Ollscoil na Gaillimhe
University of Galway

Policies and Procedures

Code: **QA402**
Title: **Data Classification Policy**
Date: **25 November 2022**
Approval: **IT Security and Data Protection Committee**

1.0 Purpose

Classification of information/data at University of Galway in terms of confidentiality, integrity and availability for the purposes of data protection.

The correct classification of data is important to help ensure the prevention of leaks and minimizing the impact of such leaks if they do occur. As well as being good practice, it will also ensure the University remains compliant with the requirements of the Data Protection Acts 1988-2018 (as may be amended) and the European General Data Protection Regulations 2016 ("GDPR").

2.0 Scope

This policy covers all data or information held, in physical or electronic format, by the University including documents, spreadsheets and other paper and electronic data and should be applied by all staff, students and other members of the University.

This policy is also applicable to associated working with the University, agency staff, data processors, third parties and collaborators working with the University. They are responsible for assessing and classifying the information they work with and applying appropriate controls. Members of staff working with these types of associates and third parties have a responsibility to bring this guidance to their attention.

3.0 Description

This policy provides a framework for classifying and protecting University of Galway's information resources. The table overleaf outlines the security objectives in the left column and assesses the potential impact on University of Galway should certain events occur which jeopardise the information and information systems needed by the University to accomplish its mission, protect its assets, fulfil its legal responsibilities, maintain its day-to- day functions, and protect individuals. The four levels of potential impact on the University or individuals should there be a breach of security (i.e. a loss of confidentiality, integrity, or availability) are as follows:

PUBLIC	LOW (CONTROLLED)	MODERATE (RESTRICTED)	HIGH (HIGHLY RESTRICTED)
Public Data is information that can be communicated without restrictions and is intended for general public use. This data will not cause harm to any individual, group, or to the University if made public. Examples include: Standard guidelines and policies; Published University Strategy; Contact details; maps; course details, public web page, press releases, event details and advertisements. Public data is not included in the classifications below as this data will not cause harm to any individual group or to the University if made public.	The loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on the University's operations, assets, or on individuals. The loss of confidentiality, integrity, or availability has been minimized as the data has been pseudonymised.	The loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on the University's operations, assets, or on individuals.	The loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on University's operations, assets, or on individuals.

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 "University of Galway Highly Restricted". For example, if in a single data store copies of invoices classified as" University of Galway controlled" is stored along with payroll information classified as "University of Galway Highly Restricted", then the classification of, "University of Galway Highly Restricted" applies to the data set.

3.1. Definitions /Terms

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/counselling, 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 owner – Individual or group responsible for classifying data and generating guidelines for its lifecycle management. These are usually the officers responsible for the initial collection/input and use of the data. Synonymous with "information owner."
Impact – A combination of data confidentiality, integrity and availability. Whether a set of data is LOW, MODERATE, 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 owner – Individual or group responsible for classifying data and generating guidelines for its lifecycle management. Synonymous with "data owner"
Integrity - The assurance that information is not changed by accident or through a malicious or otherwise criminal act. As the University activities depend on the accuracy of data in databases, the University must ensure that data is protected from improper change.
Personal Data – Information relating to – (a) an identified living individual, or (b) a living individual who can be identified from the data, directly or indirectly, in particular by reference to – (i) an identifier such as a name, an identification number, location data or an online identifier, or (ii) one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the individual.

Special Categories of Personal Data – other than in Part 5 of the Data Protection Act 2018, means – (a) personal data revealing – (i) the racial or ethnic origin of the data subject (ii) the political opinions or the religious or philosophical beliefs

of the data subject, or (iii) whether the data subject is a member of a trade union (b) genetic data (c) biometric data for the purposes of uniquely identifying an individual (d) data concerning health, or (e) personal data concerning an individual's sex life or sexual orientation.

Pseudonymisation means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified natural person. The Data Protection Acts 1988-2018 (as may be amended) still apply to Personal Data which has been pseudonymised.

Table: Data Classification

Objective	LOW	MODERATE	HIGH
Confidentiality Preserving authorised restrictions on information access and disclosure, including means for protecting personal privacy (including Data Protection responsibilities)	The unauthorised disclosure of information could be expected to have a limited adverse effect on the University's operations, assets, or on individuals Personal or Special Categories of Personal Data.	The unauthorised disclosure of information could be expected to have a serious adverse effect on the University's operations, assets, or on individuals Personal or Special Categories of	The unauthorised disclosure of information could be expected to have a severe or catastrophic adverse effect on the University's operations, assets, or on individuals Personal or Special Categories of Personal Data.
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 the University's operations, assets, or on individuals Personal or Special Categories of Personal Data.	The unauthorised modification or destruction of information could be expected to have a serious adverse effect on the University's operations, assets, or on individuals Personal or	The unauthorised modification or destruction of information could be expected to have a severe or catastrophic adverse effect on the University's operations, assets, or on individuals Personal or Special Categories of Personal Data.
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 the University's operations, assets, or on individuals Personal or Special Categories of Personal Data.	The disruption of access to or use of information or an information system could be expected to have a serious adverse effect on the University's operations, assets, or on individuals Personal or Special Categories of Personal Data.	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 the University's operations, assets, or on individuals Personal or Special Categories of Personal Data.
Data Classification	**University of Galway Controlled** With this classification protection of information is at the discretion of the data owner and there is a low risk of embarrassment or reputational harm to the University. Examples: Meeting minutes; unit working & draft documents	**University of Galway Restricted** The University 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 the University or may have short term financial impact on the university. Examples: Student or employee records; grades; employee performance reviews; personal identifiable information.	**University of Galway 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 the University 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

4.0 Responsibilities

Name	Responsibility
Chief Operating Officer	Policy Owner
Data Owners	Classification of data and implementation of the controls appropriate to the classification
Data Handlers (Users)	Ensuring that sensitive information they produce is appropriately protected and marked with the appropriate classification
Internal Audit	Monitoring and reporting compliance with the policy
Data Protection Officer	Revisions to the policy

4.0 Related Documents

QA400 Data Protection Policy
QA401Data Handling Policy
QA442 Record Retention Policy
ISS Policies and Procedures available on ISS website