Data Breach Notification Policy

Version 1 - Approved by Youssef Ouyhya

Contents

1. Objective

The objective of this policy is to outline the guidelines and processes for notifying individuals, regulatory authorities, and other relevant stakeholders in the event of a data breach. This policy ensures that appropriate and timely actions are taken to mitigate the impact of a breach, comply with UAE regulatory standards (such as NESA, NCEMA, and Federal Decree-Law No. 45 of 2021 on Personal Data Protection), as well as

international standards such as GDPR and ISO 27001, while safeguarding the privacy and security of affected individuals' data.

2. Scope

This policy applies to all employees, contractors, and third-party service providers who handle personal data or other forms of sensitive information for CNTXT. It encompasses all systems, processes, and technologies, including cloud infrastructure, on-premise environments, and hybrid IT systems.

3. Policy Statement

At CNTXT, we prioritize the security and privacy of the data we collect and manage. If sensitive data (e.g., personal data, protected health information (PHI), or other confidential information) is accessed, used, or disclosed in a way that is not permitted under relevant privacy laws, regulations, or security frameworks, the event will be considered a Data Breach.

Data breach notification procedures are established and reviewed regularly to ensure swift and consistent responses to Information Security Incidents that result in data breaches. These procedures ensure compliance with ISO 27001, NESA, NCEMA, and international regulations.

4. Reporting of Suspected Breach

Any CNTXT employee, contractor, or third-party provider who discovers or suspects a potential data breach must immediately report it to the Information Security Officer (ISO) or the Security Incident Response Team (SIRT).

Failure to report a suspected breach within 24 hours may result in disciplinary action and could be considered a violation of the Federal Decree-Law No. 45 of 2021 in the UAE.

5. Investigation of Suspected Breach

Upon notification, the ISO or designated Security Incident Response Team (SIRT) will launch an investigation into the suspected breach. This investigation must assess:

- Whether the breach occurred and if it was intentional or unintentional.
- The type and extent of sensitive data involved.
- The potential impact on data subjects, customers, and the organization.

Not all incidents constitute a reportable breach. For example, the following scenarios do not require notification:

- Internal Good Faith Handling: Sensitive data accessed by a CNTXT employee in good faith, where there is no further unauthorized disclosure or misuse.
- Internal Disclosures: Sensitive data inadvertently shared between CNTXT employees, with no further unauthorized use.

The ISO must conduct a Risk Assessment to determine if the breach poses a significant risk to the rights and freedoms of data subjects. The risk assessment shall be documented, and any breach involving a high risk of harm will require immediate notification as per the process outlined below.

6. Breach Notification to the Customer and Regulatory Authorities

Timeline for Notification:

In the event of a confirmed data breach, CNTXT will:

- Notify the affected individuals and the competent regulatory authority within 72 hours of becoming aware of the breach, as required under Federal Law No. 45 of 2021 and ISO 27001 standards.
- If notification is delayed beyond the 72-hour timeframe, a written explanation for the delay must be submitted to the relevant authority.

Notification to Affected Individuals:

Where a data breach is likely to result in high risks to the rights and freedoms of affected individuals, CNTXT shall directly notify those individuals without undue delay. The notification must include:

- The nature of the breach.
- Categories and approximate number of affected individuals.
- Mitigating actions taken by CNTXT to address the breach.
- Measures individuals can take to protect themselves from potential harm.
- CNTXT's contact information for further inquiries.

Local and International Regulatory Compliance:

- NESA and NCEMA compliance requires that breaches affecting critical infrastructure or high-level systems must be reported to relevant UAE authorities within 72 hours.

- GDPR Compliance (if applicable to international data): Notifications must also align with GDPR guidelines for breaches involving the personal data of EU citizens.

7. Breach Mitigation

Upon discovering a data breach, CNTXT shall take immediate steps to mitigate the damage, including:

- Data Containment: Isolate compromised systems to prevent further exposure.
- Remediation: Implement security patches or technical measures to address vulnerabilities.
- Data Recovery: Recover lost or compromised data where feasible.
- Communication: Provide clear guidance to affected individuals on how to protect themselves from potential fallout.

The effectiveness of the mitigation steps taken must be evaluated and documented.

8. Document Security Classification

This document is classified as Internal – Confidential under the Data Classification Policy of CNTXT. Any unauthorized access or sharing of this policy will be considered a violation of the company's security policies.

9. Non-Compliance

Compliance with this policy will be monitored through internal audits, automated monitoring systems, and feedback from the ISO and management teams. Any violation of this policy may lead to disciplinary action, including termination of employment or contractual agreement, depending on the severity of the breach.

10. Responsibilities

- Information Security Officer (ISO): Oversees the approval and review of this policy, manages investigations, and ensures compliance with regulatory requirements.
- Security Incident Response Team (SIRT): Assists in investigating and mitigating security incidents and coordinating breach notifications.
- Employees and Contractors: Required to report potential breaches and comply with organizational security policies.

11. Schedule

This policy must be reviewed on an annual basis or whenever significant changes occur within the regulatory environment or the organisation’s technology stack.

Version History

Version	Date	Change Description	Author
1.0	22-Oct-2024	Initial version, updated for UAE compliance (NESA, NCEMA),Updated to align with Federal Decree-Law No. 45 of 2021	Nidhi Goel

Version history

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