Information Security Incident Reporting and Management Process

What is this process about?
It provides users with information which can be used to report an actual or suspected information security incident.

Who is this process aimed at?
All users who have been authorised by the University to access, download or store University information.

Who can you contact if you require further information?

IT Service Desk on 0141 273 1234 or internal extension 1234 or https://myservice.gcu.ac.uk

Information Security Incident Reporting and Management Process

1 Purpose

The purpose of this process is to provide a series of steps which are used to report and manage all actual or suspected information security incidents which threaten the preservation of the confidentiality, integrity or availability of University information.

To further support the process all users of University information and information systems are required to understand their roles and responsibilities when an incident occurs.

2 Scope

This process applies to staff, students and visitors and any other person who has been given authority to access University information and information systems. The controls outlined in procedures A, B and C apply to all locations from which University information and information systems can be accessed from and to all information created, managed or received by the University in any format, stored in any system or device.

3 Objectives

The primary objectives of this process are to ensure the University;

- Responds to an incident following prompt and accurate reporting of that incident.
- Manages an incident allocating relevant resource and ensuring an appropriate and proportionate management response.
- Recovers from an incident through effective and timely management of that incident and ensure a lessons are learned to mitigate against future incidents.
- As required, ensure that appropriate authorities or regulators are informed in accordance with legislation and good practice.

4 Responsibilities

- All users that is members of staff, students or visitors who has been authorised by the University to use University IT Facilities and to gain access to University networks and information systems, are responsible for reporting an incident involving University information; All incidents must be reported immediately
- The Principal and Vice Chancellor has senior management accountability for information security and for providing a culture of information security
- Executive Deans, Directors, Heads of Department and other Line Managers have accountability for reporting, investigating and taking action following an incident within their relevant business areas
- The Director of Information Technology has accountability for reporting, investigating and ensuring that actions are taken to address incidents involving information technology systems and network security
- The information security team have responsibility for investigating and closing incidents

Reporting and Management Procedures

A Person Reporting: Incident Reporting Procedure

All actual or suspected information security incidents (incidents) must be reported immediately using the following procedure;

- Report incident to the IT Service Desk immediately via one of the following;
    - Internal extension x1234
    - External 0141 273 1234
    - ISTD@gcu.ac.uk
    - https://myservice.gcu.ac.uk
- Provide service desk with relevant information; includes name, job title and a description of the incident
- Follow and act upon any advice the service desk may give at the time of reporting
- Ensure you keep safe a copy of the call details and in particular the call number

In summary all incidents must be reported to the IT Service Desk. The service desk will offer first line support in an attempt to resolve the issue. As the person reporting the incident you will receive a copy of all information relayed to the service desk including ticket number.

B IT Service Desk: Incident management Procedure

On receiving a call reporting an actual or suspected information security incident the service desk will;

- Create a call and record all relevant details
- Offer first line support; if resolved, complete all relevant sections of the **Information Security Incident Management Form,** send copy to the Head of Section of the person reporting the incident and seek permission from Information Security Team to close call; if not resolved
- Assign call to Information Security Team
- Email individual members of the Information Security Team, at the time of reporting, alerting them to the incident
- Complete all relevant sections of the **Information Security Incident Management Form** and send copy to the Head of Section of the person reporting the incident
- Hand over to Information Security Team

In summary the service desk will create a call, attempt to close call using from to manage details. If second line support is required than service desk will forward call and from to Information Security Team to manage incident.

C Information Security Team: Incident Investigation Procedure

On receipt of a Vfire call and or email from the service desk alerting them to an actual, or suspected information security incident, the Information Security Team will begin an investigation into the incident.

The Information Security Manager or his nominee will assume the role of lead investigator. The lead investigator will be responsible for;

- Confirm that an incident has occurred; Immediately on receipt of a call or email from the service desk,
- Closing call, if no incident has occurred; if incident has occurred
- Identifying and assigning resources, as required
- Implementing measures which will enable proportionate response, containment and recovery
- Identifying actions to recover any losses, rectify the impact or limit risks
- Managing the Information Security Incident Reporting and Management Form
- Activating the escalation procedure
- Identify and log lessons learned in order to prevent future incidents

The lead investigator will be responsible for liaising with and reporting to the Head of Information Compliance in the event of an incident.

The Head of Information Compliance is responsible for confirming that a reportable information security incident has occurred and should be reported to the ICO. The University Secretary and Executive Board members will have senior accountability for reporting any reportable incidents to the ICO.

Information Security Policies: https://www.gcu.ac.uk/staff/it/itregulationspolicies/