Information Security Incident Management Policy

InfoSec Incident Management and Consequence Management Policy

Brunel University London

An ISO/IEC 27001:2013: *Aligned Document - Implementing Cyber and Information Security Best Practice*

Internal Use Only

Mick Jenkins
Chief Information Security Officer

Document control

Superseded documents

Version history

Version	Date	Comments
0.1	21 Mar 2016	First draft
0.2	18 Nov 2016	Document split into Policy and Procedural documents
0.3	09 Dec 2016	Updates and corrections from Information Access Officer
0.4	13 Dec 2016	Correction to job Title Head of IT Infrastructure & Operations
1.0	06 Apr 2017	Approved by Exec
1.1	20 Nov 2018	Correction to Job Titles
1.1	17 Jun 2020	Annual Review

Outstanding issues and omissions

Issue control

Owner:	Chief Information Security Officer
Signature: MGJ	Date: 06 Apr 2017
Approver:	Chief Information Officer
Signature: PK	Date: 06 Apr 2017
Distribution:	

ISO 27001 - Conformance

This section indicates the University Conformance to ISO27001:2013.

University ISMS Control Number	SOA – Number A16 – Information security incident management
ISO 27001:2013 Conformance Control	Information Classification Objective A.16.1 - Management of information security incidents and improvements

1.0 Cyber & InfoSec Incident Management System

1.1 Introduction

This policy provides a framework for reporting and managing

- Information Security incidents affecting the University's informational assets and IT systems;
- Losses and breaches of information;
- Near-misses and information security concerns.

Please refer to BUL-GLOS-000 - SyOPs for the glossary of terms, acronyms and their definitions for the suite of BUL ISMS documentations.

1.2 Scope

This policy aims to support the prompt and consistent management of information security incidents in order to minimise any harm to individuals or the organisation.

To this end all users and managers of University information and IT systems need to:

- understand their roles in reporting and managing suspected incidents;
- report actual or suspected information security incidents promptly, following the procedure, BUL-PROC-16.2 Infosec Incident Management Procedure;

All Users (whether employees, contractors or temporary staff and third party users) and all owners of University information security assets or systems are required to be aware of and to follow this procedure.

Everyone has an important part to play in reporting and managing information security incidents in order to mitigate the consequences and reduce the risk of future breaches of security.

This Policy applies to all locations from which University information is accessed including off-campus use. As the University operates internationally through its locations abroad, the remit of the Policy shall include such locations and shall pay due regard to non UK legislation that might be applicable.

1.3 Objective

The University recognises the importance of, and is committed to, effective Cyber & Information security incident management in order to help protect the confidentiality and integrity of its information assets, availability of its information systems and services, safeguard the reputation of the University and fulfil its legal and regulatory obligations.

The University will ensure that:

- Incidents are detected and reported in a timely manner
- Incidents are properly investigated and handled efficiently and effectively
- Incidents are communicated appropriately and appropriate levels of University management are involved in the response
- The impact of incidents is minimised and action taken to prevent further damage
- Incidents are reviewed and subsequent improvements made to policies and procedures where required
- Evidence is gathered, recorded and maintained appropriately
- Incidents are recorded and documented
- External bodies and data subjects are informed as required

2.0 Cyber & Information Security Incident Management Policy

Information systems which are known to be (or suspected of being) compromised will be isolated from the University network until the incident has been investigated, resolved and risks sufficiently reduced.

- Guidance and procedures for the detection, assessment, communication, reporting and escalation of security vulnerabilities, events and incidents will be provided via the ISMS bulletins, training programs and the University Incident Management Plan (IMP) updates;

- Suspected Cyber & information security incidents and events must be reported via the appropriate management channels;

- Responsibilities for the reporting and escalation of security vulnerabilities, events and incidents are to be clearly defined and communicated to all relevant personnel;

- Security events and incidents should be assessed according to the event/incident classification scale provided via the BUL-PROC-16-02 Infosec Incident Management Procedure Appendix A: Classification of Information Security Events/ Incidents and, where necessary, escalated accordingly;

- A Cyber & Information security incident response team (or teams) comprising representatives from all relevant parts of the University, shall coordinate the management of and response to incidents which require escalation in accordance with the Cyber & Information Security element of the University Incident Management Plan (IMP);

- Incidents involving personal data will be reported to the Information Access Officer;

- All incidents will be reported to the CISO who is responsible for the management of the IMP and the capture of associated metrics and incidents which are reported each quarter to senior management. This includes all university incidents, emergencies, and occurrences which are captured on the security incident database for cascade to appropriate personnel;

- Details of the Cyber & Information Security Incident Response Plan will be made available via the overarching University IMP and cyber & information security bulletins;

- All information security incidents will be recorded by the Cyber Security department for analysis, data capture, and data reporting;

- Post incident reviews will be carried out in order to identify where improvements in policies, procedures and information security controls can be made;

- The types, volumes and impact of security incidents will be recorded and reviewed and summary reports will be used as input to the University's cyber & information security risk register which forms part of the ISMS;

- Specific incident reports will be reviewed by the Cyber & Information Security Steering Group who may advise on corrective action in the future;

- Cyber & Information security incident procedures will be communicated to all relevant personnel and tested periodically as part of the University IMP training programme;

- Technical support and guidance will be provided by the Computer Centre.

3.0 Implementation

This policy is implemented through the development, implementation, monitoring and review of the component parts of the Information Security Management Systems as set out in the Information Security Policy Framework.