Owner:	Chief Technology Officer
Version number:	2.0
Date of approval:	June 2021
Approved by:	Director of IT & Chief Technology Officer
Effective date:	November 2018
Date of last review:	June 2021
Due for review:	June 2022

System Management Policy

1. SCOPE AND PURPOSE

1.1 This policy is a sub-policy of the 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 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 topics related to BU System Management which includes:

a) System Management
b) Server Configuration
c) Virtual Servers
d) Network Storage Systems
e) Backup
f) Change Management
g) Service Level Agreements

2. KEY RESPONSIBILITIES

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

[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

2.2 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 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 complying by adopting the process and procedures which support this policy.

3. LINKS TO OTHER BU DOCUMENTS

3.1 There are a number of other policies and procedures which sit alongside this policy. Some of these are as follows:

a. Information Security
b. Acceptable Use
c. Data Protection
d. Asset Management - Information Classification
e. Application Protection
f. Security Architecture
g. Technical Security Infrastructure
h. System and Software Vulnerability Management
i. Hardware/Software Acquisition
j. Physical and Environmental Security
k. Server Configuration
l. Access Management
m. Physical Protection
n. Resilience
o. Patch Management

Policy

4. SYSTEM MANAGEMENT

4.1 Computer systems, network and telecommunications installations should be designed to cope with current and predicted information processing requirements and protected using a range of in-built controls to ensure that they can meet the security requirements of the critical business applications they support, i.e., protect against the compromise of confidentiality, integrity and availability of information being processed.

4.2 There should be documented standards/procedures for information system, network, and telecommunication installation designs, which require:

a) designs to take account of security architecture principles, business, and security requirements
b) compatibility to be maintained with other information systems, networks and telecommunication installations used by the organisation
c) the installations to be designed to cope with foreseeable developments in the organisation's use of IT

4.3 They should:

a) be managed from a central point
b) minimise the need for manual intervention

c) be set up so that they can be configured remotely, and automatically monitored against predefined thresholds
d) encrypt administrative access to information systems, network devices and telecommunications equipment

4.4 Designed to incorporate security architecture principles by:
a) building security into the installation design
b) using multiple layers of different types of protection
c) granting users, the minimum level of access
d) incorporating a coherent, integrated set of technical standards
e) supporting consistent naming conventions
f) minimising single points of failure
g) providing fail secure systems where in the event of a system failure, information is not accessible to unauthorised individuals and cannot be tampered with or modified

4.5 The system, network and telecommunications equipment should have:
a) sufficient capacity to cope with peak workloads
b) expansion/upgrade capabilities to cope with projected demand
c) a control and monitoring facility capable of providing management reports

4.6 The system, network and telecommunications equipment should be designed to:
a) include the installation of malware protection software on key servers
b) enable a standard predetermined server configuration to be built, the installation of which can be automated
c) enable authorised users to access multiple systems and resources via single sign-on
d) be managed from a central point
e) support the prompt application of security updates to respond to changing threats and vulnerabilities, and attacks when they occur

4.7 Networks should be designed to:
a) incorporate the use of security domains to segregate information systems with specific security requirements or different levels of trust
b) employ firewalls in a manner that prevents them from being bypassed
c) isolate particular types of network traffic using a dedicated network to prevent impact on other network traffic
d) perform network traffic prioritisation and ‘class of service’ to reduce network latency
e) restrict the number of entry points into networks
f) allow access only to ‘trusted’ users by preventing unauthorised devices from connecting to networks

4.8 Key components of computer and network installations should be protected by:
a) segregating critical business applications from all other applications and information, as agreed with their business owners
b) storing source code (or equivalent) in a secure location away from the live environment and restricting access to a limited number of authorised individuals
c) segregating different types of software and information

4.9 Live environments should be segregated from development and acceptance testing activity by using different computer rooms, processors, virtual servers, domains and partitions

5. SERVER CONFIGURATION

5.1 Servers should be configured to function as required and prevent unauthorised or incorrect updates to ensure servers operate as intended and not compromise the security of computer installations or other environments.

5.2 Servers should be configured in accordance with documented standards/procedures, which cover:

a) providing standard firmware configurations
b) using standardised, predetermined server images to build/configure servers
c) changing vendor defaults and other security parameters
d) disabling or restricting unnecessary functions and services
e) restricting access to powerful system utilities and host parameter settings
f) protecting against unauthorised access
g) performing standard security management practices

5.3 Servers should be provided with standard firmware configurations.

5.4 Server images should be reviewed, tested and kept up-to-date with recent patches and changes to build/configurations.

5.5 Servers should be configured to disable or restrict:

a) non-essential or redundant services
b) communication services that are inherently susceptible to abuse
c) communication protocols that are prone to abuse
d) execute permissions on sensitive commands or scripts
e) powerful system utilities or control panels
f) run commands or command processors
g) the ‘auto-run’ feature

5.6 They should be configured to protect memory against misuse by malicious or compromised applications.

5.7 Access to system utilities and server parameter settings should be:

a) restricted to a limited number of authorised individuals
b) restricted to narrowly-defined circumstances
c) subject to authorisation

5.8 Servers should be protected against unauthorised access by:

a) disabling unnecessary or insecure user accounts
b) changing important security-related parameters to be different from the defaults set by vendors or suppliers
c) invoking time-out facilities that automatically log off computing devices after a predetermined period of inactivity, clear screens and require users to sign-on again before restoring screens

5.9 They should be subject to standard security management practices, which include:

a) restricting physical access to a limited number of authorised individuals
b) keeping them up-to-date
c) maintaining up-to-date malware protection software to prevent infection by malicious software
d) applying a comprehensive set of system management tools
e) monitoring so that events such as hardware failure and attacks against them can be detected and responded to quickly and effectively
f) using secured technologies

g) reviewing them on a regular basis to verify configuration settings, evaluate password strengths and assess activities performed on the server

6. VIRTUAL SERVERS

6.1 Virtual servers should be, subject to approval, deployed on robust, secure, physical servers and configured to segregate sensitive information to prevent business disruption as a result of system overload or disclosure of sensitive information to unauthorised individuals.

6.2 Virtual servers should be deployed, configured and maintained in accordance with documented standards/procedures.

6.3 Standards/procedures should cover the protection of:

a) physical servers that are used to host virtual servers
b) hypervisors associated with virtual servers
c) virtual servers that run on a physical server

6.4 Physical servers that are used to host virtual servers should be protected by:

a) locating them in physically secure environments
b) restricting physical and logical access to a limited number of authorised individuals
c) requiring authorisation when any access is needed

6.5 Physical servers that are used to host virtual servers should be protected against:

a) unmanaged and ad hoc deployment of virtual servers
b) resource overload by restricting the maximum number of virtual servers that can be created on each physical server

6.6 Hypervisors should be configured to:

a) segregate virtual servers according to the confidentiality requirements of information they process
b) logically separate each virtual server to prevent information being transferred between discrete environments
c) restrict access to a limited number of authorised individuals who are capable of creating virtual servers and making changes to them correctly and securely
d) encrypt communications between virtual servers
e) segregate the roles of hypervisor administrators

6.7 Virtual servers should be protected by applying standard security management practices to hypervisors, which include:

a) applying a strict change management process to help ensure the hypervisor remains up-to-date
b) monitoring, reporting and reviewing administrator activities to help ensure actions and privileges that they are allowed to perform are specifically aligned to their duties
c) restricting access to the virtual server management console (or equivalent) to a limited number of authorised individuals
d) monitoring network traffic between different virtual servers and between virtual servers and physical servers to detect malicious or unexpected behaviour and known attacks

6.8 Each virtual server should be protected by applying appropriate security management practices.

7. NETWORK STORAGE SYSTEMS

7.1 Network storage systems should be protected using system and network controls to ensure network storage systems operate as intended, are available when required and do not compromise the security of information they store.

7.2 Network storage systems, such as Storage Area Network (SAN) and Network Attached Storage (NAS) should be deployed, configured and maintained in accordance with documented standards/procedures.

7.3 Standards/procedures should cover:

a) design and configuration of network storage systems
b) performing standard security practices
c) protection of network storage management consoles and administration interfaces
d) security arrangements specific to NAS and SAN

7.4 Network storage systems should be designed and configured to:

a) use standardised components
b) be managed from a central point using a minimum number of management consoles
c) restrict access to particular areas of storage to prevent unauthorised or unauthenticated access
d) enable authorised users to access multiple systems and resources via single sign-on

7.5 Network storage systems should be subject to standard security management practices.

7.6 Sensitive information stored on network storage systems should be protected according to its security requirements

7.7 Network storage system components should be protected by:

a) restricting administration access to a limited number of authorised staff;
b) using access controls that support individual accountability, and prevent unauthorised access
c) restricting management functions
d) using secure web protocols and secure services for running terminal sessions

8. BACKUP

8.1 Backups of essential information and software should be performed on a regular basis, according to a defined cycle to ensure that, in the event of an emergency, essential information or software can be restored within critical timescales.

8.2 Backups of essential information and software should be performed frequently enough to meet business requirements.

8.3 There should be documented standards/procedures for performing backups, which cover:

a) the types of information and software to be backed up
b) backup cycles
c) methods for performing backups (including validation, labelling and storage)
d) protection of backups

8.4 Backups should be:

a) performed using dedicated backup management software to strengthen the security of information backed up
b) recorded in a log which includes details about data backed up, the date and time and media used
c) verified to ensure that backed up software and information can be restored successfully
d) related to control points in live processes
e) reconciled to the live version when copies are taken
f) clearly and accurately labelled
g) protected from accidental overwriting, and subject to the same level of protection as live information

8.5 Backup arrangements should consider legal, regulatory and contractual requirements.

8.6 Critical timescales for data to be backed up should be identified.

8.7 Backup arrangements should enable operating systems, application software, system software associated with technical infrastructure and business information to be restored within a critical timescale by using one or more of the following:
a) online storage, which typically provides access to backups of information almost instantaneously
b) near-line storage, which enables the restore of information within minutes
c) off-line storage, which can often result in longer restore times

8.8 Backups should be protected from loss, damage, and unauthorised access, by:
a) storing backup media in accordance with manufacturer specifications
b) locating them in a locked, fireproof computer media safe on-site to enable important information to be restored quickly
c) keeping copies in secure facilities off-site to enable systems or networks to be restored using alternative facilities in the event of a disaster
d) restricting access to a limited number of authorised individuals

9. CHANGE MANAGEMENT

9.1 System Management activity is subject to the existing BU Change Management policy and related processes and controls.

9.2 Changes to business applications, information systems and network devices should be tested, reviewed, and applied using a change management process to ensure that changes are applied correctly and do not compromise the security of business applications, computer systems or networks.

9.3 A change management process should be established, which covers any type of change.

9.4 The change management process should be documented, and include approving and testing changes to ensure that:
a) they are made correctly and securely
b) they do not compromise security controls
c) no unauthorised changes have been made

9.5 Prior to changes being applied to the live environment:
a) change requests should be documented and accepted only from authorised individuals
b) changes should be approved by an appropriate business representative
c) the potential business impacts of changes should be assessed

d) changes should be tested to ensure vulnerabilities have not been introduced and help determine the expected results
e) changes should be reviewed to ensure that they do not compromise security controls
f) back-out positions should be established so that information systems and networks can recover from failed changes or unexpected results

9.6 Changes to information systems and networks should be:
a) performed by skilled and competent individuals who are capable of making changes correctly and securely
b) supervised by an IT specialist
c) signed off by an appropriate business representative

9.7 Arrangements should be made to ensure that once changes have been applied:
a) version control is maintained
b) a record is maintained, showing what was changed, when, and by whom
c) details of changes are communicated to relevant individuals
d) checks are performed to confirm that only intended changes have been made
e) documents associated with information systems and networks are updated
f) the classification of information associated with information systems and networks is reviewed
g) standard secure configurations are updated, to ensure changes apply to new builds

9.8 Checks should be performed on a regular basis to identify unapproved changes and confirm that only intended changes have been made.

10. SERVICE LEVEL AGREEMENTS

10.1 Computer and network services that support critical business processes and applications should only be obtained from service providers capable of providing required security controls and supported by documented contracts or service level agreements to define the business requirements of any computer or network services, including those for information security, and to ensure they are met.

10.2 Service agreements should specify:
a) who is in charge of the computer and network services being provided
b) who is in charge of delivering the required service
c) the level of criticality of the service
d) dates/times when the service is required
e) the capacity requirements of systems and networks
f) maximum permissible down-time
g) critical timescales
h) the penalties to be imposed in the event the service provider fails to deliver the pre-agreed level of service

10.3 Service agreements should specify access control requirements, including:
a) access restrictions
b) authentication methods
c) restrictions on methods of connection and access to particular services
d) segregating computer and network components, such as dedicated lines or virtual local area networks (VLANs) for sensitive network traffic

10.4 Service agreements should specify requirements for:
a) segregation of duties and facilities
b) protection against malware

c) protecting sensitive information in transit (e.g. by using encryption)
d) installation and maintenance activity relating to hardware and software
e) change management and patch management
f) information security incident management (including details of key contacts and escalation procedures)
g) detecting service interruptions and recovering from them
h) ensuring business and system continuity of service

10.4 Arrangements should be made to:

a) restrict the use of services to those provided by approved suppliers
b) obtain independent confirmation of the security controls applied by the service provider
c) deal with security issues via a single point of contact and through an individual who is sufficiently senior and competent to deal with security issues effectively

10.5 Service agreements should be:

a) assessed by an information security specialist
b) signed off by an appropriate business representative and the service provider
c) enforced according to the agreed, documented conditions
d) reviewed on a regular basis to ensure service targets are being achieved and security requirements are being met

General

11. REFERENCES AND FURTHER INFORMATION

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

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