Edinburgh Napier
UNIVERSITY

Vulnerability Management Policy

Audience and Applicability

- The Information Security Team at Edinburgh Napier University, who are responsible for providing vulnerability scanning services and the reporting data from them and taking action to protect the University from security vulnerabilities.
- Technical Operations Owners at Edinburgh Napier University, who are responsible for ensuring that they manage the security vulnerabilities in their systems and take necessary remedial action within prescribed timescales. A Technical Operations Owner is anyone with technical administrative control over a given University system.
- IT infrastructure and support teams at Edinburgh Napier University, who are responsible for ensuring that systems provided for others to use are secure by default, that all preinstalled software is properly maintained and that systems are properly recorded in asset management tools.
- Anyone accessing Edinburgh Napier University systems or services - including wired and wireless networks - who may find that their access is limited or blocked if their device is determined to pose an unacceptable level of risk due to the presence of security vulnerabilities.
- This policy does not apply to systems which are designated for teaching or research purposes, where the presence of security vulnerabilities is necessary for those purposes e.g. intentionally vulnerable systems for use in penetration testing labs. However, such systems must not pose an unacceptable level of risk to other University systems, must be suitably isolated from other University systems and must not be accessible to anyone not authorised to interact with them.

Requirements

Software Updates

1. All systems shall have software updates applied regularly, according to the patching regime defined in *Annex A – Vulnerability Management Technical Standard*.
2. Technical Operations Owners shall have a documented software update plan for their systems. For devices that are not automatically updated, this should detail how and when updates get applied, and who is responsible for doing and checking the updates. The strategy should account for system availability requirements, relevant dependencies and staff absences to ensure that software updates are always applied within prescribed timescales.
3. Line managers of Technical Operations Owners shall ensure that their team members are aware of the importance of regular patching and shall work with them to ensure that such work is prioritised appropriately, including delaying or interrupting other planned work if necessary. Similarly, Technical Operations Owners shall do the same with Service Owners, Data Owners, Business Owners, end users and other stakeholders, leading to a culture where regular maintenance of systems is expected and desired.
4. Technical Operations Owners shall ensure that they are aware of when their vendors announce end of-support-dates for their software and shall be responsible for ensuring that University systems are either decommissioned, upgraded or migrated to in-support versions of software prior to the end-of-support date being reached and ideally well in advance of it.
5. Where supported and deemed safe to do so, software update mechanisms shall be configured to apply updates automatically.
6. Where supported and especially in cases where a single update is being applied to a large number of systems, updates shall be deployed in batches/rings/waves beginning with dedicated test systems and followed by early adopters, risk-tolerant users and finally ending with risk-adverse users and business-critical systems. This helps to minimise the risk of widespread disruption due to a broken update.
7. Where centralised tools are used to manage software updates, the reporting features of the tools shall be used to ensure that updates are being applied successfully and within the required timescales. Technical Operations Owners shall be responsible for ensuring that any update failures identified by such tools are investigated and remediated.

Automated Vulnerability Scanning

8. The Information Security Team shall be authorised and required to carry out regular automated vulnerability scanning activities against Edinburgh Napier University assets, according to the scanning regime defined in *Annex A – Vulnerability Management Technical Standard*.
9. The Information Security Team shall ensure that an appropriate set of automated vulnerability scanning services are procured for use by the University, such that

infrastructure and web application scans can be carried out against on-premise and cloud-hosted assets.

10. The Information Security Team shall make the results from such scans available to Technical Operations Owners and other relevant persons. Technical Operations Owners shall be responsible for acting upon the scan results in accordance with *Annex A – Vulnerability Management Technical Standard*.
11. The Information Security Team shall use the set of automated vulnerability scanning services to attempt to locate any assets which may be connected to University networks but which are not present in the relevant asset management tools. They shall attempt to determine the correct Technical Operations Owner for any such assets and request that they update the relevant asset management tools. If no Technical Operations Owner can be determined, the asset may be disconnected from University networks as per the *Enforcement* section below.
12. The Information Security Team may use the set of automated vulnerability scanning services or other relevant tools to attempt to locate any instances of a specific high-severity vulnerability if deemed necessary or advised to do so by a trusted partner.
13. When new services are being introduced, a scan shall be performed and all resulting issues addressed before any of the following activities are carried out:
    - External access to the service from the internet is allowed.
    - Information belonging to the ‘Confidential’ classification is added/copied/imported to or stored in the service.
    - Authenticated access to the service is expanded beyond just those end users who are part of any development, testing or trial group.
14. Technical Operations Owners shall be responsible for requesting scans for new services at the appropriate time and service delivery plans should be structured to allow time for vulnerabilities to be addressed if found.

Manual/Human-Led Security Testing (Pen-Testing)

15. Upon the request of Technical Operations Owners or as otherwise directed by the Cyber Security Oversight Group, the Information Security Team shall arrange for a competent third-party to carry out manual security testing of all assets comprising a specific system.
16. The need for and frequency of manual security testing shall be determined by the criticality of the system.
17. Technical Operations Owners shall make themselves available as required for pre-enagagement scoping and post-engagement review calls with the Information Security Team and the third-party to ensure that the latter has all necessary information to carry out the testing and to provide an overview of their findings and recommendations.
18. Technical Operations Owners shall be responsible for acting upon the test results in accordance with *Annex A – Vulnerability Management Technical Standard*.

Vulnerability Reporting

19. If a member of University staff or an external contractor under contract by the University becomes aware of a suspected or known vulnerability in any University system or service, they shall report it in the manner defined in *Annex A – Vulnerability Management Technical Standard*.
20. To facilitate individuals who are not affiliated with the University to report suspected or known vulnerabilities in University systems or services, information about vulnerability reporting shall be published on a public University website.

Enforcement

21. If a system is found to have unresolved security vulnerabilities (including due to misconfiguration), no valid exemption exists and the Technical Operations Owner either cannot be identified, or is unable or unwilling to address the vulnerabilities in a manner compliant with this Policy, the Information Security Team, acting on the authority of the Cyber Security Oversight Group and considering both the level of risk posed by the vulnerabilities to the University and the business impact of disrupting user access to the system, may restrict or fully remove the system's network connectivity.
22. The Information Security Team shall attempt to identify and contact the Technical Operations Owner (if known) and the relevant Dean/Director to inform them if such action is being taken. Depending on the level of risk, this contact may not happen until after the system's network connectivity is restricted or removed.
23. Normal network connectivity shall only be reinstated for a system once all of the vulnerabilities have been addressed to the satisfaction of the Information Security Team, as evidenced by a vulnerability scan or other suitable mechanism(s).

Exemptions

In certain circumstances it may be appropriate to exempt particular assets from vulnerability management, for example:

- Systems used in the teaching or research of software vulnerabilities, malware or security testing techniques.
- Systems which are known to suffer outages when scanned by a vulnerability scanner.
- Systems for which there is a known incompatibility between essential application software and an available software update for the operating system or other application software.
- Systems which utilise software no longer receiving updates from the vendor, but which perform specialist functions and cannot be easily replaced with a supported alternative.

24. If an exemption is required, it shall first be discussed between the Information Security Team and the Technical Operations Owner and then if agreed, recorded and reviewed in the manner defined in *Annex A – Vulnerability Management Technical Standard*.

25. Exemptions shall be requested if required, as systems which have vulnerabilities present and which do not have a valid exemption may lose network connectivity as per 21 above.
26. Alternative technical controls such as network isolation, the use of additional firewalls and network monitoring shall be used to reduce the risk posed by hosts exempted from vulnerability management.

Approval and Updates

- This policy has been introduced by the Cyber Security Oversight Group and all proposed updates to this policy will be reviewed and approved by that group. The Cyber Security Oversight Group reports to the University Risk & Resilience Committee, a sub-committee of the University Audit & Risk Committee and ultimately University Court.
- It is anticipated that as a new policy, there will need to be several early revisions of this policy as we receive feedback, learn from and adapt to its implementation.
- Unless otherwise stated in the revised version of the policy, all policy versions are effectively immediately upon publication. Anyone to which this policy applies should ensure that they are always referring to and acting in accordance with the current version of the policy.

Annex A – Vulnerability Management Technical Standard

Unless covered by a valid exemption to the Vulnerability Management Policy, University systems must:

- Have the Elastic and Tenable Agents installed and operational, if the device is running Windows, macOS or Linux.
- Have all installed software updated, including applying any manual configuration changes required to make the update effective, within 14 calendar days of an update being made available by the vendor, where one or more of the following are true:
    - The update fixes vulnerabilities described by the vendor as ‘critical’ or ‘high risk’
    - The update addresses vulnerabilities with a CVSS v3 base score of 7 or above
    - There are no details of the level of vulnerabilities the update fixes provided by the vendor
- Be configured to allow network connections from IP addresses used by the current set of automated vulnerability scanning services.
- Be configured to allow authentications from service accounts used by the current set of automated vulnerability scanning services.

Managed end user devices running Windows or macOS shall be continuously scanned using Tenable Agent, which currently reports vulnerability results for online assets daily.

Managed servers running Windows or Linux shall be continuously scanned using Tenable Agent, which currently reports vulnerability results for online assets daily.

Internet-accessible University IP address ranges and DNS names may also be externally scanned on a regular schedule.

Individual web applications shall be scanned on a schedule with a web application vulnerability scan, using URLs and credentials provided by the Technical Operations Owner. The frequency of such scans will be determined by the criticality of the system.

Unmanaged (including staff and student personal) devices on networks such as eduroam and any others intended for the use of such devices shall not be scanned.

Availability of Vulnerability Information

All Technical Operations Owners have been given access to the Tenable platform, which provides details of the specific vulnerabilities found in their systems. Technical Operations Owners are responsible for ensuring that they check this vulnerability information on a regular basis and shall take action as required to address vulnerabilities within the timescales detailed above.

Vulnerability Reporting

Upon the discovery of a suspected or known vulnerability in any University system or service by a member of staff or contractor working on behalf of the University, the discoverer shall report it to the IS Service Desk. A problem will be created to track the issue and it will be initially assigned to the Information Security Team for verification.

Exemptions

If a Technical Operations Owner believes that an exemption to the Vulnerability Management Policy is required, they shall first informally discuss the requirement with a member of the Information Security Team. If the Information Security Team member determines that an exemption is appropriate, they shall record the following information in the Vulnerability Management Exemptions list in SharePoint:

- Hostname(s)
- IP Address(es)
- Technical Operations Owner
- Reason for the exemption
- Details of any mitigating controls that will be implemented, if applicable
- Agreed duration of the exemption before a review is required (dependent on risk)

The Information Security Team shall make the current list of active exemptions available to the Cyber Security Oversight Group as requested. CSOG may ask for an exemption to be reviewed at any time, even if the exemption is not approaching its expected end date.

The Information Security Team will regularly review the current list of active exemptions and any that are approaching their expected end date will result in the Information Security Team contacting the Technical Operations Owner to determine if the exemption should be removed or extended. If the Technical Operations Owner does not respond to this request, the exemption will be removed upon the end date being reached.

Document Information

Publication/review date	2 June 2025
Review frequency	6 months
Date of next review	Before 30 November 2025

Document History

Version	**Date**	**Summary of changes**
0.1	01/08/2024	Initial version.
0.2	30/05/2025	All references to “System Owner” replaced with “Technical Operations Owner” to align with definitions used in OneTrust. All references to “Information Risk Oversight Group” replaced with “Cyber Security Oversight Group”. Replaced references to Rapid7 products with Elastic and Tenable products. Removed paragraph about additional Remediation Projects. Several minor updates in response to comments.
1.0	02/06/2025	Approved for publication by CSOG.