Owner:	Chief Information Officer
Version number:	**5**.0
Date of approval:	23 June 2023
Approved by:	ARG
Effective date:	24 June 2023
Date of last review:	May 2023
Due for review:	May 2024

BU Staff and Authorised Users Information Security Policy

1. SCOPE AND PURPOSE

1.1 This is the Bournemouth University (BU) Staff and Authorised Users Information Security Policy, which is approved at university board level. It is a sub-policy of the BU Information Security Policy.

1.2 This policy applies to all staff[1] employed by the University and authorised users[2] that have access to information and information technology provided by or through Bournemouth University (BU).

1.3 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.

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

1.5 This policy covers the following topics:

a) BU's expectations of those outlined in 1.2
b) information security awareness programmes
c) information security awareness communications
d) information security education/training
e) information owner's roles & responsibilities

2. KEY RESPONSIBILITIES

2.1 The BU Board has delegated day-to-day responsibility for compliance with the policy to the Chief Information Officer (currently the Chief Operating Officer).

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

[1] This includes individuals working on a voluntary, honorary, placement or casual basis (PTHP), visiting faculty, emeritus, contractors, board members, visitors or those employed through an agency.
[2] This includes all registered students (UG, PG, full and part-time and apprentices) and alumni

2.3 Information 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 1.2 are responsible for compliance by following the policies, procedures and standards which support this policy.

3. LINKS TO OTHER BU DOCUMENTS

In addition to this document and the supporting set of standards, there are several BU policies which complement this policy, as follows:

- BU Security Policy
- Acceptable Use Policy
- Data Protection Policy
- Disclosure of Information on Employees
- Guidance Note on Disclosure of Student Personal Data to Third Parties
- Intellectual Property Policy and Procedures
- PCI DSS Information Security Policy
- BU Staff Disciplinary Procedure
- Staff Handbook
- Student Policies, Procedures and Regulations
- Social Media Policy and Procedures – STAFF
- Social Media Policy and Procedures - STUDENT

POLICY

4. Human Resource Security – Employment Lifecycle

Expectations of those outlined in 1.2 who have been agreed or had approved access to BU Information (excluding students).

4.1 Information security responsibilities and qualifications, for those outlined in 1.2, will be specified in the documentation which specifies their relationship (e.g., job description).

4.2 Those outlined in 1.2 will be required to comply with the set of information security policies as defined within the Information Security Policy.

4.3 Upon termination of employment, those outlined in 1.2 will be required to return assets (or equivalent) that belong to BU, including:

a) important documentation (e.g., about business processes, technical procedures, and key contact details) stored on portable storage media or in paper form
b) equipment (e.g., mobile devices, laptops, tablets, smartphones, portable storage devices and specialist equipment)
c) software (including media, documentation, and licensing information)
d) authentication hardware (e.g., physical tokens, smartcards, and biometric equipment).

4.4 Upon termination of the relationship, those outlined in 1.2 will be required to confirm (in writing) that they have returned or destroyed all copies of information owned by the university that was within their control.

4.5 A method will be established and implemented to

- enable those outlined in 1.2 to confirm their acceptance or and compliance with the Information Security policy and supporting policies when they are issued and updated (e.g., displaying a confirmation dialogue box as part of the login process for computers or network access, when starting business applications and upon accessing the BU intranets / portals).
- assess compliance with the information security policy and supporting policies on a regular basis (e.g., in the form of audits).

5. Information Security Awareness

5.1 An information security awareness programme will be established for all those outlined in 1.2 to promote information security awareness throughout BU and establish a positive information security culture. The effectiveness of the information security awareness programme will be monitored and evaluated, and attendance will be compulsory for all those outlined in 1.2.

5.2 Objectives for the information security awareness programme will be

a) raising awareness of information risk and information security across BU
b) minimising information risk and reducing the frequency and magnitude of information security incidents across BU
c) embedding positive information security behaviour of individuals across BU
d) empowering those outlined in 1.2 to make effective risk-based decisions (e.g., having a ‘stop and think’ attitude when confronted with an unfamiliar or complex business situation, identifying risks, and weighing them before acting).

5.3 As part of their participation in the information security awareness programme, all those outlined in 1.2 will:

a) be updated regularly with information security messages using a broad range of communication methods (e.g., email, instant messaging, text messages, e-book readers, media players and intranets)
b) confirm they have read and understood the Acceptable Use Policy (and other related policies).

6. Information Security Awareness Communications

6.1 Those outlined in 1.2 who have access to information and information systems will be made aware of:

a) the meaning of information security (i.e., the protection of the confidentiality, integrity, and availability of information)
b) why information security is needed to protect information and systems
c) the common types of threat BU faces (e.g., identity theft, malware, hacking, information leakage and insider threat)
d) the importance of complying with information security policies and applying associated standards/procedures
e) their personal responsibilities for information security (e.g., protecting privacy related information and reporting actual and suspected information security incidents).

6.2 Information security awareness messages will cover details about information and related threats, including the:

a) definition of the information lifecycle and the risks of handling the different formats of information at different stages of its lifecycle
b) difference between critical information, which needs to be available and have integrity, and sensitive information, which can only be disclosed to authorised individuals
c) threats associated with users, the technology they use and the physical location(s) of the local environment.

6.3 Information security awareness messages will cover details about required activity, including the

a) actions and behaviour expected of those outlined in 1.2 to help address known threats (including rules on the use of blogging and social networking websites and being aware of social engineering attacks)
b) steps to be taken to address information security control weaknesses
c) information security arrangements requiring proactive steps by those outlined in 1.2, such as when handling information beyond the control of BU (e.g., when working at home or travelling, and using the telephone and voice messaging services)
d) need to comply with information security procedures such as those for 'clear desk' initiatives and logging off or locking systems when leaving a computing device unattended
e) methods of restricting physical access to BU's facilities (e.g., verifying the identities of strangers or third-party persons requesting physical access, and requiring them to follow documented access management procedures)
f) need to consult others for advice and guidance if there are questions about expected behaviours.

6.4 Those outlined in 1.2 who have access to and use electronic communication technologies will be made aware:

a) of expected behaviours (e.g., only attaching files to emails when necessary, avoiding the sharing of email threads, or posting sensitive information in blogs and web posts)
b) of the security features provided with electronic communications
c) that the content of messages may be legally and contractually binding
d) those electronic communications may be monitored and intercepted subject to other internal controls

6.5 Those outlined in 1.2 who have access to information and information systems will be made aware of the dangers and safety of:

a) being overheard when discussing university information over the telephone or in public places
b) including sensitive information in voice messages on landline and mobile voicemail messaging systems.

7. Information Security Education / Training

7.1 Information Security education/training will be given to provide those outlined in 1.2 with the knowledge and skills they need to conform with the Information Security policy and its supporting documents.

7.2 Information Security education/training will be given to provide those outlined in 1.2 with the skills they need to correctly use:

a) business applications (including enterprise software, commercial-off the-shelf software (COTS) and desktop applications (e.g., those developed using spreadsheets))
b) computer equipment (including desktop computers, laptops, tablets, and smartphones)
c) specialist equipment (e.g., scanning devices, bar code readers, data capture appliances and monitoring equipment
d) portable storage media (e.g., CDs, DVDs, magnetic tapes, hard disks, and portable storage devices)
e) networking technologies such as local area networks (LANs), wireless local area networks (WLANs), Voice over IP (VoIP), Internet and Bluetooth
f) telephony and conferencing equipment, including teleconference and videoconference facilities (e.g., speakers, cameras, and display screens) and online web-based collaboration
g) office equipment, including printers and photocopiers, facsimile machines and scanners and multifunction devices (MFDs)
h) access control mechanisms (e.g., passwords, tokens and biometrics).

7.3 Information Security education/training given to those outlined in 1.2 will include guidance on how to protect information, and cover:
a) creating and protecting electronic files
b) classifying and labelling information
c) deleting unwanted information once no longer required
d) separating university and personal information.

7.4 Information Security education/training will be given to provide those outlined in 1.2 with the knowledge and skills they need to apply information security controls associated with protecting:
a) business applications (e.g., using templates instead of existing documents to create new electronic documents or using validation routines when developing spreadsheet-based applications)
b) equipment (e.g., using file-based encryption to protect electronic files stored on mobile devices, portable storage media and in transit, and password-protecting consumer devices)
c) access control mechanisms (e.g., by physically removing smartcards from readers when leaving computers unattended)
d) connectivity (e.g., disabling communication settings, encrypting wireless networks, and using a virtual private network (VPN) when connecting to the corporate network)
e) locations in which they work (e.g., locking paper documents away overnight and logging off or locking desktop computers and laptops when unattended).

7.5 Information Security education/training will be given to provide those IT and systems development staff outlined in 1.2 with the knowledge and skills they need to design systems and develop security controls in a disciplined manner using best practice standards.

8. Roles and Responsibilities of Information Owners

8.1 Ownership of critical and sensitive information, business applications, information systems and networks will be assigned to those outlined in 1.2 and the responsibilities of owners documented. The Information Asset register will identify the ownership.

8.2 Responsibilities of owners will include:

a) understanding and identifying information risks
b) determining university (including information security) requirements and signing them off
c) ensuring information, business applications, information systems and networks are protected in line with their importance to the university
d) defining information interchange agreements (or equivalent) for sharing with third parties
e) authorising new or significantly changed university applications, information systems and networks
f) contributing to security audits.

8.3 A process will be established for:

a) providing owners with the necessary skills, tools, staff and authority to fulfil their responsibilities
b) assigning responsibilities for protecting information, business applications, information systems and networks when owners are unavailable
c) reassigning ownership when owners leave or change roles.

8.4 Those outlined in 1.2 involved in implementing and maintaining business applications, information systems and networks will be:

a) assigned clear responsibilities
b) able to administer and use them correctly and deal with normal processing requirements
c) competent to deal with error, exception, and emergency conditions
d) aware of information security principles and associated good practice.

8.5 The university will support Information Owners in the following areas:

a) administering users (e.g., adding new university users, updating access privileges, and revoking user access privileges)
b) monitoring key security-related events (e.g., system crashes, unsuccessful login attempts of authorised users, and unsuccessful changes to access privileges
c) validating processes/data
d) reviewing error/exception reports
e) identifying potential security weaknesses/breaches.

GENERAL

9. REFERENCES AND FURTHER INFORMATION

9.1 The Information Security Policy, sub policies and standards are written in accordance with the Information Security Forum (ISF) Standards of Good Practice (SOGP).

9.2 This Policy is reviewed and updated annually, and following any significant change, by the Information Governance Committee.