Physical & Environmental Security Policy

Version 1 - Approved by Youssef Ouyhya

Contents

1. Objective

The purpose of this policy is to establish the guidelines by which physical and environmental security is managed for ISMS scope systems.

2. Scope

This document is applicable to all processes and operations in CNTXT within the scope of the ISMS.

3. Policy Statement

As a cloud-native company, CNTXT relies on the physical security measures of various cloud service providers, including the infrastructure service provider, to secure and manage production systems and customer data. No production servers or customer data are hosted on-premises. However, office premises are still secured by following guidelines for visitors, clean desks, printing, removable media, shoulder surfing, and compliance with local laws. Remote workers must ensure device security, protect customer data confidentiality, and adhere to information security policies.

4. Physical Security Policy

- CNTXT is a cloud-native company, and all our production infrastructure, including data storage, should be secured and managed by our cloud infrastructure service provider. We must rely on the physical security measures adopted by cloud service providers to ensure the security, availability, and confidentiality of our production systems.
- Further, no production servers or customer data should be hosted within our premises. As a result, the physical security of our office premises is not critical to ensure the security, availability, and confidentiality of customer data.
- Hence the risk has been transferred to the infrastructure provider to ensure the security, availability, and confidentiality of CNTXT's production systems and customer data.
- Physical security of the premises where we work continues to be essential, and the following steps are taken to secure the same:
    - Visitors: CNTXT staff may invite visitors to the office premises for business reasons or during pre-specified times for social reasons. In such cases, the staff members are responsible for the visitor's actions and always need to escort their visitors. As a general principle, do not invite anyone you do not trust or know to the office. CNTXT Staff members who spot unauthorized visitors should either ask the unauthorized person to leave or refer the issue to management.
    - Clean desk: Ensure that no classified customer data, security keys/passwords, etc., are written on whiteboards or unattended notepads, etc.

- Printing: Printing of customer classified data, security keys, passwords, etc., is prohibited.
- Removable media: Use of removable media to transfer sensitive customer data is not allowed on laptops used by CNTXT staff to perform their work.
- Shoulder surfing: CNTXT allows you to work outside the office premises. Should you find yourself working from a public place (like a coffee shop or airport), you should be aware of shoulder surfing.
- Local laws: We must abide by local laws regarding fire safety, display of licenses, etc.

5. Working Remotely

CNTXT Staff who work remotely should follow these rules:

- When working remotely, the security of the device you use to perform your work is your responsibility. For instance, your equipment should be in your presence, screen locked, or be stored securely.
- Please follow the organization’s endpoint protection and encryption standards for any equipment (company provided or otherwise) used to perform your work.
- Protect the confidentiality, security, and privacy of our customers' data by ensuring that unauthorized people may not view, overhear, or otherwise have access to such data. For example, be aware of “shoulder surfing” when working in public places like coffee shops or airports.
- All remote work must be performed in a manner consistent with CNTXT’s information security policies.

6. Document Security Classification

Company Internal (please refer to the Data Classification policy for more 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 is to be reviewed annually and whenever significant changes occur in the organization.

End of Physical & Environmental 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