Owner:	Chief Information Officer (CIO)
Version number:	2.0
Date of approval:	**21 June 2019**
Approved by:	**University Board**
Effective date:	21st June 2019
Date of last review:	**21st June 2019**
Due for review:	21st June 2021

Information Security Policy

1. SCOPE AND PURPOSE

1.1 This is the Bournemouth University (BU) Information Security Policy, which is approved at university board level.

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 provides a high level framework for the management of information security, information assurance and information risk management throughout the university.

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

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

2. KEY RESPONSIBILITIES

2.1 The BU Board has delegated day-to-day responsibility for 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

[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 alumni

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 users are responsible for complying by adopting the process and procedures which support this policy.

3. LINKS TO OTHER BU DOCUMENTS

3.1 This Information Security Policy is the top-level document which references a set of policy sub-documents all of which have equal standing, which state official university policy in various information security areas. These policy sub-documents will be referred to as strategic policy documents.

3.2 In addition to the set of strategic policy documents which are referred to in section 5 there are several BU documents which complement this policy, as follows:

- Data Protection Policy
- Data Breach Management Plan

4. Policy

4.1 The university is committed to implementing ISO 27000 security controls that conform to best practice, as set out in the *ISF The Standard of Good Practice for Information Security*. Section 5 of this policy outlines a framework to protect BU based on best practice and is therefore endorsed and enforced by this governing policy.

4.2 The Information Security policy and its set of strategic policies must be supported by documented standards/procedures.

4.3 All members of the university and users of its systems will be advised of the Information Security policy and its content and will be expected to comply as per the BU Staff and Authorised Users Information Security Policy. (see Section 5)

4.4 Agreements with third parties involving accessing, processing, communicating or managing the university's information, or information systems, should cover all relevant security requirements, and be covered in contractual arrangements. Referencing and ensuring third parties are aware of this policy and the BU Acceptable Use policy is mandatory. Further statements can be found in the Third Party Access policy, the External Supplier Management policy and the Asset Management policy. (see Section 5)

4.5 Information systems within the university should be classified in a way that indicates their importance to the organisation and appropriate owners appointed for all critical and sensitive information, and information systems.

4.6 Security risk assessments will be carried out on all information systems on a regular basis or before a major change in order to identify potential risks to the system and its information and determine the controls needed to manage those risks. The risk assessment will be carried out in the first instance by the relevant business and system owners.

4.7 The university will establish and maintain appropriate contacts with both internal and external agencies in respect of its information security policy to maintain its relevance, e.g. business partners, law enforcement authorities, regulatory bodies, network and telecommunications operators.

4.8 Any breaches of this policy will be reported to the policy owner, who will take appropriate action.

5. INFORMATION SECURITY FRAMEWORK

5.1 This section provides a brief overview of the policy sub-documents. These "strategic policy" documents each have equal importance and state the official university policy in various Information Security related areas.

5.2 Each strategic policy document only contains high-level descriptions of expectations and principles: they are deliberately free from practical details of policy implementation and regulations.

5.3 Acceptable Use Policy

5.3.1 The Acceptable Use Policy (AUP) is an enhancement to this policy. It defines BU's rules on how an individual can use technology, including software, computer equipment and network connectivity provided by the university.

5.4 BU Staff and Authorised Users Information Security Policy

5.4.1 The purpose of this policy is to create a security-positive environment where individuals are accountable for protecting information and individuals are provided with the knowledge and skills required to apply security controls effectively.

5.4.2 These principles assign ownership and responsibility for particular information and systems to designated individuals and establish an information security awareness programme, which is supported by a range of education/training activities.

5.5 Information Classification Policy

5.5.1 This policy sets out to ensure information and systems are protected in accordance with information security and compliance requirements.

These principles establish an information classification scheme and a method for protecting assets and information in physical and electronic formats.

5.6 Business Applications Policy

5.6.1 The purpose of this policy is to ensure business applications incorporate consistent security functionality to protect information during creation, processing, transmission, storage and destruction

5.6.2 These principles apply sound information security architecture principles to business applications (including internal and external web-based applications) and protect information used by business applications throughout its lifecycle.

5.7 Third Party Access Policy

5.7.1 This policy ensures third parties are legally and contractually bound to protect sensitive or critical information relating to either the organisation or the customer.

These principles protect business applications with third party access by performing information risk assessments to determine security requirements, and by applying security arrangements supported by agreed, approved contracts.

5.8 Access Management Policy

5.8.1 This policy ensures that only authorised users can gain access to business applications, systems, computing devices and networks, and that individual accountability is assured.

5.8.2 These principles establish methods of restricting access to business applications, systems, computing devices and networks by requiring users to be authorised before being granted access privileges, authenticated using access control mechanisms and subject to a rigorous sign-on process before being provided with access.

5.9 Systems Management Policy

5.9.1 This policy sets out to ensure information systems and supporting technical infrastructure meet business and security requirements, function as required and are maintained in a managed and secure manner.

These principles ensure BU design, configure and deploy information systems in a consistent and accurate manner, and maintain supporting technical infrastructure using a rigorous change management process.

5.10 Technical Security Infrastructure Policy

5.10.1 This policy supports a consistent approach organisation-wide to selecting, building and deploying technical security infrastructure components and ensure they support business activities.

5.10.2 These principles establish a sound technical security infrastructure based on an enterprise-wide security architecture, which addresses the protection of information and critical infrastructure using identity and access management, cryptographic solutions and information leakage protection.

5.11 Network Management Policy

5.11.1 This policy ensures business information transmitted over all types of network is protected against unauthorized disclosure, interception, interference and interruption.

These principles ensure BU design, implement and manage physical, wireless and voice networks to be resilient, prevent unauthorized access and support current and future business activities in a secure manner.

5.12 Threat and Vulnerability Management Policy

5.12.1 This policy establishes an approach to reduce levels of vulnerability, protect information against threats, highlight system and network errors, detect potential and actual attacks and support investigations.

5.12.2 These principles will ensure BU manage threats and vulnerabilities associated with information, systems and networks by maintaining up-to date patch levels, deploy comprehensive, up-to-date malware protection and perform continuous monitoring.

5.13 Security Incident Management Policy

5.13.1 To resolve information security incidents of all types in a consistent, effective manner, minimize their business impact and reduce the risk of similar incidents occurring.

5.13.2 These principles will allow BU to implement a comprehensive and approved incident management process for information and systems that includes the identification, response, recovery and post implementation review of information security incidents.

5.14 Local Operations Security Policy

5.14.1 This policy ensures that information risks throughout BU are identified and understood, and security activities within local operations are carried out in a timely and accurate manner.

5.14.2 These principles will help co-ordinate information security activities in individual operational areas by addressing the risks associated with business users, information, technology and locations.

5.15 Desktop Applications Policy

5.15.1 This policy ensures that desktop applications are created in a secure manner, the information they process is protected, and an accurate record of each desktop application is maintained.

5.15.2 These principles will establish a methodology for developing and maintaining desktop applications, which includes methods for protecting them and recording them in an inventory.

5.16 Mobile Computing Policy

5.16.1 This policy ensures that information processed, stored and transmitted by mobile devices, is protected against the full range of threats.

5.16.2 These principles establish how BU will configure mobile devices, including the use of portable storage devices, to function as required and protect information during all stages of the information lifecycle.

5.17 Electronic Communications Policy

5.17.1 This policy preserves the integrity of important business messages, prevent unauthorised disclosure of sensitive information handled by electronic communication systems and maximise availability.

5.17.2 These principles protect electronic communication systems (e.g. email, instant messaging and VoIP) by setting policy for their use, configuring security settings, performing capacity planning and hardening the supporting technical infrastructure

5.18 External Supplier Management Policy

5.18.1 This policy ensures BU's information is protected when being handled by external suppliers and that security requirements are satisfied and maintained when acquiring hardware and software from external suppliers.

5.18.2 These principles ensure information security requirements are documented in agreements with external suppliers (including suppliers of hardware, software and services, such as outsourcing and cloud) and incorporate security requirements throughout all stages of the relationship with each supplier.

5.19 Systems Development Management Policy

5.19.1 This policy ensures business applications are developed in a secure environment and meet business and information security requirements.

5.19.2 These principles establish a structured systems development methodology that involves isolating development environments, applying security throughout the development process and performing quality assurance

5.20 Systems Development Life Cycle Policy

5.20.1 This policy ensures business and information security requirements are met throughout a systems development process and at implementation.

5.20.2 These principles will implement a systems development methodology that addresses security during requirements gathering, design and build, testing and implementation.

5.21 Physical and Environmental Security Policy

5.21.1 This policy ensures that important IT facilities and services are available when required and to prevent unauthorized disclosure and unavailability of information.

5.21.2 These principles protect IT facilities and services against malicious attack, accidental damage, loss of power, natural hazards and unauthorised physical access.

5.22 Information Security Business Continuity Policy

5.22.1 This policy ensures the organisation is resilient to attack and can continue to operate effectively in the event of a disaster or crisis.

5.22.2 These principles develop an organisation-wide business continuity strategy and programme that includes co-ordinating and maintaining business continuity plans and arrangements across the organisation.

5.23 BU Information Security Standards

5.23.1 A standards document assigning quantifiable measures for each of the policy areas within the Information Security framework.

General

6. REFERENCES AND FURTHER INFORMATION

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