Data Classification Policy
OCAD University

Title: *Information & Data Classification Policy*	
Category: *CATEGORY OF POLICY*	**Approval Date:** May 5, 2014
Effective Date : May 6, 2014	**Review Date:** TBD
Authority: Board of Governors	
Sponsor: *Alan Simms, VP, Finance & Administration*	
Contact: Vice-President, Finance & Administration: 416-977-6000.	
Previous Versions: Please contact the Office of the Vice-President, Finance & Administration, to view any of the following previous policy versions: ☐ none	

Purpose*:*

University information comes from many sources and has special needs for storage and security related to volume and sensitivity. Information or data generated or received during the course of day-to-day operations is University owned and is an institutional asset.

This policy serves the following purposes:

1) Provides a data classification plan for University information that can be referenced in other policies, guidelines, standards, and procedures relating to information.
2) Outlines the responsibilities that members of the University community have with respect to information security and data management.

Scope:

This policy applies to all OCAD University faculty and staff or any external entity operating under contract with the University and governs the access, use, storage and deletion of all institutional data.

All members of the University community have a responsibility to protect the confidentiality, integrity, and availability of data used, generated, accessed, modified, transmitted, stored or destroyed by the University.

Protecting University information requires compliance and alignment with laws, regulations, contractual requirements, security policies, procedures, standards and controls. These compliance objectives act as controls that help enhance the University's reputation and minimize risk.

Specific laws and regulations that govern University data include:

- *Freedom of Information and Protection of Privacy Act (FIPPA)*
- *PCI (Payment Card Industry) Compliance*
- *Bill C-42 Copyright Act and Bill-C-11 Copyright Modernization Act*
- *Broader Public Sector Accountability Act*

Institutional processes and guidelines, posted on the University website, addressing personal data and confidentiality include:

- *Records and Confidentiality*
- *Information & Privacy*
- *Notification of Disclosure of Personal Information to Statistics Canada*
- *Research Ethics Policy*

***Definitions**:*

The terms *"information"* and *"data"* are used interchangeably for the purposes of this policy.

Use of information means any access to, collection, storage, transmission, processing, or destruction of information.

Custody of information means the keeping, care, watch, preservation, or security of information for a legitimate University purpose.

Control of information means the power or authority to make a decision about the use or disclosure of information in University records

An *Information Security Breach* involves a circumvention of information security controls, the unauthorized use of information or the unintended exposure of information.

A Data Steward is a senior management level position, such as a Dean or budget unit head, which has been delegated responsibility, on behalf of the University, for the creation, maintenance, protection, and use of specific information. A budget unit head is a senior manager at the University, normally at or above the Director-level. The Data Steward role is defined by the job title or position responsible for specific data, as determined by the University, and is not specific to any unique individual.

A Data Custodian is an employee of the University, or an external entity operating under contract with the University, designated by the departmental Data Steward who serves as the functional person(s) responsible for enacting the maintenance, protection and use of specific information as per its classification.

A Data User is a member of the University who accesses information that is in the custody or control of the University. Data Users are individuals which have access and are in possession of information in order to perform assigned duties.

The *Chief Information Officer* is the institutional leader responsible for information technology and computer systems that support the University's goals.

Policy (body):

a. Data Classification Responsibilities

Each data asset has a single owner or Data Steward even if that data is in use by multiple departments. The data owner is usually the originating recipient or source of the data asset at the University.

Department unit or Faculty are responsible for implementing appropriate managerial, operational, physical, and technical controls for access to, use of, transmission of, and disposal of University data in compliance with this policy.

The use of University data, and the technology involved in its management, is controlled through data stewardship, which assigns functions and roles to key people who will be in charge of ensuring the execution of this policy.

Data stewardship provides the authority and ability for designated Data Stewards to make and execute decisions regarding specific data and its proper use. The data stewardship role deals with data security, quality, and sharing issues.

Data stewardship includes the ongoing promotion and monitoring of responsible control of sensitive data and information assets including:

- Asset responsibility/ownership
- Asset inventory
- Asset classification or re-classification
- Asset controls
- Non-compliance reporting

b. Roles

Roles and responsibilities assigned to University employees need to be defined and documented in alignment with this policy. Controls or safeguards for University employees to implement and comply with this policy may include the following:

- Signing of confidentiality agreements
- User awareness and training
- Succession planning
- Changes to access privileges
- Formalized disciplinary processes

During employment with the University employees with access to confidential or sensitive information will receive periodic reminders of their responsibilities and receive ongoing, updated security awareness training, to ensure their understanding of current threats and corresponding security procedures to mitigate such threats.

Should an employee's or user's relationship with the University change formalized processes to revise access privileges or secure data will be enacted as applicable to specific confidential or sensitive data.

c. Data Steward Responsibilities

A Data Steward is responsible for the following:

- Applying or re-assessing a security classification to information using the classification scheme defined in the Procedural Guidelines associated with this policy
- Determining the risk tolerance that affects information security
- Assigning operational responsibility for information to one or more Data Custodians
- Establishing and maintaining rules and procedures for the appropriate use and protection of information
- Ensuring that the use and protection of information is consistent with all applicable policies and regulations, including relevant legislation
- Maintaining awareness of relevant regulations and legislation the University is required to follow
- Understanding of Institutional policies or procedures the University has enacted to ensure compliance with regulations/legislation
- Self-auditing and reporting to assess the departmental level of compliance with institutional policies and legal requirements
- Plans to address auditing, whether internal or external, including grant audits
- As applicable, enacting the responsibilities of a Data Custodian

In the event a Data Steward is unavailable for an extended period, the responsibilities of Data Steward will be based on defined delegation of authority, as formalized in advance through consultation with Human Resources.

d. Data Custodian Responsibilities

A Data Custodian is responsible for the following:

- Enacting how the data in an asset is used and who can access the data based on defined permissions determined by the Data Steward
- Understanding the rules and procedures for the appropriate use and protection of information
- Understanding the flow of information in relevant operational processes, both manual and automated
- Implementing and maintaining physical and logical controls that enforce established rules and procedures
- Granting and revoking access to information, under the direction of the Data Steward
- Enabling the timely detection, reporting, and analysis of incidents where circumvention, or attempted circumvention, of controls takes place

- Reporting non-compliance with this policy to the Data Steward as well as monitoring of compliance
- Periodic audits and reporting to determine compliance with the policy
- Updating status and controls of data based on re-classification by the Data Steward

Data Custodians are responsible for the storage of information. Data Custodians must be aware of the information's classification and it is their responsibility to apply the appropriate measures and controls. Data Custodians do not grant access to information. Data Custodians follow current data classification schema and implement controls specified by the Data Steward. In the case of new data it is the responsibility of Data Custodians to request the Data Steward determine access if it is not already defined.

e. Data User Responsibilities

All Data Users are responsible for understanding the classification of the data they are working with and ensuring that these assets are handled with the appropriate level of care. Data Users must not share **confidential** and **internal** information without approval from the Data Steward.

A Data User is responsible for the following:

- Restricting the use of information to only the purposes specified by the Data Steward.
- Complying with rules and procedures in force regarding the use of information.
- Complying with controls implemented by the Data Custodian.

Any Data User, including Data Stewards and Custodians, who duplicates and stores information, or any subset of information, including paper copies, assumes the responsibilities of Data Custodian for that information.

f. Data Usage

Extenuating circumstances may necessitate exceptions to this policy or these procedures, including compelling circumstances affecting the health and/or safety of an individual. All exceptions must be documented and approved by the Data Steward, and where applicable, in consultation with the University's Legal Counsel.

All Data Users that access University data must do so only in conformance to this policy. Data Users must ensure that University data assets under their direction or control are properly labeled and safeguarded according to their sensitivity, proprietary nature, and criticality.

Access control mechanisms must also be specified, implemented and utilized to ensure that only authorized users can access data to which they have been granted explicit access rights. Unless designated otherwise by a Data Steward uniquely identified, authenticated and authorized University employees, including IT Services and Human Resources staff, serve as Data Custodians for all applicable University data.

g. Data Transmission

All users that access University data to enable its transmission must do so only in conformance with this policy. As specified in current Data Classification Schema, data transmitted must be encrypted or have had other confidentiality and/or integrity mechanisms applied. If a user is unsure of the appropriate precautions to take when transmitting data they must consult the Data Custodian.

New external or internal technology platforms or new approaches to managing and analyzing data, may require revisions to or application of new Data Classification procedures to adapt to new ways of handling and securing data transmission, whether inside or outside the University. This policy will be revised, updated or appended in accordance with any new approved method of Data Transmission. Any Data User who duplicates and stores information, or any subset of information, is expected to adhere to defined procedures based on Data Classification and assumes the responsibilities of Data Custodian for that information.

h. Data Storage

All users that are responsible for the secure storage of University data must do so only in conformance with this policy. Where necessary, data stored must be secured through encryption or through the use of other confidentiality and/or integrity mechanisms

Data that is personal to the operator of a system and stored, processed, or transmitted on a University IT resource as a result of incidental personal use is not considered University data. University data stored on non-University IT resources must still be verifiably protected according to the guidelines defined or appended to or referenced by this policy.

i. Minimum Security Standards

The Office of the Chief Information Officer is charged with the promotion of data security awareness within the University community and, working with Human Resources will coordinate and facilitate training on relevant security standards in support of this policy. The Chief Information Officer will receive and maintain reports of incidents, threats and malfunction that may have a security impact on the University's information systems, and will receive and maintain records of actions taken or policies and procedures developed in response to such reports and will coordinate the creation, maintenance, enforcement and design of relevant security standards in support of this policy.

Procedures:

In order to classify data, it is necessary that a Data Steward be identified for all data assets. The Data Steward of the data is responsible for classifying applicable data according to the classification schema appended to the Information and Data Classification Policy. Deans or budget unit heads are usually the designated Data Stewards of information assets within each of their units.

Data Classification consists of determining:

a) How the data in an asset is used, stored and destroyed

b) Who is authorized to access the data

Non-compliance:

All employees and contracted service providers are bound by this policy and are responsible for its strict enforcement. A breach of this policy could have severe consequences to the University, its ability to provide services, or maintain the integrity, confidentiality, or availability of services.

Intentional misuse resulting in a breach of any part of this policy will result in disciplinary action. Severe, deliberate or repeated breaches of the policy may be considered grounds for instant dismissal; or in the case of an OCAD University contracted service provider, termination of existing contracts and legal action.

APPENDIX A: PROCEDURAL GUIDELINES

1. Classification Guidelines (Data Classification Schema)

Data Stewards are responsible for determining the level of sensitivity based on the following categories.

CLASSSIFICATION	DEFINITION (EXAMPLE)	MINIMUM SAFEGUARDS RECOMMENDED			
		ACCESS RESTRICTIONS	TRANSMISSION	STORAGE	DISPOSAL
PUBLIC	Information deemed to be public by legislation or policy. Information in the public domain. Examples include annual reports, public announcements, the public telephone directory, and specific categories of employee information.	No restrictions on access.	No special handling required.	No special safeguards required.	Can be recycled.
INTERNAL	Information not approved for general circulation outside OCAD University or a University faculty or departments. Loss would inconvenience the organization or management; disclosure is unlikely to result in financial loss or serious damage to credibility. Examples include internal memos, minutes of meetings, internal project reports.	Access limited to employees and other authorized users.	Encryption recommended for public networks.	Stored within a controlled access system (e.g. password protected file or file system or locked file cabinet or office)	Shredded, erased.
CONFIDENTIAL	Information that is available only to authorized persons. Loss could seriously impede the organization's operations; disclosure could have a significant financial impact or cause damage to the organization's reputation. Disclosure could have legal repercussions. Examples include specific categories of employee records and all student personal information, student and employee recruitment records, unit budgets, and accounting information, legal suits, medical/health information, appeals, and grievances as well as clinical patient data and information protected by law.	Access limited to those with a demonstrated need to know.	Encryption mandatory for public networks. Encryption optional on internal networks. Not directly accessible from public networks. Hardcopies must use secure methods for external transportation. Consideration of travel restrictions for specific data.	Stored within a controlled access system (e.g. password protected file or file system or locked file cabinet). Additional controls implemented as necessary to comply with relevant legislation. For any portable medium such as USB or mobile devices Encryption is required	Shredded, degaussed (removal of magnetic information) or securely erased

INFORMATION & DATA CLASSIFICATION POLICY STATEMENT

In certain circumstances Federal or Provincial laws or University contracts with third parties may require that information be classified as **Confidential**.

All information handled by members of the University Community should be clearly identified as falling into one of the three categories in the Data Classification Schema; **Confidential, Internal** or **Public**. Where possible the classification should be included or embedded within the information itself.

The default classification for all data not classified by a Data Steward must be either **Internal** or **Confidential** until classified otherwise. The default classification will apply to new data being collected until classified otherwise.

If there is ambiguity as to what information is contained within the asset and a definitive classification of the information cannot be made, then the information asset must be classified as **Confidential** until such time that it can be definitively identified as a lower level of classification.

Once data is classified, appropriate handling controls will be applied by the Data Custodian based on the guidelines defined or appended to or referenced by the Information and Data Classification Policy. If an information asset that is classified as **Internal** or **Confidential** eventually becomes released to the public then it may be reasonable to declassify it to **Public**.

Compliance with this classification standard will not ensure that data will be properly secured. Assessment of information systems to determine what level of security is required to protect data will be applicable according to the guidelines defined or appended to or referenced by the Information and Data Classification Policy and will be updated as required.