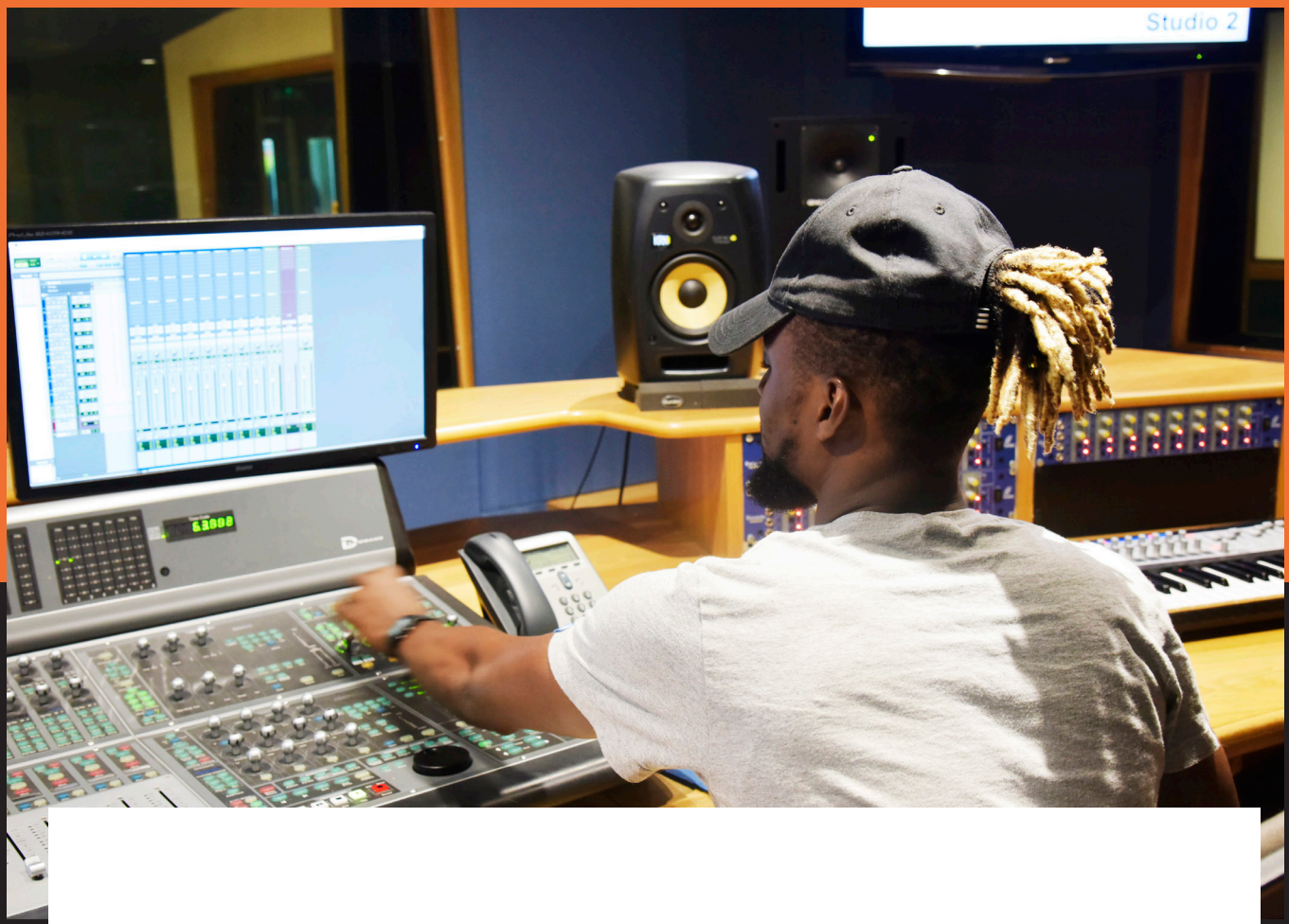
BUCKINGHAMSHIRE
NEW UNIVERSITY
EST. 1891



INFORMATION SECURITY INCIDENT MANAGEMENT POLICY

bucks.ac.uk

Contents

Approved by:	**ITSC**	Date first published:	**Jun-2016**
Version No.	**1.2**	Date updated:	**Jun-2018**
Owner:	**IS&T Directorate**	Review Date:	**Jun-2020**

This document has been designed to be accessible for readers. However, should you require the document in an alternative format please contact the Academic Quality Directorate.

Introduction

1. This policy is a constituent part of the Buckinghamshire New University Information Security Policy Framework which sets out a system of governance and accountability for information security management across the University.

2. Buckinghamshire New University relies on the effective management and flow of information to enable staff and students to communicate and work effectively on its business worldwide.

3. Safe use of the University's information and IT systems is essential to keep it working effectively. All users of University information have a responsibility to:

    - Minimise the risk of vital or confidential information being lost or falling into the hands of people who do not have the right to see it;
    - Protect the security and integrity of IT systems on which vital or confidential information is held and processed; and
    - Report suspected information security incidents promptly so that appropriate action can be taken to minimise harm.

4. The University takes information security very seriously. It is necessary to take prompt action in the event of any actual or suspected breaches of information security or confidentiality to avoid the risk of harm to individuals, damage to operational business and severe financial, legal and reputational costs to the organisation.

.

Purpose

5. This policy provides a framework for reporting and managing:

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

6. 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.

Objectives

7. 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.

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

    - Understand their roles in reporting and managing suspected incidents; and
    - Report actual or suspected information security incidents promptly, following the Information Security Incident Management Procedure.

9. The policy and its supporting procedures provide clear and consistent methodology to help to ensure that actual and suspected incidents and near misses are:

- Reported promptly and escalated to the right people who can take timely and appropriate action; and
- Recorded accurately and consistently to assist investigation and highlight any actions necessary to strengthen information security controls.

Scope

What is an information security incident?

10. An information security incident is any event that has the potential to affect the confidentiality, integrity or availability of University information in any format. Examples of information security incidents can include but are not limited to:

    - The disclosure of confidential information to unauthorised individuals;
    - Loss or theft of paper records, data or equipment such as tablets, laptops and smartphones on which data is stored;
    - Inappropriate access controls allowing unauthorised use of information;
    - Suspected breach of the acceptable use policy;
    - Attempts to gain unauthorised access to computer systems, e, g hacking;
    - Records altered or deleted without authorisation by the data "owner";
    - Virus or other security attack on IT equipment systems or networks;
    - "Blagging" offence where information is obtained by deception;
    - Breaches of physical security e.g. forcing of doors or windows into secure room or filing cabinet containing confidential information left unlocked in accessible area;
    - Leaving IT equipment unattended when logged-in to a user account without locking the screen to stop others accessing information; and
    - Covert or unauthorised recording of meetings and presentations.

This policy applies to

11. This policy applies to:

    - All information created or received by the University in any format, whether used in the workplace, stored on portable devices and media, transported from the workplace physically or electronically or accessed remotely.
    - All staff and students, affiliates or contractors working for or on behalf of the University and any other person permitted to have access to University information.
    - All University IT systems managed by the IS&T Directorate.
    - Any other IT systems on which University information is held or processed.

Who is Affected by the Policy

12. The policy applies to all users of University information. Users include all employees and students of the University, all contractors, suppliers, University partners and external researchers and visitors who may have access to University information.

Where the Policy Applies

13. The policy applies to all locations from which University information is accessed including home use.

Lines of Responsibility

14. All users who are given access to University information, IT and communications facilities are responsible for reporting any actual or potential breach of information security promptly in line with the incident management procedures.

15. The Head of IT Operations is the Lead Officer responsible for reporting, investigating and taking appropriate action to address breaches of physical security and suspected attempts to gain unauthorised access to secure areas, and for escalating incidents to the Information Security Officer.

16. The Head of Infrastructure and Systems, as Information Security Officer is the Lead Officer responsible for investigating and taking appropriate action in all cases involving loss, theft or unauthorised disclosure of University information and for liaising with the others in the management of other information security incidents.

Monitoring and Evaluation

17. The **Business Continuity and Security Forum (BuCS)** is responsible for reviewing the information security related policies and procedures that comprise the Information Security Management System (ISMS), monitoring compliance with the ISMS, reviewing incidents and recommending actions where necessary to strengthen information security controls. The Head of Infrastructure and Systems chairs the group. Where appropriate, the group will arrange training for lead officers responsible for investigating information security incidents.

18. The **University's Internal Auditors** will provide additional monitoring with both routine and ad hoc audits, as instructed.

Implementation

19. 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.

Related Policies, Procedures and Further References

University Policies and Procedures

20. This policy forms part of the University Information Security Policy Framework and its underpinning policies, procedures and guidance which are published on the IS&T Directorate's shared drive.

21. This policy should also be read in conjunction with the Information Security Incident Management Procedures which set out how to report and manage an actual or suspected breach of information or IT security.

Legal Requirements and External Standards

22. Use of information, IT and communications is subject to U.K. and Scottish law and other relevant law in all jurisdictions in which the University operates.

23. All current UK Legislation is published at http://www.legislation.gov.uk/. This policy and procedure are based on good practice guidance including:

    - BS ISO 27001 Information Security Management
    - The Information Commissioner's Office:

Definitions

Information

24. The definition of information includes, but is not confined to, paper and electronic documents and records, email, voicemail, still and moving images and sound recordings, the spoken word, data stored on computers or tapes, transmitted across networks, printed out or written on paper, carried on portable devices, sent by post, courier or fax, posted onto intranet or internet sites or communicated using social media.

Confidential Information

25. The definition of confidential information can be summarised as:

    - Any personal information that would cause damage or distress to individuals if disclosed without their consent; or
    - Any other Information that would prejudice an individual or organisation.

Information Security Management System

26. "That part of the overall management system based on a business risk approach to establish, implement operate, monitor review maintain and improve information security. The management system includes organisational structure, polices, planning activities, responsibilities, practices, procedures, processes and resources." BS ISO/IEC 27001: 2005: Information Security.