
# Policy

# Information Security Incident Reporting and Management

| | |
|---|---|
| Document Filename | Information Security Incident Reporting and Management policy.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/Role | | Name of Approvers (s) | | | Date |
|---|---|---|---|---|---|
| Glasgow Caledonian University Executive Board | | | | | |
| **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 outline a structure for reporting and managing information security incidents. Efficient and effective management of information security incidents will be assisted by the provision of a clear and concise definition of what constitutes an Information Security incident.

## 1.2 Scope

This policy applies to all users of University information, irrespective of location and to all information held by or on behalf of the University, irrespective of 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 of 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.

**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 confidentiality, integrity availability or value of University information, regardless of format.

**Remote Location:** Any place of work other than the registered place of work.

**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.

**University IT Facilities:** All University owned or leased accommodation which houses computer hardware or software which in turn is owned, leased or licensed to and operated by the University. This includes;

- Computer hardware and software owned by, leased or licensed to the University and connected to the University network (s) by whatever means
- Computer hardware and software owned by, leased or licensed to the University and not connected to the University network (s)
- All networking, data processing and information and communications systems, including connections to external computers or networks including systems accessed through commercial or other arrangements

### 1.4 Supporting Documents

***Information Security Incident Reporting and Management Process.***

## 2 Policy

It is University policy to report all actual or suspected information security incidents immediately upon discovery. All such incidents must be reported to the IT Service Desk who will manage the incident in accordance with ***the Information Security Incident Reporting and Management Process***.

It is University policy for the Information Compliance and Information Security teams to assess each incident, determine the level of response, ensure the response is proportionate to the threat and inform external bodies or data subjects as required.

It is University policy to review all incidents for lessons learned and to identify improvements in policies and procedures.

The responsibility for reporting incidents lies with staff, students and visitors. That is any person who has access to University IT Facilities, University information and information systems.

## 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/