Drake Information Technology Services

STEWARDSHIP AND CUSTODIANSHIP OF INSTITUTIONAL DATA

POLICY STATEMENT

Drake University's Information Security Policy requires controls to manage risks to the confidentiality, integrity, and availability of University information. This policy defines the roles and responsibilities of University employees who access and manage University data to protect the integrity, accuracy, validity, confidentiality, and privacy of data in aggregate or particulate.

REASON FOR POLICY

To preserve and promote accountability for the handling of University data.

ENTITIES AFFECTED BY THIS POLICY

- All units of the University

WHO SHOULD READ THIS POLICY

- Unit heads and administrators
- Individuals responsible for handling data that contains Personally Identifiable Information attributes or is owned by the University for use in its daily operations.

WEBSITE ADDRESS FOR THIS POLICY

Drake University Policy Library: *drake.edu/policy*

Drake Information Technology Services

STEWARDSHIP AND CUSTODIANSHIP OF INSTITUTIONAL DATA

TABLE OF CONTENTS

Drake Information Technology Services

STEWARDSHIP AND CUSTODIANSHIP OF INSTITUTIONAL DATA

I. RELATED DOCUMENTS, FORMS, AND TOOLS

- Records Retention Policy (University)

II. DEFINITIONS

Custodian: An individual with access to institutional information or who uses that information in the legitimate course of University business. (Ability to edit, input, alter, annotate, delete, etc.)

Local Information Security Analyst: An IT staff employee or security officer with specific responsibilities for protecting IT data and systems.

Local Support Providers: Drake employees who have responsibility for managing and maintaining information technology assets and who are employed outside of the Drake Information Technology Services.

Managers: Employees of the University who have management or supervisory responsibility for Production System information: Any system of software and hardware that delivers data for the operational needs of the University and which, if harmed, would negatively impact University operations or reputation.

Owners: The University is the owner of all institutional information with the exception of content authored by individuals who retain intellectual property rights.

Stewards: A University office/official with executive responsibility over certain institutional information and its daily administration and operations.

User: Anyone who consumes University information resources.

III. RESPONSIBILITIES

Drake Information Technology Services

- Maintains overview responsibility for implementation of this policy.
- Trains and educates the university community on this policy.
- Monitors technological developments, changes in the law, user behavior, and the market, and updates this policy, as appropriate.

Information Technology Security Advisory Board

- Reviews policy impact statements.
- Approves policies for review by the Faculty Senate and President's Council.

IV. PURPOSE

All members of the University community share in the responsibility for protecting information resources to or for which they have access or custodianship. Stewardship and custodianship of University administrative data will facilitate access to data that supports the work of those with official educational or administrative responsibilities within the institution, consistent with legal, ethical, and practical considerations. This policy defines four groups of people and their roles and responsibilities for protecting information resources. Individuals may have multiple roles and responsibilities.

V. PROCEDURES

1. OWNERS

The University is considered the information owner of all University information; individual units within the institution may have stewardship responsibilities for portions of the information.

2. STEWARDS

Stewards are those members of the University community who have the primary responsibility for particular information. Each type of *production system information* needs a steward. One becomes the steward either by designation or by virtue of having acquired, developed, or created information resources for which no other party has stewardship. For example, the campus librarians are the

NOTICE

While the University permits limited personal use of Drake-owned or controlled information technology resources, faculty and staff members (as well as student employees, graduate assistants, graduate research assistants, research assistants, and teaching assistants) do not acquire an absolute right of privacy in communications transmitted or stored on University computers.

stewards of the library catalogs and related records, and the members of the Office of the Provost and the deans of the University are the stewards of student data. For purposes of the Information Security Policies, faculty members are considered the stewards of their research and course materials; students are considered the stewards of their own work.

2.1 Establishing security policies and procedures.

Stewards may establish specific information security policies and procedures for their information where appropriate. Stewards are responsible for defining the procedures related to the creation, retention, distribution, and disposal of information over which they have stewardship. These should be consistent with the University Information Security Policies and the University's Records Retention Policy, as well as with other University policies, contractual agreements, and laws. Stewards may impose additional requirements that enhance security. They are also responsible for the following.

2.2 Assigning classification

Stewards are responsible for determining the classification of their information and any specific information handling requirements that go beyond the University Information Security Policies, particularly as may be imposed by confidentiality agreements with third parties. Confidential information or information for internal use only shall be marked as such when it is presented or distributed to users, especially when failing to do so could lead to a misunderstanding of the classification. Additional markings specifying handling and distribution requirements may be added.

2.3 Determining authorizations

Stewards determine who is authorized to have access to their information. They shall make sure that those with access have a need to know the information and know the security requirements for that information. Stewards have the responsibility to determine if and when a confidentiality agreement should be signed. Information may be disclosed only if disclosure is consistent with law, regulations, and internal University policies, including those

covering privacy. Except under unusual and specifically recognized circumstances, access shall be granted to individuals in such manner as to insure an auditable account of access.

2.4 Record Keeping

Stewards shall keep records documenting the creation, distribution, and disposal of confidential institutional information. This process is also recommended for other types of information.

2.5 Incident reporting

Stewards shall report suspected or known compromises of their information to their managers, the chief information technology officer, and/or a local information security analyst. Reported incidents will be treated as confidential unless there is a need to release specific information.

Stewards should designate a back-up person to act if they are absent or unavailable. Stewards may not delegate ownership responsibilities to third party organizations (such as outsourcing firms) or to any individual who is not a fulltime Drake University employee. When both the steward and the back-up steward are unavailable, pressing steward decisions may be made by the department head who ordinarily handles the information.

3. CUSTODIANS

Custodians are in physical or logical possession of information and/or information systems. Like stewards, custodians are specifically designated for different types of information. In many cases, a department head or a director in the Drake Information Technology Services will act as the custodian. If a custodian is not recognizable based on an existing information systems' operational requirements, then the chief information technology officer will designate a custodian. Custodians follow the instructions of stewards, operate systems on behalf of stewards, but also serve users authorized by stewards. Custodians should define the technical options, such as information criticality categories, and then allow stewards to select the appropriate option(s) for their information. Custodians also define information systems architectures and provide technical consulting assistance to stewards, so information systems can be

built and run to best meet business objectives. If requested, custodians additionally provide reports to stewards about information system operations, information security problems, and the like. Custodians are furthermore responsible for safeguarding the information in their possession, including implementing access control systems to prevent inappropriate disclosure, as well as developing, documenting, and testing information systems contingency plans.

4. MANAGERS

Managers are members of the University community who have management or supervisory responsibility, including deans, department chairs, directors, group leaders, supervisors, etc. Faculty who supervise teaching and research assistants are included. Managers have all the responsibilities of users and, where information resources originate, stewards. In addition, they share responsibility for information security with the people they manage and supervise. They also are responsible for the following:

4.1 Establishing security policies and procedures.

If managers decide to establish specific information security policies and procedures for the people they manage or supervise, these should be consistent with the University Information Security Policies, as well as with other University policies, contractual agreements, and laws.

4.2 Managing authorizations

Managers should make sure their subordinates have the access authorizations needed to perform their jobs. The authorizations themselves are acquired from the stewards of the information resources. Managers should make sure their subordinates' access is discontinued or appropriately terminated when their employment ends. Managers are responsible for administering and retaining confidentiality statements for their subordinates if confidentiality statements are required by the steward(s) of the information.

4.3 User training and awareness

Managers are expected to provide an environment that promotes security. They are also responsible for making sure their

subordinates have the training and tools reasonably needed to protect information.

4.4 Incident handling and reporting

Managers shall report suspected or known compromises of information resources, including contamination of resources by computer viruses, to their managers, the chief information technology officer, and/or local information security analyst. They are expected to cooperate with the investigation of follow-up and recovery from security incidents, including taking any disciplinary action deemed necessary by the appropriate University authorities. Reported incidents will be treated as confidential unless there is a need to release specific information.

5. USERS

Every University community member is an information resource user; users consume information and data. Users include students, faculty, staff, contractors, consultants, and temporary employees. Users are required to abide by all security requirements defined by stewards, implemented by custodians, and/or established by Drake Information Technology Services and cited in University policy. Users are required to familiarize themselves with, and act in accordance with, all Drake University information security requirements. Users are also required to participate in information security training and awareness efforts. Users should request access from their immediate manager, and report all suspicious activity and security problems.