

Information Security Incident Examples

What is this information about?

It provides examples of what constitutes an information security incident.

Who is this information 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>

An information security incident

Can be defined as any event that has the potential to affect the preservation of the confidentiality, integrity, availability or value of University information, regardless of format.

Examples of information security incidents include but are not limited to;

- Unauthorised or accidental disclosure of classified or sensitive information; e.g. email containing classified or sensitive information sent to incorrect recipients
- Theft or Loss of classified or sensitive information; e.g. hard copy of classified or sensitive information stolen from bag or left in cafe
- Unauthorised modification of classified or sensitive information; e.g. altering master copy of student or staff record
- Theft or loss of equipment that contains classified or sensitive information; e.g. laptop containing classified or sensitive information stolen from bag or left at conference
- Unauthorised access by first second or third party to University information systems; e.g. example virus, malware, denial of service attack
- Unauthorised access to areas containing IT equipment which stores classified or sensitive information; e.g. unauthorised entry into a data centre or network cabinet rooms

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