ADMINISTRATIVE PROCEDURE

Information Governance: Roles & Responsibilities

Procedure Contents

- **Related Policy**
- **Procedure Context**
- **Procedure**
- **FAQ**
- **Related Information**
- **History**

Effective Date: 22 October 2012
Last Updated: 22 October 2012
Responsible University Officer:
VP Technology/CIO
Procedure Owner: J. Kelly Flanagan
(responsible for developing, implementing, &
managing the procedure)
Procedure Contact: Christine Tolman
(First point of contact for procedure users)

RELATED POLICIES: **Information Security and Appropriate Use**
Computer and Electronic Communications General Use
Access to Student Records

PROCEDURE CONTEXT

Information is a vital institutional resource whose value is enhanced when used appropriately and diminished when misused, misinterpreted, or when its access is unnecessarily restricted. While providing access to, and safeguarding university information is a shared university responsibility, this document describes the information governance roles and responsibilities required, from the more general and managerial, to the more specific and technical that facilitate secure and appropriate sharing of university information.

PROCEDURE

The university has established the following information governance roles--

Information Trustee – Broad, university-wide information oversight
Information Steward – Broad, unit-specific information oversight
Information Custodian – Technical, unit-specific information oversight
Information System Manager – Technical, unit-specific, hands-on information system manager
Information Request Coordinator – Technical, university-wide, information management expert
Information User – Authorized user of university information in conduct of university business

Those with information governance responsibilities are supported by a number of university entities or individuals: the Office of Information Technology, the Office of the General Counsel, the Information Security and Privacy Committee (ISPC), the Information Security Officer, and the Compliance and Audit Office.

RESPONSIBILITIES

Information Trustee (VP)

Information Trustees are senior university officials (VP level) with planning and policy-level responsibility for information governance. Within their functional areas, they also have management responsibility for defined collections of institutional information. Information trustees work with the Information Technology VP/CIO to ensure that the appropriate resources (staff, technical support, infrastructure, etc.) are available to support the information needs of the university. In addition, they serve on the University's Information Technology Policy and Planning Committee (ITPC).

Information Trustee responsibilities include

- Assigning and overseeing Information Stewards.
- Overseeing the establishment of information protection and access policies in their areas.
- Approving the classification of information as recommended by their Information Steward(s)
- Determining institutional interpretation of legal and regulatory requirements for information in their areas.
- Promoting appropriate information use and information quality.
- Overseeing the development and execution of information security breach response plans.

Information Steward

Information Stewards are university officials (assistant/associate vice president, dean, or director level) with direct operational-level responsibility for the management of institutional information in their area of responsibility as determined by the Information Trustee.

Information Steward responsibilities include

- Assigning and overseeing Information Custodians in their units.
- Authorizing Information System Managers.
- Interpreting and assuring compliance with federal, state, and university policies and regulations regarding the release of, responsible use of, and access to institutional information.
- Recommending the classification of information within their stewardship according to the university's information classification scheme.
- Reviewing and approving requests for access to university information.
- Ensuring that information quality and information definition standards are developed and implemented to promote complete, accurate, valid and timely information collection.
- Overseeing the development, implementation, and maintenance of a Business Continuity Plan for institutional information under their control.
- Approving their units' readiness and response plan for responding to security breaches consistent with the university's response plan.
- Participating with the University Information Trustee, other Information Stewards, Information Custodians, Information Security Officer, and legal representatives from the Office of the General Counsel, in the development of university information access policies and procedures.

Information Custodian

Information Custodians are managers with day-to-day responsibility for the management of institutional information in their organization.

Information Custodian responsibilities include

- Managing user access to information as prescribed and authorized by the appropriate Information Steward.
- Providing communication and training to users on how to access and appropriately use and protect institutional information.
- Classifying the information within their stewardship according to the university's information classification scheme.
- Retrieving security tokens and notifying OIT Information Security of all staff transfers, leaves, moves, and terminations.
- Developing, implementing, and communicating record retention requirements to the university community in conjunction with University Archives and the Office of the General Counsel.
- Assuring that the quality of university information within their stewardship meets the standards for its intended use.
- Developing their units' readiness and response plan for responding to security breaches consistent with the university's response plan.
- Monitoring information access based on university policy.

Information Request Coordinators

Information Request Coordinators are information management experts in the Office of Information Technology (OIT) assigned to facilitate the information request and approval process. Their responsibilities include

- Assisting with the clarification of information requests (the types and the means of delivery)
- Assuring that requests are directed to the appropriate information stewards
- Updating and maintaining the information governance repository

Information System Manager

Information System Managers are the computer system administrators (in university units or in OIT), authorized by an Information Steward, who operate and manage the systems and servers that collect, store, manage, and provide access to institutional information.

Information System Manager responsibilities include

- Maintaining physical and system security and safeguards appropriate to the classification level of the information in their custody.
- Complying with applicable university security standards.
- Maintaining Disaster Recovery plans and facilities appropriate to business needs and adequate to maintain or restart operations in the event systems or facilities are impaired, inaccessible, or destroyed.
- Providing information users access as prescribed and authorized by appropriate Information Stewards.

- Following information handling and protection policies and procedures established by the appropriate Information Stewards.
- Complying with all federal and state laws, federal regulations, and university policies applicable to the institutional information in their custody.

  NOTE: University units that develop databases and/or systems from institutional sources and then provide access to this information to other users are considered Information System Managers. These Information System Managers must be authorized by the appropriate information steward, approved to further redistribute institutional information, and must implement the minimum required safeguards for the source information as prescribed by the information steward.

Information User

Information User responsibilities include

- Complying with applicable federal and state laws, regulations, and university policies associated with the institutional information used.
- Using institutional information only as required for the conduct of university business within the scope of job duties.
- Implementing safeguards prescribed by the appropriate information steward for non-public information.
- Reporting any security violations, unauthorized access, information misuse, or information quality issues to the appropriate information steward for remediation.
- Discussing access needs with Supervisor, including changes that may be needed as a result of job responsibility changes or moving to a different unit.

Other Supporting Entities in Information Governance:

Office of the General Counsel

- Provides legal advice, including information classification advice, to Information Trustees, Information Stewards, Information Custodians and other university personnel regarding compliance with state and federal law.
- Participates in groups convened by the Information Technology Planning and Policy Council (ITPC) related to Information Governance policies or procedures.

Information Security and Privacy Committee (ISPC)

- Works under the direction of the Executive Risk Management and Compliance Committee ERMCC to establish university-wide information security policies, standards, and measures to protect information and systems.
- Provides information security policy advice and program support to the Information Trustees, Information Stewards, Information Custodians, Authorized University Officials and/or Supervisors, and Information Users.
- Recommends assurance standards and methods in support of information and information access processes.

Information Security Officer

- Provides staff support to the ISPC.

- Collaborates on and develops, publishes, and maintains university-wide information privacy and strategic security plans, procedures, and guidelines.
- Identifies security program elements and determines which units or offices must be involved in building a comprehensive security program.
- Assists campus organizations in responding to information security incidents, investigations, disciplinary actions, and legal matters by engaging appropriate personnel.
- Acts as the first arbiter for disputes, requests for exceptions, and complaints regarding university information systems security policies, practices, and related issues.
- In collaboration with the ISPC and campus colleges and units develops and executes a university Information Security Program.
- Assures that the approved information security assurance standards and methods are communicated to campus.
- Provides training and support concerning information security policy and procedures.

Office of Information Technology

- Establishes, develops, implements, and manages OIT's access processes, systems and procedures, in coordination with Information Custodians, Information System Managers, and other security and system administrators.
- Develops and executes technical security procedures for vulnerability assessments.
- Conducts technical assessments and forensics during security incident responses.

Compliance and Audit Office

- Audits compliance of information use
- Assists and advises units who are assessing their security and information use
- Assists with verification of units university information security standards status

FREQUENTLY ASKED QUESTIONS

There are no frequently asked questions for this procedure—yet.

RELATED INFORMATION

- ***Access to Student Records Policy***
- ***Access to Student Records Procedure***
- ***Computer and Electronic Communications General Use Policy***

HISTORY

Effective:
22 October 2012

Superseded:
XXXXXXX Procedure