Dublin City University

Data Classification Policy

Contents

Purpose

The purpose of this policy is to support the classification of data to allow for the protection of Dublin City University data, or data held by Dublin City University, in terms of confidentiality, integrity, and availability.

Scope

This policy cover all data captured, processed or stored by the Dublin City University University. It applies to all members of the Dublin City University community, including faculty, staff, and students and organisations or individuals handling data on behalf of DCU.

Terms

The following terms are used in this document.

Availability - The assurance that information and services are delivered when needed. Certain data must be available on demand or on a timely basis.

Confidentiality - The assurance that information is disclosed only to those systems or persons who are intended to receive the information. Areas in which confidentiality may be important include nonpublic student or staff information, records relating to health, or infrastructure specifications.

Data – Coded representation of quantities, objects and actions. The word "data" is often used interchangeably with the word "information" in common usage.

Data custodian – Individual or group responsible for classifying data and generating guidelines for its lifecycle management. Synonymous with "information custodian."

Impact – A combination of data confidentiality, integrity and availability. Whether a set of data is LOW, MEDIUM, HIGH, or of VERY HIGH impact will inform the data classification and whether or not the data set should be considered sensitive data.

Information – Data processed into a form that has meaning and value to the recipient to support an action or decision. "Information" is often used interchangeably with "data" in common usage.

Information custodian – Individual or group responsible for classifying data and generating guidelines for its lifecycle management. Synonymous with "data custodian."

Integrity - The assurance that information is not changed by accident or through a malicious or otherwise criminal act. As DCU's business depends upon the accuracy of data in databases, DCU must ensure that data is protected from improper change.

Responsibilities

1. All Information Owners are responsible for ensuring that this policy is adopted within their area of responsibility.

2. The classification of information will be the responsibility of the Information custodian.

3. Individual staff members are responsible for ensuring that sensitive information they produce is appropriately protected and marked with the appropriate classification.

Policy Requirements for Information Assets

All existing DCU information belongs to one of the classifications below. Unless otherwise classified, information should be treated as 'DCU Controlled'.

All new information assets categorised as confidential or higher should be categorised & labelled for handling according to information handling procedures defined by the Information Owner minimally based on the Data Handling Guidelines.

Controls must be implemented by the Information Owner according to the classification to which the information belongs.

Information is classified, and may be reclassified, by the Information Owner.

Note: All DCU records are subject to the Freedom of Information Acts. Categorising information does not exclude it from the provisions of Freedom of Information or Data Protection legislation.

Information Classification Guide

This guide provides a framework for classifying and protecting DCU's information resources. It outlines the security objectives in the left column and assesses the potential impact DCU should certain events occur which jeopardise the information and information systems needed by the university to accomplish its mission, protect its assets, fulfill its legal responsibilities, maintain its day-to-day functions, and protect individuals.

The three levels of potential impact on DCU or individuals should there be a breach of security (i.e., a loss of confidentiality, integrity, or availability) are as follows:

The *potential impact* is **LOW** if:
− The loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on DCU's operations, assets, or on individuals.

The *potential impact* is **MODERATE** if:
− The loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on DCU's operations, assets, or on individuals.

The potential impact is **HIGH** if
− The loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on DCU's operations, assets, or on individuals.

Public information, i.e. information that can be communicated without restrictions, and is intended for general public use, is not included in the framework below as this data will not cause harm to any individual, group, or to DCU if made public. Examples include: Standard guidelines and policies; Published University Strategy; Contact details; maps; Course catalogue, public web page, press releases, event details and advertisements.

In terms of classifying data, if for any one of the data element/combination of elements the potential impact in terms of unauthorised disclosure, unauthorised modification, or loss of data is identified as ‘High’, then the complete data set should be classified as ‘DCU Highly Restricted’.

For example, if in a single data store copies of invoices classified as ‘DCU Controlled’ occupies the same space as payroll information classified as ‘DCU Highly Restricted’, then the classification of ‘DCU Highly Restricted’ applies the data set.

POTENTIAL IMPACT			
Security Objective	**LOW**	**MODERATE**	**HIGH**
Confidentiality Preserving authorised restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.	The unauthorised disclosure of information could be expected to have a limited adverse effect on DCU's operations, assets, or on individuals.	The unauthorised disclosure of information could be expected to have a serious adverse effect on DCU's operations, assets, or on individuals.	The unauthorised disclosure of information could be expected to have a severe or catastrophic adverse effect on DCU's operations, assets, or on individuals. .
Integrity Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.	The unauthorised modification or destruction of information could be expected to have a limited adverse effect on DCU's operations, assets, or on individuals.	The unauthorised modification or destruction of information could be expected to have a serious adverse effect on DCU's operations, assets, or on individuals.	The unauthorised modification or destruction of information could be expected to have a severe or catastrophic adverse effect on DCU's operations, assets, or on individuals.
Availability Ensuring timely and reliable access to and use of information.	The disruption of access to or use of information or an information system could be expected to have a limited adverse effect on DCU's operations, assets, or on individuals.	The disruption of access to or use of information or an information system could be expected to have a serious adverse effect on DCU's operations, assets, or on individuals.	The disruption of access to or use of information or an information system could be expected to have a severe or catastrophic adverse effect on DCU's operations, assets, or on individuals.
Data Classification	**DCU Controlled** With this classification protection of information is at the discretion of the custodian and there is a low risk of embarrassment or reputational harm to DCU. *Examples*: Meeting minutes; unit working & draft documents	**DCU Restricted** DCU has a legal, regulatory or contractual obligation to protect the information with this classification. Disclosure or loss of availability or integrity could cause harm to the reputation of DCU, or may have short term financial impact on the university. *Examples*: Student or employee records; grades; employee performance reviews; personally identifiable information.	**DCU Highly Restricted** Protection of information is required by law or regulatory instrument. The information within this classification is subject to strictly limited distribution within and outside the University. Disclosure would cause exceptional or long term damage to the reputation of DCU, or risk to those whose information is disclosed, or may have serious or long term negative financial impact on the University. *Examples*: PPS numbers; Physical or mental health record relating to individuals; Critical research data.

A list of the applicable regulations and statutes is included in the DCU ICT Compliance Policy (www.dcu.ie/internal/staff/ISS/policies).

NOTE: Particular care should be exercised when using mobile devices, such as laptops, PDAs, USB keys and mobile phones to access/store confidential information. The size, and ease with which such devices can be transported, increases the potential risk of data disclosure/loss. Such a loss can potentially have a severe or catastrophic adverse effect on DCU's operations, assets, or on individuals.

For further advise please contact the ISS Service Desk: email: ISS.ServiceDesk@dcu.ie or Tel: (700) 5007.

Document Change Management

Dublin City University believes that it is important to keep this Data Classification Policy current in order to ensure that it addresses security issues accurately and is up-to-date with evolving business issues and technologies. This policy is a living document that will be reviewed annually and/or updated as needed.

The Director of Information Systems and Services (ISS) will draft necessary changes and have them reviewed and approved by the Executive Group of DCU as appropriate. The Director of ISS and the members of the ICT Security Implementation Group will communicate changes to the University communities. Anyone in the University can determine the need for a modification to the existing policy. Recommendations for changes to this policy should be communicated to the Director of ISS.