End User Device Policy

I. Purpose

To mitigate risks and vulnerabilities, individuals are responsible for ensuring that the computers and devices used to access Nested Knowledge services and systems are protected by basic security measures.

II. Scope

This policy affects all employees, contractors, and consultants of Nested Knowledge.

Definitions

End-user device: Any desktop or laptop computer, any tablet, smart phone, or other mobile device is an end-user device. “End-user device” does not include removable storage like USB flash drives.

End-user: A member of the Nested Knowledge workforce who accesses to information technology resources.

III. End-User Device Policy

We require end-user devices to be protected by the security procedures described:

- Access to the device is protected with a password, PIN, or suitable biometric alternative.
- Where practicable, the screen or device locks after an inactivity timeout, and a password, PIN, or suitable biometric alternative is required to unlock it.
- On devices, when available and practicable, application updates, including security updates, are applied at least once every quarter.
- On devices, where available, practicable, and advisable, a firewall is enabled.
- On devices, where available, practicable, and advisable, anti-virus software is installed and automatic check for updates occurs at least weekly.
- Software or apps should not be installed unless the user explicitly trusts the source and knows a legal license exists.
- Employees must comply with software vendor license agreements and copyright holders’ notices. Making unauthorized copies of licensed and copyrighted software, even for evaluation purposes, is strictly forbidden.
- Employees are discouraged from storing client materials on their local machines; instead, files that are not in the production environment should be stored in an encrypted cloud folder.

IV. Anti-Malware Policy

We require Nested Knowledge employees and contractors to run antivirus software on the computers at specified periods. We require employees and contractors to use Malwarebytes to scan and detect malware and ransomware. Positive findings must be reported to the CTO.

Antivirus software installs must be updated (either by updating ruleset or fresh reinstalling) whenever scans are performed.

Schedule

The schedule for scanning is subject to change, but it will not fall below the minimum of twice annually. The schedule will be revised based on the level of threats and size of the company.

Reporting

Positive results in the scan must be reported to one or more members of the Incident Response team. If a virus is detected, all members of the IR team must be notified immediately.

Response

1. The offending applications and files will be uninstalled or removed until the report returns zero results.
2. The incident response team will analyze the malware attack surface and inventory the information that was available on the infected device since last scan.
3. Based on the information available on the infected device, the appropriate Incident Response and Data Protection procedures will be enacted. Information about the threat will be escalated to clients/customers, according to the guidelines in our escalation policy.

Enforcement

Failure to comply with this policy may result in disciplinary actions.

Revision History

Author	Date of Revision/Review	Comments
K. Cowie	12/15/2021	Draft Completed
K. Holub	12/15/2021	Policy approved
K. Kallmes	12/18/2021	Policy approved
P. Olaniran	10/25/2022	Minor revisions

Return to Policies