in place. See also EP25: Executive Policy on Emergency Management and Safety Plans, *Business Policies and Procedures Manual* (*BPPM*) section 50.39: Emergency Planning and Preparedness, and/or *BPPM* 90.15: Essential Records Protection.

Care must be taken to ensure that information is not recoverable using available forensic tools when a computer and/or its storage media are scheduled for surplus sales or other reuse either within or outside of the University. Prior to disposal, internal, confidential, and regulated data recorded in any media must be disposed of in a manner that renders the data unrecoverable and/or destroyed. Refer to *BPPM* 90.01 for details.

University Data Policies

Data Security Policy (cont.)

DATA RETENTION AND DISPOSITION (cont.)

Departments are responsible for the required retention, preservation, destruction, and disposition of University public records in accordance with retention periods approved by the Washington State Records Committee. (*RCW* 40.14). See *BPPM* 90.01.

SECURITY AND PRIVACY INCIDENTS

All security incidents or suspected incidents involving institutional data must be reported immediately to the Information Technology Services (ITS) Security Operations Center at 509-335-0404.

Various state and federal laws and regulations may contain specific breach reporting requirements (e.g., FERPA, HIPAA, GDPR, GLBA, Washington State *RCW* 42.56.590). Breaches, or potential breaches of University confidential or regulated information must be reported immediately to the Chief Information Security Officer (CISO) or the Office of the Chief Information Officer (CIO).