Policy
Information Security

Document Approval and Version Control

Title	Name of Approvers	Date
Information Security Policy	Glasgow Caledonian University Executive Board	19/10/2017

Revision	Status	Author (s)	Reviewed By	Approved By	Issue Date
0.1	Draft	James Dunsmore	Valeria Webster		
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

Purpose of this policy is to outline a series of controls that will safeguard the University's information from security threats that could have an adverse effect on its operations or reputation, whilst fulfilling its duty of care towards the information that it has been entrusted with. This is achieved by preserving the confidentiality, integrity, availability and value of University information through the use of optimal controls.

1.2   Scope

This policy and other specific secondary information security policies issued to support it, will apply to all information processed, accessed, manipulated or stored by the University whether owned or managed and is applicable to all staff, students and visitors.

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.

Information System: Any information processing system procured by and licensed to the University for Use in any of its IT Facilities.

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.

Information Security Incident: Any event that has the potential to affect the preservation of the confidentiality, integrity, availability or value of University information, regardless of format.

1.4   Supporting Documents

Information Classification and Handling Policy, Information Security Incident Reporting and Management Process.

2   Policy

The University is committed to protecting the security of its information and information systems. It is also committed to a policy of education, training and awareness for information security and to ensuring the continued business of the University.

It is the University's policy that the information it manages shall be appropriately secured to protect it against unauthorised or unintended losses of confidentiality, failures of integrity or interruptions to the availability and value of that information and to ensure appropriate legal, regulatory and contractual compliance.

The Information Governance Committee will oversee information security within the University, formulate and disseminate information security policies, procedures and guidelines that, subject to Executive Board approval, all staff, students and visitors are required to comply with.

Information security is the responsibility of every member of staff, student and visitor. Access to University information shall be set at a level that allows the staff student or visitor to carry out their activities as stated in their role or contractual agreement.

Information security awareness training is available to and must be completed by, all members of staff.

To determine the appropriate level of control that should be applied to information, a risk-based approach will be utilised to ensure residual risk is aligned to the University's risk appetite.

Specialist advice on information security shall be made available throughout the University and advice can be sought via the University's Information Security Team.

Where an actual or suspected information security incident occurs or may occur, it must be reported promptly to the IT Service Desk for thorough investigation as defined in the ***Information security Incident Reporting and Management Process.*** Records of the number of information security incidents and their type must be kept and reported on a regular basis to the Information Governance Committee.

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/