Vendor Management Procedure

Version 1 - Approved by Youssef Ouyhya

Contents

1. Objective

The objective of this document is to outline the responsibilities and process to be followed while managing relationships with third parties or vendors critical to CNTXT's services.

2. Scope

This document applies to all staff in CNTXT using various vendors whose services are critical to the operational integrity and availability of the services that CNTXT provides to its customers or with whom critical data is shared.

3. Vendor Management Procedure

3.1 Responsibilities

- It is the responsibility of the Information Security Officer, along with all the Business heads, to ensure the following:
    - Identifying all CNTXT vendors/suppliers.
    - Vetting the security controls of third parties before establishing a third-party contract relationship.
    - Ensuring an approved and up-to-date CNTXT vendor/supplier agreement is in place and has been signed by every third party.
    - Maintaining a current and accurate listing of all CNTXT vendors/suppliers.
    - Monitoring third parties for adherence to provisions within vendor/supplier agreements (where applicable), service level agreements (SLAs), and contractual security requirements, as applicable.
    - Performing periodic or continuous reviews of security measures implemented by third-party service providers.
- Business heads must always notify the Information Security Officer whenever they are contracting a new vendor or in case of any changes to services provided by existing vendors.

3.2 Managing Contracts and Service Level Agreements

- Once a vendor has been selected, it is the responsibility of the Business Heads and Information Security officer to ensure that an official contract has been signed between CNTXT and the vendor.
- In the case of using SaaS vendors, subscription-based products may be chosen to carry out business functions, and in such cases, signing contracts is not possible. For all such cases, it is the responsibility of the Information Security Officer to ensure the terms of service published by the vendor are appropriately reviewed.

- The Information Security Officer must ensure that Non-Disclosure Agreements or Confidentiality agreements are in place with vendors who have access to sensitive data. In case this is not possible, the Information Security Officer must review the privacy policy published by such vendors.

3.3 Vendor Risk Management

- The list of vendors must be identified and maintained by the Information Security Officer on a periodic basis. This list must be reviewed at least once a year by the Information Security Officer.
- Each vendor is evaluated based on the following principles:
    - Impact to CNTXT's operations due to unavailability/ breach of vendor services.
    - Vendor's access to CNTXT's sensitive data/ information assets.
- Further, Vendors must be assessed for their suitability based on the following considerations:
    - Do we have a way to contact the vendor when we face any service interruptions or degradation?
    - Does the vendor have any information security certifications like SOC2, ISO27001, etc?
    - Is there sufficient information from the vendor to indicate the security practices they follow?
    - In the absence of the above, does the vendor need to be sent a vendor assessment questionnaire?
    - What are CNTXT's options if the vendor experiences downtime? What happens if the vendor ceases operations suddenly? Are there other potential vendors that CNTXT could work with in such cases?
- Based on the evaluation, the criticality of the vendor services is given below:
    - High
        - Critical services are disrupted
        - The vendor has access to most or all critical data
    - Medium
        - Critical services are functional
        - The vendor has restricted access to critical data
    - Low
        - Minimal impact on critical services
        - Minimal access is provided to the vendor
- Depending upon the business needs and the severity of the risk of data involved, the vendor's certificates or security reports must be collected from the vendor. The Information Security Officer should ensure the validity of these reports.
- For all vendors that carry the highest risk, appropriate due diligence in the form of reviewing their Information security certifications or evaluations through questionnaires is mandatory.

3.4 Vendor Monitoring & Reviews

- The Information Security Officer must review the list of vendors and their criticality at least annually.
- It is the responsibility of the business heads to ensure that they monitor the service being delivered by the vendors. In case of any deficiencies noted, they must inform the Information Security Officer immediately to ensure corrective measures are taken.

4. Document Security Classification

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

5. 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.

6. 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.

7. Schedule

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

End of Vendor Management Procedure. 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