Policy
Information Security for Project Management

Document Filename	Information Security for Project Management.docx
Version	1.1
Information Classification	Open
Status	Approved
Date	19 October 2017
Policy Owner	Brian Fitzsimmons
Policy Contact	b.fitzsimmons@gcu.ac.uk

Document Approval and Version Control

Title		**Name of Approvers (s)**			**Date**
Information Security for Project Management		Glasgow Caledonian University Executive Board			19/10/2017
Revision	**Status**	**Author (s)**	**Reviewed By**	**Approved By**	**Issue Date**
1.0	Draft	Brian Fitzsimmons	Mark Johnston, Hazel Lauder, Information Management Forum		
1.0	Draft	Brian Fitzsimmons	Information Governance Committee		
1.1	Approved	Brian Fitzsimmons		Executive Board	19/10/2017

Contents

1 Document Overview

1.1 Purpose

The purpose of this policy is to define a series of controls that will ensure Information Security is incorporated into University project management methodology, regardless of type or owner of project.

1.2 Scope

This policy applies to all projects, staff, contracted third parties and any other person who has been authorised by the University to access its information, irrespective of registered work place location.

1.3 Definitions

University: Glasgow Caledonian University is a Scottish Registered Charity, No. C021474 with its registered office at Cowcaddens Road, Glasgow G4 0BA, Scotland, UK.

Staff: Staff are salaried members of the University or individuals contracted by or to the University to provide a service.

Student: A person pursuing any course of study at the University.

Visitor: A visitor is anyone, not a member of staff or student, requiring access to University services or premises.

User: A member of staff, student or visitor who has been authorised by the University to use University IT Facilities and to gain access to University networks and information systems.

Information: The result of processing, manipulating, or organising data. Examples including but not limited to, text, images, sounds, codes, computer programmes, software and databases.

Confidentiality: Property that information is not made available or disclosed to unauthorized individuals, entities, or processes.

Integrity: Property of accuracy and completeness.

Availability: Property of being accessible and usable upon demand by an authorized entity.

Information Security: The practise of preventing unauthorised access, use, disclosure, disruption, modification or destruction of information, regardless of format.

Privacy Impact Assessment: A process which assists the University in identifying and reducing the privacy risks of a project.

Risk Assessment: A systematic process of evaluating the potential risks that may be involved in a projected activity or undertaking.

1.4 Supporting Documents

Information Security Policy, Information Classification and Handling Policy,

2 Policy

It is University policy to ensure that information security is incorporated, as an explicit requirement, into the management life cycle of all University defined projects, irrespective of type, owner or management methodology employed.

It is University policy to ensure that all University information contained within the life cycle of the project is secured to protect against breaches of confidentiality, failures of integrity or interruptions to the availability and value of that information and to ensure appropriate legal, regulatory and contractual compliance.

It is University policy to ensure that all project documentation and communication (s) which contain classified, commercially sensitive and personal and personally sensitive information is classified, handled and labelled as detailed in the ***Information Classification and Handling Policy.***

Where a University defined project involves the use of personal information or any other activity which could have an impact on the privacy of individuals, a Privacy Impact Assessment must be carried out as detailed in the ***Project Privacy Impact Assessment document***.

Where a University defined project involves accessing and or storing University information a risk assessment must be carried out as detailed in the ***Project Information Security Risk Assessment document***.

3 Review

The Information Governance Committee is responsible for keeping this policy current. This policy will be reviewed annually or more frequently as required.

4 Breaches of Policy

A breach of University policies, rules or regulations is considered as an issue of potential misconduct, which will be dealt with as a disciplinary matter under the University’s Conduct & Capability policy. If there is anything in this policy that you do not understand, please discuss it with your line manager.

5 Information

If you have any questions regarding this policy please contact the University’s Information Security Team via the IT Service Desk.

6 Policy Awareness

All individual users of University IT Facilities and information systems must comply with the appropriate information security policies, regulations, code of conducts, guidelines and practises and procedures including any external accountability.

It is a condition of use of the IT Facilities that a user’s activity may be logged and or monitored and that information in their IT account, including but not limited to, files, images, documents, audio, videos, browsing history, communication history, may be accessed and processed with or without their consent as outlined in the ***Monitoring and Accessing Information policy***.

7 Guidance

For guidance and further information please go to

https://www.gcu.ac.uk/staff/it/itregulationspolicies/