Security Incident Procedures

Security Incident definition

A security incident is defined as a suspected, actual, attempted, successful, accidental or malicious:-

- unauthorized access, use, disclosure, modification or destruction of information
- interference with an information technology operation
- violation of explicit or implied acceptable use policy.

Examples include, but are not limited to:-

- Workstation intrusion (e.g. Virus)
- Unauthorised access or use of systems or data
- Unauthorised changes to workstation or software
- Loss or theft of equipment (e.g. laptops, hard drives, USB drives etc) used to store private or potentially sensitive information.
- Compromised user account (e.g. password disclosures)

Report a security incident

Any suspected breach must be reported as soon as possible to the IT Helpdesk either via the widget, email (ITServices@cavc.ac.uk), or via phone (internal 1315, external 02920250315).

Consequences of breaches

Any confirmed breach of security will be dealt on a per incident basis dependant on the seriousness of the breach. Consequences of breaches are but is not limited to:-

- Formal warning
- Written warning
- Dismissal

Date approved:	**17 May 2013**	**Responsible Manager:**	**Director of IT and IS**
Approved by:	**Quality Standards Board**	**Executive Lead:** :	VP Finance and Resources
Review date:	**May 15**	**Accessible to Learners:** :	Yes