Owner:	**Director of IT**
Version number:	2
Date of approval:	**March 2019**
Approved by:	**Information Security Steering Group**
Effective date:	March 2019
Date of last review:	**February 2019**
Due for review:	March 2021

Information Security Incident Management Policy

1. SCOPE AND PURPOSE

1.1 This policy is a sub-policy of the Information Security policy and applies to all staff employed by the University including individuals working on a voluntary, honorary, placement or casual basis or through an agency and any other authorised users that have access to information and information technology provided by or through Bournemouth University (BU).

1.2 This policy sets out BU's intent and commitment and its expectations of those listed above to preserve the confidentiality, integrity and availability of the information it holds on behalf of its students, staff and other stakeholders.

1.3 This policy also aims to ensure BU's regulatory compliance, operational resilience, reputation and ability to sustain revenue.

1.4 This policy covers the following topics:

a) Information Security Incident Management
b) Cybercrime Attacks
c) Forensics investigations

2. KEY RESPONSIBILITIES

2.1 The BU Board has delegated day-to-day responsibility for ensuring compliance with the policy to the Chief Information Officer.

2.2 Executive Deans of Faculties and Directors/Heads of Professional Services will be responsible for information security within their area of business and directly accountable to the Chief Information Officer (CIO) and BU Board for findings in non-compliance to this policy

2.3 Business and System owners, including academic staff, are responsible for implementing the administrative and technical controls which support and enforce this policy.

2.4 All those outlined in 1.1 are responsible for complying by adopting the process and procedures, which support this policy.

3. LINKS TO OTHER BU DOCUMENTS

3.1 In addition to this document and the supporting set of "strategic policy" documents which form the Information Security policy set, there are several BU policies which complement this policy, as follows:

- Data Protection Policy for Staff and BU Representatives
- BU Disciplinary Policy
- Information Security Policy
- BU Acceptable Use Policy
- BU Staff and Authorised Users Policy
- Threat and Vulnerability Management Policy
- Mobile Computing Policy
- Information Classification Policy

Policy

4. Information Security Incident Management Framework

4.1 A framework for the management of information security incidents is to be established.

4.2 The information security incident management capability will be supported by documented standards/procedures, which:

a) Define the roles and responsibilities of the information security incident management team

b) cover the involvement of relevant stakeholders

c) detail the types of information needed to assist information security incident management

d) specify the tools needed to assist information security incident management

e) require details about information security incidents to be collated and reviewed

4.3 The Information Security team will oversee Information Security incidents, and have:

a) defined roles and responsibilities

b) sufficient skills/experience in managing information security incidents

c) authority to make critical business decisions and escalate incidents

d) methods of involving internal and external stakeholders

4.4 Information required to help manage information security incidents should be easily accessible and include:

a) contact details for relevant parties
b) security related event logs
c) details about affected business processes operations and applications
d) technical details such as network diagrams and system configurations
e) Threat intelligence and the results of threat analysis

4.5 Information relevant to managing information security incidents will be made available to help staff follow the information security incident management process, and as a result make timely decisions.

4.6 Individuals responsible for managing information security incidents should be supported by tools to help complete each stage of the information security incident management process.

4.7 Details about information security incidents experienced will be recorded and maintained on a continuous basis, using a consistent approach.

4.8 Information about security incidents will be collated and reviewed regularly, to help:

a) determine patterns and trends of information security incidents
b) identify common factors that have influenced incidents (typically by performing a root cause analysis)
c) determine the effectiveness of controls
d) provide a comparison of internal and external incident information
e) improve future information risk assessments and security audits.

5. Information Security Incident Management Process

5.1 There will be a process for managing individual information security incidents, which includes:

a) identifying information security incidents
b) responding to information security incidents
c) recovering from information security incidents
d) following up information security incidents

5.2 Information security incidents will be:

a) reported to IT Service Desk

b) Recorded in a log, or equivalent

c) Categorized and classified.

d) kept confidential and secured appropriately

5.3 The response to information security incidents will include:

a) analysing available information, such as system, network and technical logs; and logs from relevant security products

b) handling necessary evidence

c) investigating the cause of information security incidents

d) collaborating with IT and operational subject matter experts

e) containing and eradicating the information security incident

5.4 Recovery from information security incidents will involve:

a) Rebuilding systems or networks to a previously known secure state when required

b) Restoring from information that has not been compromised by the information security incident

c) Closure of the information security incident

5.5 Following recovery from information security incidents:

a) reviews will be performed to identify the cause of the information security incident

b) assessments will be carried out to determine the business impact of the information security incident and review the recovery actions performed

c) forensic investigations will be performed, if required

d) existing security controls will be examined to determine their adequacy

e) corrective actions will be undertaken to minimize the risk of similar incidents occurring

f) details of the information security incident will be documented in a post incident report

6. Forensic Investigations

6.1 Internal investigations will follow the principles of the relevant BU HR Internal Investigation Procedure. Evidence should be collected:

a) with the intention of possible legal action

b) with respect for individuals' privacy and human rights

c) from IT sources relevant to the incident

d) from non-IT sources relevant to the incident

6.2 Evidence collected should include passwords and encryption keys needed to access password protected or encrypted areas of storage containing electronic evidence.

6.3 Electronic evidence should be collected in accordance with legal constraints by:

a) creating a list of possible privacy implications

b) identifying constraints in employment legislation

c) complying with legal conditions in which investigations are allowed, e.g. UK Regulation of Investigatory Powers Act 2000

6.4 The forensic investigation should be supported by recording important information about the investigation including:

a) Attributes of electronic evidence

b) a chronological sequence of events, including timestamps

c) investigative actions carried out by two or more elected and independent individuals

6.5 The sources of forensic information should be protected by:

a) restricting physical and logical access of target computer equipment to a limited number of authorised individuals

b) preventing individuals tampering with possible evidence

c) establishing controls to prevent 'housekeeping routines' such as deleting emails, deletion of documents and record archives which might contain electronic evidence

6.6 The integrity of evidence should be protected by:

a) demonstrating that appropriate evidence has been collected, preserved and that it has not been modified

b) analysing evidence in a controlled environment

c) having evidence reviewed by an impartial, independent expert to ensure that it meets legal requirements

d) ensuring that processes used to create and preserve evidence can be repeated by an independent external party

e) limiting information about an investigation to nominated individuals and ensuring it is kept confidential

6.7 Results from a forensic investigation should be reported to relevant internal parties and appropriate external parties

General

7. REFERENCES AND FURTHER INFORMATION

7.1 The Information Security policy and this sub policy are written in accordance with the Information Security Forum (ISF) Standards of Good Practice (SOGP).

7.2 Please refer to the Data Protection policy for further information.