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 faculty, staff, students, authorized University affiliates, and third parties who access, share, store, process, and transmit institutional data.

DEFINITION

Institutional data are the items of information, which are collected, used, and maintained by WSU for strategic and operational functions, to include administrative data and other data maintained and safeguarded for institutional purposes. This includes data held by central offices as well as data held by departments or individuals. These data policies apply to all institutional data such as that held for the purposes of administration, research, scholarship, education, outreach, and engagement.

ENFORCEMENT

The Office of the Chief Information Officer is responsible for enforcing this policy. 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).

EXCEPTIONS

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

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. 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 throughout its entire life-cycle by executive officers of the University (i.e., University area and college heads). As such, University area and college heads (e.g., vice presidents, deans, directors) fulfill the role of information owner and are accountable for the information security and privacy of institutional data under their care.

ROLES AND RESPONSIBILITIES

Information Owner

An information owner is accountable for the stewardship of institutional data within their area of responsibility. They are responsible for ensuring the implementation of the information security and privacy requirements for safeguarding institutional data, to include its generation, collection, storage, processing, transmission, usage, access, release, maintenance, and disposal. An information owner may delegate these administrative duties to one or more University administrators known as data custodians for specific institutional data sets or functional areas. The information owner, however, retains ultimate accountability, to include when data is shared or released to third parties.

Responsibilities of the information owner include the following:

- Assigning appropriate classifications to institutional data
- Ensuring that the appropriate security controls are implemented for safeguarding the confidentiality, integrity, and availability of institutional data
- Establishing appropriate use and data handling processes and procedures for operational and administrative management of institutional data
- Establishing and approving appropriate criteria for granting access to institutional data based on the appropriate level of access authorization and need-to-know
- Accepting the residual information security and privacy risk to the University and individuals from area or college business operations, and any actions taken to avoid, mitigate, or transfer the risk

University Data Policies

Data Administration Policy (cont.)

Data Custodian

A data custodian is a University administrator who is assigned to and is accountable to an information owner. A data custodian has administrative and/or operational responsibility over the specific institutional data sets delegated to them by an information owner. This individual is responsible for facilitating, implementing, and enforcing institutional data policies, standards, and procedures established by the University and/or the information owner.

Responsibilities of the data custodian include the following:

- Identifying and documenting systems containing institutional data within their specific area of responsibility
- Categorizing institutional data within their specific area of responsibility according to University information security and privacy policies, standards, procedures, and guidelines
- 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 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
- Ensuring that area or college policies and procedures are consistent with University policies, standards, and procedures

Data User

A data user is any University employee, student, individual, affiliate, or third party who is authorized to access institutional systems and data.

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
- Reporting suspected or actual vulnerabilities pertaining to the confidentiality, integrity, or availability of institutional data
- Reporting suspected or actual breaches in the confidentiality, integrity, or availability of institutional data to the Office of the Chief Information Officer

Chief Information Officer (CIO)

See EP37: WSU Information Security Policy for the definition of CIO.

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 also help with determining the information security and privacy risks associated with 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 that are appropriate for the roles and responsibilities of the authorized individuals. Authorization to access institutional data is granted by the appropriate information owner or University administrator to those with a legitimate need. Authorization is granted based on the classification of University data to be accessed, an individual's roles and responsibilities, and need-to-know.

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 data must be categorized according to the following:

Data Classifications

Public—Information that is currently released or approved to be released to the public without restriction by the appropriate information owner. 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. Examples of public information are employee directory information, public University outreach and research publications, press releases, and information on the public WSU website (https://wsu.edu/).

Internal—Information that is intended for official WSU business purposes only. This information may be made available to authorized University personnel with a legitimate need 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. It is not appropriate for information in this classification to be made available to the general public. 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. Examples of internal information may include information concerning various University business transactions, operations, and strategies and methods that may be considered to provide a competitive advantage.

University Data Policies

Data Authorization and Access Policy (cont.)

Data Classifications (cont.)

Confidential—Information that is specifically protected by law, contracts, third-party agreements, or for other University business reasons as established by the appropriate information owner. Access may be granted to this classification of information by the appropriate information owner to only authorized personnel with a legitimate 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 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 individuals. Information in this category may include employee personnel records, financial information, donor information, intellectual property, attorney/client privileged information, information regarding critical infrastructure of physical structures and assets, and the security and infrastructure of information technology systems.

Regulated—Information that is specifically protected by federal, state, local, or industry policies and/or laws and regulations, for which strict protection, use, and handling requirements are dictated. Access may be granted to this classification of information by the appropriate information owner to only authorized personnel with a legitimate 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 law. Unauthorized access, disclosure, or loss of integrity or availability of this information could cause serious harm to the University and its operations, assets, or individuals. Data in this classification may be exempt from public records or other legal requests.

As an institution of higher education, WSU collects, stores, and processes a vast quantity of very sensitive data in conducting its day-to-day business operations and is therefore subject to the various information security and privacy laws that regulate the access, use and handling of that information. The list below includes, but is not limited to, specific laws and regulations that are included in this classification.

- Family Educational Rights and Privacy Act (FERPA)
- Gramm-Leach-Bliley Act (GLBA)
- Health Insurance Portability and Accountability Act (HIPAA)
- Health Information Technology for Economic and Clinical Health Act (HITECH Act)
- Payment Card Industry Data Security Standard (PCI DSS)
- European Union General Data Protection Regulation (GDPR)
- Protected Personal Information (*RCW* 19.255.010; *RCW* 42.56.590)
- Federal Trade Commission (FTC) Red Flag Rule (Identity Theft Regulation)
- Regulations Governing the Protection of Research Data (e.g., Federal Information Security Management Act (FISMA), Controlled Unclassified Information (CUI), Washington State Uniform Trade Secrets Act (*RCW* 19.108))
- National Security Information

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

Internal, confidential, and regulated institutional data 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 Data to Third Parties below.

DATA USAGE RESPONSIBILITY

Each individual with access to institutional data has the responsibility to use those 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, 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, 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 DATA TO THIRD PARTIES

The release of institutional internal, confidential, and regulated data must be in compliance with federal and state laws and regulations and must be approved by the appropriate information owner(s). The area or college considering the release of confidential or regulated data must request a statement of information security risk from the Office of the CIO. The business unit(s) must accept accountability and responsibility for the stated data security and privacy risk prior to releasing the data. Such a release must be documented by a written agreement between the University and the third party. 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 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

The availability and integrity of 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. Data collection, storage, and maintenance must be performed as close to the original source of the data as feasible. Access to data for maintenance purposes must be authorized by the appropriate information owner.

All collection, storage, and maintenance of centrally-managed institutional data must be appropriately managed and maintained by centrally-administered institutional systems and processes.

It is the responsibility of each unit that generates, collects, stores, and maintains institutional data to ensure the application of uniformly high standards in data management to ensure the availability and integrity of the institutional data under their care throughout its entire life-cycle. See 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, privacy, integrity, and availability of institutional data, and to prevent the unauthorized use, release, modification, or loss of institutional information assets.

DATA SECURITY POLICY STATEMENT

Institutional data that is categorized as confidential or regulated, and is stored, processed, or transmitted on University or third-party information systems, must be encrypted.

Mobile devices and portable storage 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.

See also EP37.

REPORTING INFORMATION SECURITY INCIDENTS

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

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. Refer to *BPPM* 90.01 for details.

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.