Endpoint Security Policy

Version 1 - Approved by Youssef Ouyhya

Contents

1. Objective

This policy outlines how CNTXT protects unauthorized access to its production systems or critical data via endpoints like laptops that are used by CNTXT staff members. It also details what should be done if such endpoints are lost, destroyed, or otherwise damaged.

2. Scope

This policy applies to all staff members with endpoint systems that are used to access production systems or critical data within the scope of ISMS at CNTXT.

3. Policy Statement

Securing endpoint devices (like laptops) is paramount to ensuring the Confidentiality, Integrity, and Availability of our customer data. To ensure endpoint security, CNTXT staff should install firmware and software updates, use antivirus software on endpoints with access to critical systems, enable hard disk encryption, use strong passwords (preferably with a password manager), activate auto-screen-lock, report lost or damaged devices, follow removable media guidelines, and comply with periodic reviews and audits.

4. Definitions

- Endpoints: An endpoint is any device that is physically an endpoint on a network. These can include laptops, desktops, mobile phones, tablets, and servers.
- Endpoint Security: Endpoint security is used to protect CNTXT systems when accessed via remote devices such as laptops. Each laptop with the ability to access CNTXT systems can be a potential entry point for security threats

5. Endpoint Security Guidelines

CNTXT staff should take the following steps to ensure the security of the endpoints they use to perform their work:

- CNTXT staff is responsible for installing critical firmware and software updates on the endpoints they use exclusively or those where they’re the assigned owner. All communal assets (like large TVs etc.) should have assigned owners.
- CNTXT requires that all endpoints with access to critical systems like the production infrastructure use antivirus software to protect themselves and our critical systems from malware.
- All CNTXT staff are required to turn on the hard disk encryption option of their respective operating systems (ex: FileVault on Mac).

- As detailed in the password policy, CNTXT staff should use strong passwords to protect against unauthorized access to their system or any services they use. While it is not mandatory, it is recommended to use a password manager.
- All staff must turn on auto-screen-lock on their systems within a reasonable amount of inactive period. While the screen lock will protect your device in most cases, it is recommended that you do not leave your computer unattended and unlocked. The maximum allowed period of inactivity before which screen lock should be activated is recommended to be at 20 minutes.
- Employees must immediately report lost, stolen, or damaged devices to the management, who will then attempt to stop access to critical systems and data through the exposed device.
- Employees must follow the removable media guidelines outlined in Physical Security Policy and Asset Management Policy.
- Endpoints may be verified for compliance with this policy through various methods, including but not limited to periodic reviews, Sprinto App monitoring, and internal and external audits.
- Endpoint security does not require the following:
    - Collect, log, or track personal activity (including website visits or purchases).
    - Remote viewing.
    - Key-logging.

6. Document Security Classification

Company Internal (please refer to the Data Classification policy for details).

7. Non-Compliance

Compliance with this policy shall be verified through various methods, including but not limited to automated reporting, audits, and feedback to the policy owner. Any staff member found to be in violation of this policy may be subject to disciplinary action, up to and including termination of employment or contractual agreement. The disciplinary action shall depend on the extent, intent, and repercussions of the specific violation.

8. Responsibilities

The Information Security Officer is responsible for approving and reviewing policy and related procedures. Supporting functions, departments, and staff members shall be responsible for implementing the relevant sections of the policy in their area of operation.

9. Schedule

This document shall be reviewed annually and whenever significant changes occur in the organization.

End of Endpoint Security Policy. For version history, please see the next page.

Version history

Version	Log	Date
1 Current	Policy version approved by Youssef Ouyhya	26 Oct, 2024
1	New Policy version Created	26 Oct, 2024