Threat and Vulnerability 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 community of stakeholders.

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

1.5 This policy covers the topics related to Threats and Vulnerability Management which includes;
   a) Systems and Software Vulnerability Management
   b) Malware Awareness
   c) Malware Protection Software
   d) Security Event Logging
   e) System/Network Monitoring
   f) Intrusion Detection

2. KEY RESPONSIBILITIES

2.1 The BU Board has delegated day-to-day responsibility for ensuring compliance with the policy to the Director of IT.

---

\(^1\) 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, including academic staff, are responsible for implementing the administrative and technical controls that support and enforce this policy.

2.4 All those outlined in 1.1 are responsible for complying by adopting the process and procedures that ensure the implementation of this policy.

3. **LINKS TO OTHER BU DOCUMENTS**

3.1 In addition to this document and the supporting set of strategic policy documents there are several BU policies which complement this policy, as follows:
   - Data Protection Policy for Staff and BU Representatives
   - BU Acceptable Use Policy

4. **SYSTEM AND SOFTWARE VULNERABILITY MANAGEMENT**

4.1 There will be documented standards/procedures for system and software vulnerability management which specify the:
   a) requirement to manage system and software vulnerabilities associated with business applications, information systems and network devices
   b) method of identifying the publication or discovery of technical vulnerabilities (e.g., in the public domain), in a timely manner
   c) need to scan business applications, information systems and network devices for system and software vulnerabilities
   d) Bournemouth University’s approach to patching (i.e., the patch management process)
   e) methods of patch distribution (e.g., automated deployment)

4.2 Standards/procedures will be supported by a system and software vulnerability management process to manage system and software vulnerabilities associated with:
   a) business applications, operating system software and firmware (e.g., on servers, mobile devices, and consumer devices)
   b) computer equipment (including servers, desktop computers and laptops)
   c) consumer devices (including tablets and smartphones)
   d) virtual systems (e.g., virtual servers and virtual desktops)
   e) network storage systems (including Storage Area Network (SAN) and Network-Attached Storage (NAS))
   f) network equipment (e.g., routers, switches, wireless access points and firewalls)
g) VoIP telephony software and conferencing equipment
h) office equipment (e.g., network printers, photocopiers, facsimile machines, scanners, and multifunction devices (MFDs))
i) specialist systems (e.g., information systems that support or enable the organisation’s physical infrastructure such as embedded systems and control systems (includes CCTV and Network based Locking Systems)

4.3 The system and software vulnerability management process will be:
   a) documented
   b) approved by the Director of IT
   c) supported by an individual or team with defined roles and responsibilities for vulnerability management
   d) assigned an owner
   e) applied on a continuous basis (e.g., monthly)

4.4 The system and software vulnerability management process will be used by system owners in collaboration with the business owners and to help:
   a) determine the importance of business applications, information systems and networks (e.g., based on the information handled, the business processes supported and the environments in which they are used) to help identify the extent of vulnerabilities and timescales/priorities for remediating vulnerabilities
   b) assess system and software vulnerabilities as soon as they become publicly known (e.g., tracking CERT advisories and subscribing to vulnerability notification services)
   c) identify and obtain patches (including patch bundles, critical updates and service packs) when they are available to remediate discovered vulnerabilities (e.g., by working with software vendors, or downloading from approved vendor websites)
   d) decide when to deploy patches and analyse the results of testing the patches
   e) record patches that have been applied

4.5 The system and software vulnerability management process will be supported by performing vulnerability scans of business applications, information systems and network devices to help:
   a) identify system and software vulnerabilities that are present in business applications, information systems and network devices
   b) determine the extent to which business applications, information systems and network devices are exposed to threats
   c) prioritise the remediation of vulnerabilities (e.g., using the vendor’s patch release schedule)
   d) provide a high-level view of vulnerabilities across the organisation’s technical infrastructure (e.g., to make comparisons and identify trends)

4.6 Vulnerability scanning of business applications, information systems and network devices will be performed:
a) using automated vulnerability scanning software or a commercial vulnerability scanning service
b) on a regular basis (e.g., monthly or in response to a new threat)

4.7 Vulnerability scanning will be:
   a) restricted to a limited number of authorised individuals
   b) using approved and dedicated systems
   c) monitored

4.8 System and software vulnerabilities will be remediated using a patch management process, which:
   a) specifies methods of validating patches (e.g., ensuring that the patch is from an authorised source)
   b) assesses the business impact of implementing patches (or not implementing a particular patch)
   c) ensures patches are tested against known criteria
   d) describes methods of deploying patches in a timely manner (e.g., grouping multiple patches and using software distribution tools)
   e) provides methods of deploying patches to systems that are not connected to the network (e.g., standalone computers) or devices that connect to the network infrequently (e.g., travelling staff)
   f) reports on the status of patch deployment across the organization
   g) includes methods of dealing with the failed deployment of a patch (e.g., redeployment of the patch)

4.9 Methods will be established to protect information in the event a system or software vulnerability cannot be remediated with a patch, or an available patch cannot be applied (e.g. by disabling services, adding additional access controls and performing detailed monitoring).

5. MALWARE AWARENESS

5.1 There will be documented standards/procedures covering protection against malware, which:
   a) provide users with information about malware
   b) warn users how to reduce the risk of malware infection

5.2 Users will be informed about the:
   a) prevalence of malware and associated risks (e.g., unauthorised access to critical business applications, corruption of critical business information or leakage of sensitive information)
   b) ways in which malware can install itself on computing devices
   c) common symptoms of malware infection (e.g., poor system performance, unexpected application behaviour, sudden termination of an application)

5.3 Users will:
a) be advised to manually scan (on-demand scanning) files for malware when connecting portable storage devices to computing devices, or when receiving unknown or questionable files (e.g., by email).
b) be notified via Marketing and Communications (M&C) of significant new malware-related risks (e.g., by email, freeware, or suspicious websites)
c) be required to report suspected or actual malware to a single point of contact for support (IT Services Service Desk)
d) be supported by specialist technical support at required times (e.g. normal business hours)

5.4 The risk of malware infection will be reduced by warning users not to attempt to:
   a) install software from untrusted sources
   b) open untrusted attachments
   c) click on suspicious or unknown hyperlinks within emails or documents
   d) manually resolve malware problems

5.5 Malware protection will include:
   a) implementing emergency procedures for dealing with malware-related information security incidents (e.g., sharing detected malware with malware protection software vendors in order to create a signature that can be distributed throughout Bournemouth University and the community)
   b) monitoring external intelligence sources (e.g., media, security vendors, and specialist intelligence organisations) for new malware threats
   c) informing external parties of the organisation’s malware protection standards/procedures when necessary.

6. MALWARE PROTECTION SOFTWARE

6.1 There will be documented standards/procedures related to malware protection software, which specify:
   a) methods for installing and configuring malware protection software (e.g., anti-virus protection software, anti-spyware software)
   b) update mechanisms for malware protection software (including automatic updates)
   c) the processes required to review the effectiveness of malware protection software
   d) steps required to reduce the risk of malware being downloaded

6.2 Malware protection software will be installed on systems that are exposed to malware (e.g., those that are connected to networks or the Internet, support the use of portable storage devices or are accessed by multiple external suppliers)

6.3 Malware protection software will protect against all forms of malware (e.g. computer viruses, worms, trojan horses, spyware, rootkits, botnet software, keystroke loggers, adware, and malicious mobile code).
6.4 Malware protection software will be distributed automatically, and within defined timescales to reduce the likelihood of systems being exposed to the most recent malware (including those that are associated with ‘zero-day’ attacks).

6.5 Malware protection software will be configured to scan components of a system based on a risk informed approach.

6.6 Malware protection software will be configured to:
   a. be active at all times (e.g., by scanning files as they are accessed to provide real-time protection, or by being configured to be active at all times and to restart if stopped)
   b. perform scheduled scanning at predetermined times
   c. provide a notification when suspected malware is identified (e.g., by producing an event log entry and providing an alert)
   d. disable and quarantine files suspected of containing malware (e.g., for further investigation)
   e. remove malware and any associated files immediately upon detection
   f. ensure that important settings cannot be disabled, or functionality minimised

6.7 Regular reviews of servers, desktop computers, mobile devices and consumer devices will be performed to ensure that:
   a) malware protection software has not been disabled
   b) the configuration of malware protection software is correct
   c) updates are applied correctly within defined timescales
   d) emergency procedures are in place to deal with a malware-related information security incident

6.8 The risk of downloading malware will be reduced by:
   a) configuring web browsers so that users are asked if they wish to install mobile code
   b) allowing only trusted mobile code to be downloaded (i.e., signed with a trusted digital certificate)

7. **SECURITY EVENT LOGGING**

7.1 Reliable security event logs will be established (e.g., to store messages about system crashes, unsuccessful login of authorised users, and unsuccessful changes to access privileges), which are supported by documented standards/procedures.

7.2 Standards/procedures will cover:
   a) management of security event logging
   b) identification of business applications and technical infrastructure systems on which event logging will be enabled to help identify security-related events
c) configuration of information systems to generate security-related events (including event types such as failed login attempts, system crash, deletion of user account and event attributes such as date, time, UserID, file name, IP address)
d) storage of security-related events within event logs
e) analysis of security-related event logs (including normalisation, aggregation, and correlation)
f) protection of security-related event logs
g) retention of security-related event logs (e.g., to meet legal, regulatory, and business requirements for possible forensic investigations)

7.3 Security event log management will include setting policy, defining roles and responsibilities, ensuring the availability of relevant resources, and guidance on the frequency and content of reports.

7.4 Security event logging will be performed on information systems that:
   a) are critical to the organisation (e.g., financial databases, servers storing medical records or key network devices – systems which store, process or transmit information classified as confidential or above); and/or
   b) have experienced a major information security incident; and/or
   c) are subject to legislative or regulatory mandates

7.5 Business applications and technical infrastructure systems will be configured to:
   a) enable event logging (using a standard format, such as syslog, MITRE Common Event Expression, or equivalent)
   b) generate appropriate event types (e.g., service creation, system crashes, object deletion and failed login attempts)
   c) incorporate relevant event attributes in event entries (e.g., IP address, username, time and date, protocol used, port accessed, method of connection, name of device and object name)
   d) use a consistent, trusted date and time source (e.g., using the Network Time Protocol (NTP) supported by global positioning system (GPS), atomic clocks or timeserver on the Internet) to ensure event logs use accurate timestamps

7.6 Security-related event logging will be:
   a) enabled at all times
   b) protected from unauthorised access and accidental or deliberate modification or overwriting (e.g., using write-only media or dedicated event log servers).

7.7 Mechanisms will be established so that:
   a) storage space is allocated based on expected volumes of event information
   b) when event logs reach a maximum size, the system is not halted through lack of disk space and logging continues with no disruption
7.8 Security-related event logs will be analysed regularly (e.g., using automated security information and event management (SIEM) tools or equivalent) to help identify anomalies, and include:
   a) processing of key security-related events (e.g., using techniques such as normalisation, aggregation, and correlation)
   b) interpreting key security-related events (e.g., identification of unusual activity)
   c) responding to key security-related events (e.g., passing the relevant event log details to an information security incident management team)

7.9 SIEM tools will be configured to:
   a) identify expected events (to help reduce review and investigation activities for legitimate business events)
   b) detect unexpected events (to help reduce the likelihood of false positives and false negatives)

7.10 Security-related event logs will be:
   a) reviewed regularly
   b) archived regularly (e.g., using a rotation schedule) and digitally signed before being stored
   c) stored securely for possible forensic analysis at a later date
   d) retained according to retention standards/procedures

8. SYSTEM / NETWORKING MONITORING

8.1 The performance of business applications, information systems and networks will be monitored against agreed thresholds to identify irregularities which may indicate a compromise:
   a) by reviewing current utilisation of systems at normal and peak periods
   b) using automated monitoring software that generates alerts (e.g., via a management console, email messages or SMS text messages to mobile telephones)
   c) by reviewing event logs of system and network activity regularly (e.g., to help identify suspicious or unauthorized activity)
   d) by investigating bottlenecks/overloads

8.2 System/network monitoring activities will be conducted regularly, and involve:
   a) checking whether powerful system utilities/commands have been disabled on attached hosts (e.g., by using a 'network sniffer')
   b) checking for the existence and configuration of unauthorised wired and wireless networks (e.g., using automated discovery/mapping tools)
   c) discovering the existence of unauthorised systems (e.g., by using automated discovery/mapping tools)
   d) detecting unauthorised changes to software, electronic documents, and configuration files (e.g., by using file integrity checking software)
   e) identifying potential unauthorised disclosure of information (e.g.,
transfers of large volumes of data, anomalies in network traffic or unauthorised use of network protocols such as FTP)
f) checking DNS logs to identify outbound network connections to malicious servers, such as those associated with botnet command and control servers

8.3 System/network monitoring activities will be conducted to help identify:
   a) unauthorised scanning of business applications, information systems and networks
   b) successful and unsuccessful attempts to access protected resources (e.g., DNS servers, web portals and file shares)
   c) unauthorised changes to user accounts and access rights (to detect privilege escalation)
   d) extraction or modification of sensitive information (e.g., by checking the timestamp of files and using file integrity checking software)
   e) attempts to conceal unauthorised access and activity (e.g., deletion of or tampering with event logs to cover tracks)
   f) the creation of back doors that provide unauthorised privileged access to business applications, information systems and networks at a later time.

8.4 The use of network analysis/monitoring tools will be restricted to a limited number of authorised individuals (e.g., network administrators or staff in an information security function).

8.5 The owners of business applications, information systems and networks will review the results of monitoring activities.

9. **INTRUSION DETECTION**

9.1 Intrusion detection mechanisms will be employed for critical business applications, information systems and networks to identify predetermined and new types of attack.

9.2 Intrusion detection methods will be supported by documented standards/procedures, which cover:
   a) methods of identifying unauthorised activity
   b) analysis of suspected high risk and impact intrusions
   c) relevant responses to different types of attack (e.g., an information security incident management process).

9.3 Intrusion detection mechanisms will identify:
   a) unplanned termination of processes or applications
   b) activity typically associated with malware or traffic originating from known malicious IP addresses or network domains (e.g., those associated with botnet command and control servers)
   c) known attack characteristics (e.g., denial of service and buffer overflows)
d) unusual or anomalous system behaviour (e.g., keystroke logging, process injection and deviations in the use of standard protocols)
e) unauthorised access (actual or attempted) to systems or information

9.4 Intrusion detection mechanisms will be configured to:
   a) incorporate new or updated attack characteristics
   b) provide alerts when suspicious activity is detected, supported by documented processes for responding to suspected intrusions
   c) protect the intrusion detection software against attack (e.g., by hiding the presence of intrusion detection software)

9.5 Intrusion detection methods will be supported by specialist software, such as host intrusion detection systems (HIDS) and network intrusion detection systems (NIDS).

9.6 Network intrusion detection sensors (i.e., specialist hardware used to identify unauthorised activity in network traffic) will be protected against attack (e.g., by preventing the transmission of any outbound network traffic, or by using a network tap to hide the presence of the sensor).

9.7 Intrusion detection software will be:
   a) updated automatically and within defined timescales (e.g., delivery of distribution attack signature files to intrusion detection sensors via a central management console)
   b) configured to provide an alert when suspicious activity is detected (e.g., via a management console, email messages or SMS text messages to mobile telephones)

9.8 Regular reviews will be performed by IT Services to ensure that:
   a) the configuration of intrusion detection software meets requirements
   b) intrusion detection software has not been disabled or tampered with
   c) updates have been applied within defined timescales

9.9 Suspected intrusions will be analysed by IT Services and potential business impact assessed. Initial analysis will include:
   a) confirming whether an attack is actually occurring (e.g., by eliminating false positives)
   b) determining the type of attack (e.g., worms, buffer overflows or denial of service)
   c) identifying the original point of attack
   d) quantifying the possible impact of an attack.

9.10 The status of an attack will be assessed in terms of:
   a) time elapsed since the start of the attack and since detection of the attack
   b) scale (e.g., the number and type of particular systems and networks affected)
9.11 There will be a documented method (e.g., an escalation process) for reporting serious attacks (e.g., to the information security incident management team and/or Serious / Major Incident Management team).

**General**

10. REFERENCES AND FURTHER INFORMATION

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

10.2 Please refer to the Data Protection policy for further information