WASHINGTON STATE UNIVERSITY
EXECUTIVE POLICY MANUAL
Executive Policy #8
Revision Approved February 5, 2015

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 and wisely used.

Five areas have been identified which require data policy statements:

Data Administration—Management responsibility for University data,
Data Access—Inquiry and download access to University data,
Data Usage—Appropriate use and release of University data,
Data Maintenance—Upkeep of University data, and
Data Security—Physical protection of University data.

DEFINITION

University data are the items of information, which are collected, maintained, and used for the continued operations of Washington State University, specifically administrative data and other data maintained and safeguarded for University operational purposes. This includes data held by central offices as well as data held by departments or individuals. Operational data such as that held by the Offices of the Vice President for Research, Grant and Research Development, Research Assurances, and Intellectual Property Administration is covered by these data policies. Other research data, scholarly work of faculty or students, and intellectual property are not covered by this policy. For security and retention rules for such data, contact the Office of Research, the Graduate School, Student Affairs, Enrollment Management, and/or Institutional Research.

Where referenced in this policy, **data encryption** shall be accomplished according to current commercially reasonable business practices as outlined in Appendix A.

University Data Policies

Data Administration Policy

PURPOSE

Data are valuable resources for the University and must be carefully managed. This data administration policy is intended to ensure that all University data are managed as institutional assets for fulfilling the University's mission of instruction, research, and public service.

DATA ADMINISTRATION POLICY STATEMENT

University data shall be administered by executive officers of the University, referred to as data stewards.

DATA STEWARDS

Data stewards have charge over University data and are responsible for its safekeeping. Each data steward is responsible, within the bounds of University data policy, for operational policies and procedures governing inquiry and download access, dissemination, usage, collection, maintenance, and protection of the data in a designated data area. The data steward is responsible for the definition and classification of data in that area as well as verifying its authenticity as needed. Documentation characterizing shared University data will be maintained and made available for University use.

A data steward may delegate any or all of his/her data administration duties to another University administrator known as a data custodian, however the data steward retains ultimate responsibility. The data steward and data custodian for each set of University data are listed in Appendix B.

University Data Policies

Data Access Policy

PURPOSE

Data and ready access to that data in its many forms are vital to the successful operation of the University. Faculty, staff, and others need appropriate access to University data through online inquiry and/or downloads in support of University functions. In turn, faculty, staff, and others with access are obliged to appropriately use and effectively protect University 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 ACCESS POLICY STATEMENT

University data shall be accessible for inquiry and/or download by authorized employees or other authorized individuals in support of University functions appropriate to the role/duties of the authorized individual.

DATA ACCESS AUTHORIZATION

Access to University data for inquiry and/or download purposes (through centrally or departmentally supported applications software, user-written software, or other means) will be authorized on the basis of data inquiry access categories and the individual's roles/duties. An individual's access to his/her own student or employment information, however, is governed by law and is not constrained by these categories.

Data stewards will classify the data for which they are responsible according to the following inquiry access categories:

Public Data—Data that are of interest to the general public and for which there is no University business need or legal reason to limit access. Public data may be made available to the general public in printed or electronic format, e.g., at the WSU library, WSU Campus Directory, WSU web sites, etc. Anyone in the general public may view these data using such public sources. However, the University does not provide these data in other than the published form(s) without the consent of the appropriate data steward and/or Public Records Officer, or as required by law. Examples of public data are employee names, work addresses, and work telephone numbers.

Non-Public Data—All data held by the University for operational, educational, and/or other purposes which are not appropriate or available for general public use. Non-public data shall be made available to authorized University employees for inquiry/download only in support of the performance of their assigned roles/duties. Non-public data may be released to individuals or groups outside of the University community only with approval from the appropriate data steward, Public Records Officer, or as required by law. Examples of non-public data include records subject to disclosure under law including University business transactions, employee records, student records, and other data so disclosable.

Confidential Data—Data to which access is restricted for legal or other University business reasons including personal information as described in Appendix C. Examples of confidential data include a person's name together with social security number or bank account number or driver's license number, a person's WSU Network ID together with its password, certain personnel records, certain student records, etc.

University Data Policies

Data Access Policy (cont.)

DATA ACCESS AUTHORIZATION (cont.)

Access to general non-public data may be granted through authorization to use a related administrative and/or student information system. However, access to confidential data must be explicitly authorized by the data steward, based on University need, unless relevant law provides otherwise. The appropriate data steward will determine whether an individual's stated business need for access to confidential data is legitimate and appropriate. (See page five regarding release of data to third parties.)

All members of the University community are responsible to access non-public data only for legitimate purposes of University business. Each member of the University community with authorization to access non-public University data must document with a signed statement that he/she understands and will comply with University policies and procedures applicable to that data. Authorization to access non-public data and confidential data will be terminated when the individual no longer has a business need for the data or his/her affiliation with the University ends.

University Data Policies

Data Usage Policy

PURPOSE

Authorization to access University data carries with it the responsibility to use the data as intended and not for personal gain or other inappropriate purposes. This data usage policy is intended to ensure that University data are used appropriately.

DATA USAGE POLICY STATEMENT

Non-public and confidential University data shall be used only in the performance of assigned roles/duties within the University unless an approved agreement allows release to an external entity as provided for under "Release of Data to Third Parties" below.

DATA USAGE RESPONSIBILITY

Each individual with access to University data has the responsibility to use those data and any information derived from them appropriately. **Individuals will be held responsible for any use made of University data under their user IDs and passwords.** (See EP18: Computer and Network User Identification and Password Policy.)

University 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 era veteran. University 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 University data, violation of state ethics laws and rules with regard to University 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

A data steward approves the release of University non-public and confidential data under his or her jurisdiction if the release is in conformance with state and federal regulations. Information Technology Services provides a statement of data security risk to the data steward and those considering the release. Such a release is documented by a written agreement between the University and the third party. If there are financial considerations, Finance and Administration contract personnel 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

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

DATA MAINTENANCE POLICY STATEMENT

The integrity of University data shall be maintained by authorized individuals on behalf of the University.

DATA INTEGRITY

Every effort must be made to ensure the accuracy, timeliness, and completeness of University data. Data collection and maintenance shall be performed as close to the original source of the data as feasible. Access to data for maintenance purposes shall be authorized by the appropriate data steward.

All collection and maintenance of centrally-managed University data must be processed through centrally-managed edit routines. This includes uploaded data or other electronically-supplied data values.

It is the responsibility of each unit that generates and manages institutional data to ensure the application of uniformly high standards in data management to ensure that the integrity is never compromised.

A Data Advisory Group (DAG) has been established to facilitate efforts to maintain data integrity. For information regarding the Data Advisory Group go to:

https://ir.wsu.edu/Data Advisory Group

University Data Policies

Data Security Policy

PURPOSE

University data must be effectively protected from unauthorized acquisition or disclosure as well as accidental or intentional modification, destruction, or loss. This must be done to ensure data confidentiality, integrity and to prevent unnecessary litigation or penalty against the University and its employees.

University data and information can be maintained and represented in various formats including electronic storage, screen display, printed copy, etc. Each member of the University community has an obligation to protect data under his/her control.

DATA SECURITY POLICY STATEMENT

University data shall be safeguarded to ensure its confidentiality, integrity, reliability and availability.

DATA SECURITY

All confidential data connected with an individual's name shall be stored securely on physically secured storage devices or media and displayed in an encrypted or otherwise obscured manner. Confidential data will be disclosed in full only to specifically authorized individuals as needed to conduct business functions of the University.

Non-public University data shall be stored or transported on portable devices/media (laptops/tablets, USB drives, CD-ROM, DVD, etc.) only as required to conduct University business functions. Where necessary to store or transport such data on a portable device/medium, they should be protected from disclosure in the event of device/media loss using commercially reasonable business practices such as device locks or data encryption.

Non-public University data must be protected during network transmission according to commercially reasonable business practices such as secure transport mechanisms or data encryption.

Individual WSU employees and agents are responsible for accessing and implementing security software and tools the University makes available. A department or individual employee may substitute software or tools that provide a level of security equal to or greater than those provided by the University, so long as the department or individual employee has obtained all necessary licenses for such use.

All security incidents or suspected incidents involving a computer containing University confidential or personally-identifiable information must be reported immediately to the Information Technology Services (ITS) Network Operations Center at 509-335-4949.

DATA RETENTION AND DISPOSITION

A current copy of University data must be preserved to ensure the restorability of data lost to disaster or destruction. Procedures to recover lost data must be in place. However, other than the official source copy and appropriate backup copies of University data, data shall be held in other locations only as necessary and only for as long as necessary to conduct the business of the University as required by policy and/or law.

University Data Policies

Data Security Policy (cont.)

DATA RETENTION AND DISPOSITION (cont.)

Non-public and confidential data recorded in any media must be disposed of in a manner that will render the data unrecoverable. Care must be taken to ensure that information is not recoverable using readily available forensic tools when a computer and/or its storage media are scheduled for surplus sales or other re-use either within or outside of the University. Data residing on a computer or storage media should be removed before passing the device or media on to another employee unless that individual is assuming the role/duties and has the same data access privileges as the previous user.

Departments are responsible for retaining and disposing of University records in accordance with retention periods approved by the Washington State Records Committee. (*RCW* 40.14). Refer to the WSU *Business Policies and Procedures Manual*, section 90.01 for details.

University Data Policies

Appendix A – Commercially Reasonable Business Practices

Commercially reasonable standards are practices and procedures in widespread use in the business community generally considered to represent prudent and reasonable business methods. These standards provide methods of data encryption, user identification, digital signatures, etc. The use of these standards provides evidence that due diligence has been exercised by the University.

Appendix B – Data Stewards

Set of Data	**Data Steward**	**Data Custodian**
Associate Address*	Vice President, Information Services and Chief Information Officer (CIO)	Chief Information Security Officer
Donor	Vice President, Development and CEO WSU Foundation	Associate Vice President and Director of Technology and Advancement Records
Facilities, Financial, Personnel	Vice President, Finance and Administration	Executive Director of Budget and Resource Planning, Finance and Administration
Library	Provost	Assistant Director, Systems and Planning, WSU Library
Research	Vice President for Research	Director, Office of Grant and Research Development
Student	Provost	Registrar
Student Health Data	Vice President, Student Affairs	Executive Director of Health and Wellness Services

* Includes identity and access information such as authentication, authorization, individual usage data, and e-mail.

University Data Policies

Appendix C – Personal Information

Washington State **RCW 42.56.590** (Personal Information -- Notice of Security Breaches) defines "personal information" as an individual's name (last name plus first name or initial) in combination with any of the following data: social security number, driver's license number or Washington identification card number, or credit card, debit card or bank account number along with the security/access code that would permit access to the person's financial account(s).