Third-party Privileged Access Policy

Audience / Applicability

1. Anyone who accesses Edinburgh Napier University systems, in any sort of support, administrative or privileged user capacity, where their primary affiliation is to an organisation other than Edinburgh Napier University.
    - This frequently means employees, contractors or consultants who are usually employed by an organisation that isn't Edinburgh Napier University and who may perform work for many customers/clients besides Edinburgh Napier University.
2. Edinburgh Napier University staff who are responsible for organising and overseeing any work carried out by any person as described above.
    - This is typically the Edinburgh Napier University System Owner and their colleagues, but can include project managers and procurement staff for systems or services which have yet to be purchased by Edinburgh Napier University.
3. This policy does not apply to anyone who accesses Edinburgh Napier University systems exclusively as a normal user, which is defined as having no ability to alter or modify the system for any other user, or modify the access rights of any other user. This includes overseas agents and partner organisations working on behalf of the University, the activities of which are covered by other end user policies.

Requirements

4. All third-party individuals who require privileged access to Edinburgh Napier University systems must have completed the relevant Oath of Confidentiality form(s) and these must have been validated prior to any access to Edinburgh Napier University systems taking place.

5. All third-party individuals who require privileged access to Edinburgh Napier University systems must have completed their own employer's mandatory security training and any applicable Edinburgh Napier University Information Security online training module(s) prior to any access to Edinburgh Napier University systems taking place.

6. All third-party individuals accessing Edinburgh Napier University systems must do so from an end-user/client device which is owned and managed by their employer. The use of personal devices for accessing Edinburgh Napier University systems as a privileged user is prohibited.

7. End-user/client devices used by third-party individuals to access Edinburgh Napier University systems must comply with the Minimum Security Baseline for Third-Party Access.

8. Credentials for accessing Edinburgh Napier University systems as a privileged user are issued to specific, named third-party individuals for their exclusive use and must not be shared with any other person, including within their own organisation. Organisations must ensure that if they need to have multiple people accessing Edinburgh Napier University systems, that a request for privileged access is made for each individual person.

9. The default method for third-party individuals to access Edinburgh Napier University systems as a privileged user is via the Edinburgh Napier University Privileged Access Management (PAM) system. Third-party individuals are expected to comply with this requirement and are not entitled to mandate the use of a particular access method. This requirement is to be advised during discussions prior to the procurement, renewal or upgrade of systems.

10. Requests to use alternative access methods will be considered on a case-by-case basis and must be made during discussions prior to the procurement, renewal or upgrade of systems, however Edinburgh Napier University is not obliged to agree to them and if a satisfactory solution cannot be identified this could result in a potential supplier being rejected.

11. Third-party individuals must not modify the state or configuration of existing security features on Edinburgh Napier University systems without first obtaining the consent of both their contact at Edinburgh Napier University and the University's Information Security Team. This includes - but is not limited to - disabling anti-malware/anti-virus solutions, modifying local firewall rules and enabling and/or using additional remote access methods.

12. All third-party individuals who currently have privileged access to Edinburgh Napier University systems using a VPN account created by the Event Accounts system are required to migrate to access via PAM (or an agreed alternative) when advised to by either their contact at Edinburgh Napier University or a member of Information Services staff.

13. Unless they are contracted to provide reactive out-of-hours support, third-party individuals must not be able to access Edinburgh Napier University systems as a privileged user on an ad-hoc, open-ended basis.

14. All requests for privileged access by a third-party individual must be made in advance of work being carried out and must be approved by the relevant member(s) of Edinburgh Napier University staff. Access must be enabled shortly before the scheduled start of the work and then disabled again shortly after the scheduled end of the work.

15. If the work being carried out by a third-party individual is subject to Change Control, the relevant change management processes must be completed prior to the work starting and the period for which access is permitted must be aligned with the agreed change window.

16. All privileged access by third-party individuals is subject to standard monitoring and logging, details of which are available in other University policies. Additionally, screen recordings of actions performed by third-party individuals may be captured and monitored live by Edinburgh Napier University staff, or reviewed after work has been carried out.

17. All third-party individuals must report any unusual or suspicious activity they may notice when accessing Edinburgh Napier University systems. They should do this via their contact at Edinburgh Napier University (if available at the time), or by contacting the IS Service Desk.

Minimum Security Baseline for Third-Party Access

End-user/client devices used by third-party individuals must:

- Utilise an operating system, firmware, drivers and application software which is at all times:
    - Correctly licenced
    - Supported by the vendor
    - Capable of receiving security updates from the vendor
- Be enrolled in a Mobile Device Management (MDM) platform (or equivalent), which is configured to periodically collect the status of the device, enforce these requirements and allow for the device to be remotely wiped if deemed necessary.
- Be configured to download and install all available software updates automatically (if that feature is available), either directly from the vendor or from an internal update source configured by the organisation which manages the device.
- Be configured to require user authentication that meets the following requirements before the device can be used:
    - A minimum password length of 12 characters, or 8 characters if Multi-Factor Authentication is also used
- Have endpoint security software installed and active at all times on Windows, macOS and Linux devices, which must be configured to:
    - Check for updated signatures/rules/content/etc. at least daily
    - Scan programs as they are executed
    - Scan files as they are accessed, including on removable media e.g. USB drives
    - Scan websites as they are accessed, if that feature is available
    - Send status, detection and relevant event information to a centralised logging platform
- Utilise full-disk encryption.
- Utilise a host-based firewall which is configured to block unauthenticated inbound network connections by default.
- Protect any Edinburgh Napier University data stored locally, by backing it up at least daily to a secure location, with backup data encrypted at rest and in transit.

If a third-party individual believes that any of these minimum security baseline requirements cannot be met, it must be discussed with their contact at Edinburgh Napier University and the University's Information Security Team prior to the start of any work.

Document Information

Publication/review date	11 March 2024
Review frequency	Annually
Date of next review	Before 11 March 2025

Document History

Version	**Date**	**Summary of changes**
0.1	04/01/2024	Initial version submitted to IROG for comments.
0.2	05/02/2024	Updates based on IROG feedback to make applicability clearer. Submitted to IROG for sign-off.
0.3	15/02/2024	Clauses 14-17 have been updated based on feedback. Submitted to IROG for sign-off.
1.0	11/03/2024	Approved by IROG.