Responsible Executive: VP for Information Services

Responsible Office: Office of Information Services

Effective: June 27, 2017

Last Revised: June 27, 2017

University Policy 08-015

University Data Management, Classification, and Incident Response

1. Policy Statement

1.1. The purpose of this policy is to improve data and information access, accuracy, and integrity, while applying appropriate security controls and protection to manage risk.

2. Reason for Policy

2.1. Oregon State University (“university”) generates and accesses a significant amount of information and data that are essential to the university’s business operations. These data, which include social security records, academic records, employee records, contractual agreements and billing information, and student records, are necessary for university operations. Such data are strategic assets and are essential to the university’s operation as an institution of higher education. While data may reside in different databases and on different systems, in aggregate, they support institutional operations, performance, and decision-making. However, in order for the value of these data to be realized, the information must be accurate, made as widely available as possible, and used appropriately.

2.2. The university has an established history of sharing data with the many communities of which it is a part. The university is also entrusted by our constituencies with data of a private or personal nature. The university is committed to protecting such data. Additionally, there are state and federal laws that identify certain types of data that must be treated with care. This policy establishes a framework to allow the university to comply with all federal and state laws, regulations, and policies pertaining to data management, classification, and incident response, in order to protect the confidentiality, integrity, and availability of university data.

3. Scope & Audience

3.1. This policy applies to all university units, employees, students, visitors, contractors, and affiliates, and anyone who produces, manages, or accesses university data.

4. Definitions

4.1. **Data classification:** The function of categorizing data and information as Confidential, Sensitive, or Unrestricted in order to maximize the availability of information while restricting access to certain information, as appropriate.

4.2. **Data management:** The function of applying formal guidelines, procedures, and tools to store, access, and share the university's information.

4.3. **Data stewards:** Individuals responsible for assuring the accuracy and integrity of university data within their area of defined responsibility. Data stewards have regular access to data and are responsible for the management and security of information. Data stewards define processes for the collection and storage of data, recommend appropriate procedures related to institutional data, recommend levels of training, and assure adherence to records retention requirements.

4.4. **Data systems administrator:** Employees responsible for managing information systems, applications, or databases accessed by others, to conduct university business.

4.5. **Data Trustee:** The senior university executive with authority for all decisions regarding data usage for university business.

4.6. **Information security administrator:** Employee with the responsibility of specifying, implementing, and maintaining access controls to ensure that the integrity of data is maintained and that confidential data is protected.

4.7. **Information security incident:** Any real or suspected event that may adversely affect the security of university information or the systems that process, store, or transmit that information. Examples include but are not limited to unauthorized access to data, malware infections, network scanning by an outside entity, denial of service attacks, website defacement, and violations of a university security policy.

4.8. **Incident response:** A series of actions taken in the event of an information security incident. An incident response entails determining the extent of a breach, taking short- and long-term corrective actions, and reporting the details of the incident and the corrective actions to appropriate individuals.

4.9. **Third-party information technology services:** Non-university entities that have been contracted to perform specific information technology services for the university. Examples of third-party information technology services include, but are not limited to, Software as a Service ("SAAS"), Infrastructure as a Service ("IAAS"), or "Cloud" services.

4.10. **University data:** All information created, stored, sent, or received by university employees, students, and affiliates as part of their capacity as members of the university community. The terms “data” and “information” are used synonymously in this policy.

5. Responsibilities & Procedures

5.1. General Responsibilities

5.1.1. All users of institutional data are to:

a. Access data only in their conduct of university business, and in ways consistent with furthering the mission of the university;

b. Respect the confidentiality and privacy of individuals whose records they may access;

c. Observe any ethical restrictions that apply to the data to which they have access; and,

d. Abide by applicable laws, regulations, standards, and policies with respect to access, use, disclosure, retention, and/or disposal of information.

5.1.2. Users of institutional data may not:

a. Disclose data to others except as required by their job responsibilities;

b. Use data for their own or others’ personal gain or profit; or,

c. Access data to satisfy personal curiosity.

5.2. Data Management Roles and Responsibilities

5.2.1. The President of the university has ultimate oversight responsibility and authority over institutional provisions for data management, classification, and incident response.

5.2.2. The Provost is the Data Trustee for the university, and, as delegated by the President, has the authority for all decisions regarding data usage and classification for university business. The Provost approves information management and security policies proposed by the Vice Provost for Information Services (“VPIS”).

5.2.3. The VPIS is responsible for developing institutional policies and instituting programs to ensure the security, integrity, and availability of the university's information systems and assets. The VPIS reports to the Provost on such matters.

5.2.4. The Chief Information Security Officer ("CISO") serves as Director of the Office of Information Security and is responsible for:

a. Ensuring that institutional policies, procedures, and standards related to information security are implemented, maintained, and enforced;

b. Coordinating the institution's response to information security incidents;

c. Promoting training and awareness of the secure use of information, computing, and network resources; and,

d. Managing and assessing the information security operations of the institution.

5.2.5. The Data Governance Council, appointed by the Provost and advisory to the VPIS, reviews and recommends policy and procedure for managing the data of the university. Where information is shared amongst systems, the Data Governance Council will recommend processes to the VPIS.

5.2.6. The Information Technology Security Governance Council, appointed by the Provost and advisory to the VPIS, defines risk, recommends a framework and approach to mitigating that risk, advises on which risks to accept, avoid or manage more effectively, and assures security investments are balanced and well managed. The council reviews processes and protocols, recommends policy, and oversees the annual information technology audit.

5.2.7. Deans, Vice Presidents, Vice Provosts and Department Heads are responsible for:

a. Promoting understanding of and compliance with university data management, classification, and incident response policies within their units; and

b. Ensuring that adequate technical and procedural means and resources are in place to maintain the prescribed standards of care within their units.

5.2.8. Data systems administrators are responsible for ensuring that:

a. Any system containing university data is appropriately secured;

b. The appropriate use of information systems;

c. Permissions are managed appropriately to conform to university policy; and,

d. All legal and compliance requirements are met.

5.2.9. Data stewards are responsible for:

a. Ensuring, within their units, compliance with federal and state laws, rules, and regulations, university policies and procedures, and contractual obligations regarding the release of information to non-university entities;

b. Supporting the use of data to conduct university business;

c. Supporting appropriate practices for data use and data quality, and developing business processes that ensure the accuracy of data

d. Recommending and advising on the implementation of appropriate information access procedures;

e. Ensuring the accuracy of university data within their area of defined responsibility;

f. Defining processes for the collection and storage of data; and,

g. Recommending appropriate levels of training for access and use of information under their stewardship by relevant staff.

5.2.10. All members of the university community, including employees, students, and business partners, must:

a. Comply with university policies, procedures, and guidelines associated with information security;

b. Meet or exceed the minimum safeguards as required by university policy;

c. Comply with handling instructions for data as provided by university policy and procedures;

d. Report unauthorized data access, data misuse, or data quality issues to their supervisor, the appropriate data steward, or the Office of Information Security; and,

e. Complete training on the appropriate use and protection of university data, as required by the university.

5.3. Data Classification

5.3.1. Data classification establishes a framework to allow the university to comply with federal and state laws, regulations, and policies associated with information security, and to protect the confidentiality, integrity, and availability of university data. University data is classified into three categories: Confidential Information, Sensitive Information, and Unrestricted Information.

5.3.2. **Confidential Information**. Confidential Information is the most restrictive information classification. This classification pertains to information that could have serious negative consequences to the university or individuals if compromised or disclosed to those lacking appropriate approvals for access.

a. There are four types of data that fit within this classification:

   i. Information of a personal nature that could lead to identity theft or exposure of personal health information if not safeguarded;

   ii. Research data identified by a funding agency or other research partner as requiring restricted access for safety, security, privacy, proprietary, or other reasons;

   iii. Certain financial, legal, contractual, personal or other records or data that could compromise the privacy of individuals or university units;

   iv. Specific technical information about the mechanisms used to restrict access to, or otherwise secure, data within this classification.

b. Specific data elements classified as Confidential Information are listed at http://is.oregonstate.edu/ois/data-classification-data-element

c. Handling Confidential Information

   i. Access to Confidential Information is granted on a need-to-know basis only and requires prior approval from the Provost, as outlined at http://is.oregonstate.edu/policies/university-data-management-classification-and-incident-response

   ii. No confidential information may be transmitted over any network outside of the secured zones within the university network unless the full standards of care are met.

   iii. The use or storage of Confidential Information, either in paper or electronic form, must follow the Standards of Care for Confidential Information which can be found at http://is.oregonstate.edu/ois/baseline-standards-care

   iv. Unauthorized disclosure of Confidential Information must be reported to the CISO.

5.3.3. **Sensitive Information.** Sensitive Information is data that is commonly used to conduct university business, which by its nature or regulation, may have legal and/or generally expected obligations for non-disclosure outside of authorized individuals.

a. Specific data elements classified as Sensitive Information are listed at http://is.oregonstate.edu/ois/data-classification-data-element

b. Handling Sensitive Information

i. Access to Sensitive Information may be made available within the university but its use is limited to university business needs.

ii. The use or storage of Sensitive Information, either in paper or electronic form, must follow the Standards of Care for Sensitive Information found at http://is.oregonstate.edu/ois/baseline-standards-care

iii. Unauthorized disclosure of Sensitive Information must be reported to the CISO.

5.3.4. **Unrestricted Information**. Unrestricted Information is data intended for appropriate general use within the university.

a. Handling Unrestricted Information

i. In order to ensure the integrity of Unrestricted Information, the use or storage of that information must follow the Standards of Care for Unrestricted Information found at http://is.oregonstate.edu/ois/baseline-standards-care

5.4. Use of Third Party Services

5.4.1. Information provided by or gathered for the benefit of the university by third-party information technology services must comply with all requirements for data management and security. University units may establish more restrictive internal rules for use of information technology services.

5.4.2. Third-party information technology services are to follow the guidelines below for protecting data that has been classified as Confidential, Sensitive, or Unrestricted. The VPIS may conduct a risk assessment to determine whether the protection of existing services is adequate.

5.4.3. Individuals are to consider the guidelines in Section 5.3 when utilizing third-party services to manage or store data.

5.4.4. Confidential Information

a. Information classified as Confidential is generally restricted to university-owned and maintained systems. Third-party services may not be utilized to store or access confidential information unless the third party service has been reviewed and approved by the VPIS.

b. Individuals utilizing third-party services to store or access data classified as Confidential must:

i. Understand the policies associated with the use of the third party service;

ii. Limit access consistent with the restrictions established in university policy; and,

iii. Ensure that permissions to the data are accurately and appropriately managed.

c. If a third-party service does not meet the standards for storing confidential information, as determined by the VPIS, the VPIS will determine if the university can establish appropriate protections to use the service by modifying the information stored or business practices, or establishing other safeguards.

5.4.5. Sensitive Information

a. Information classified as Sensitive may be placed on a third party service if there is a legitimate business need to do so that cannot be accomplished using existing university services. Access to the data must be secured using the principle of least privilege necessary to meet the business need. The individual placing the data on a third party service is fully responsible for ensuring appropriate use, protection, and security of the data. Inappropriate controls may result in loss of data privileges.

b. Individuals managing data classified as Sensitive must:

i. Understand the policies associated with the use of that service;

ii. Limit access consistent with the restrictions established in university policy; and,

iii. Ensure that permissions to the data are accurately and appropriately managed.

c. If the third-party service does not meet the standards for storing sensitive information, as determined by the VPIS, the VPIS will determine if the university can establish appropriate protection to use the service by modifying the information stored or business practices, or establishing other safeguards.

5.4.6. Unrestricted Information

a. Information classified as Unrestricted may be stored on a third party service by employees in the course of conducting university business, whether or not a university contract is in place. Employees are responsible for ensuring that access is consistent with the restrictions established in policy, understanding the policies associated with the use of that service, and confirming permissions to the data are accurately and appropriately managed.

5.5. Data Security Incident Response

5.5.1. All security incidents involving Confidential and Sensitive Data must be immediately reported to the Office of Information Security. The CISO will lead the investigation into the incident.

5.5.2. Incidents involving information security are within the purview of the Office of Information Security. Incidents that also involve physical security, personnel action, student conduct, or other areas will be handled in accordance with established university protocols and procedures; however, the CISO will be informed of the incident to ensure that information security aspects of any incident are addressed.

5.5.3. More information on the university's Data Security Incident Response Process is available on the OIS website http://is.oregonstate.edu/ois.

5.6. Enforcement

5.6.1. Violations of this policy are grounds for disciplinary actions, in accordance with university policy, and may include but are not limited to:

a. Denial of access to university computing resources;

b. Disciplinary actions and/or criminal and civil penalties;

c. Termination of employment; and,

d. Referral to appropriate law enforcement agencies.

5.7. Exceptions

5.7.1. Exceptions to this policy must be approved by the VPIS.

6. Forms & Tools

6.1. None

7. Frequently Asked Questions

7.1. None

8. Related Information

8.1. Acceptable Use of Computing Resources
http://leadership.oregonstate.edu/sites/leadership.oregonstate.edu/files/08-005_acceptable_use_of_computing_resources.pdf

9. History

9.1. Last review date: June, 2017

9.2. Next scheduled review date: June, 2019

10. Website

10.1. http://leadership.oregonstate.edu/sites/leadership.oregonstate.edu/files/08-015_univ_data_mgmt_policy.pdf

11. Contacts

Department	Phone Number	Website
Office of Information Security	541-737-9800	http://is.oregonstate.edu/ois