Data Breach Response Policy

1. Purpose

The purpose of this Data Breach Response Policy is to establish a clear set of procedures and guidelines for ICT Services Ltd. in the event of a data breach. This policy outlines the steps to be taken to mitigate the impact of a breach, protect the integrity of data, and comply with relevant laws and regulations, particularly those of the European Union (EU)

2. Scope

This policy applies to all employees, contractors, and third-party vendors who have access to ICT Services Ltd.'s systems, networks, and data.

3. Definitions

- Data Breach: An incident where sensitive, protected, or confidential data is accessed, disclosed, altered, or destroyed without authorization, leading to a compromise of data security.
- Personal Data: Any information relating to an identified or identifiable natural person, as defined in the General Data Protection Regulation (GDPR).
- Data Controller: The entity that determines the purposes, conditions, and means of the processing of personal data.
- Data Processor: An entity that processes personal data on behalf of the data controller.
- Data Protection Officer (DPO): A designated individual responsible for overseeing compliance with data protection laws and policies.

4. Reporting a Data Breach

In the event of a suspected or confirmed data breach, employees, contractors, or third-party vendors must immediately report the incident to the designated Data Protection Officer (DPO) or the IT Security team. The report should include the following details:
- Nature of the breach (e.g., unauthorized access, data theft, system compromise).
- Date and time of the breach, if known.
- Description of the affected data (e.g., personal data, financial information).
- Potential impact on individuals and the company.
- Any immediate actions taken to contain the breach.

5. Incident Response Plan

Upon receiving a report of a data breach, the DPO or IT Security team will activate the incident response plan, which includes the following steps:
a. Containment: Take immediate action to contain the breach and prevent further unauthorized access to data or systems. This may involve isolating affected systems, changing passwords, or shutting down compromised services.
b. Assessment: Investigate the scope and severity of the breach, including identifying the types of data compromised, the extent of unauthorized access, and potential vulnerabilities exploited.
c. Notification: If the breach poses a risk to the rights and freedoms of individuals, notify the Data Protection Authority in Malta and affected data subjects without undue delay, in accordance with the requirements of the GDPR.
d. Mitigation: Implement measures to mitigate the impact of the breach, such as restoring data from backups, enhancing security controls, or providing support to affected individuals.
e. Documentation: Maintain detailed records of the breach, including the initial report, investigation findings, remediation actions, and communications with regulatory authorities and affected parties.

6. Communication and Transparency

Throughout the response process, maintain open communication with all relevant stakeholders, including employees, customers, regulatory authorities, and the public, as appropriate. Transparency is essential in building trust and demonstrating accountability for protecting personal data.

7. Compliance and Review

Regularly review and update this Data Breach Response Policy to ensure alignment with changes in technology, regulations, and organizational processes. Conduct periodic training and awareness programs to educate employees about their responsibilities in preventing and responding to data breaches.

8. Enforcement

Failure to comply with this policy may result in disciplinary action, up to and including termination of employment or contract, in accordance with ICT Services Ltd.'s disciplinary procedures and applicable laws.

9. Conclusion

This Data Breach Response Policy is designed to enable ICT Services Ltd. to respond effectively and efficiently to data breaches while upholding the principles of data protection and privacy. All employees, contractors, and third-party vendors are responsible for familiarizing themselves with this policy and adhering to its requirements.

10. Contact Information

Data Protection Authority in Malta:

IDPC

Floor 2, Airways House,
Triq Il-Kbira,
Tas-Sliema SLM 1549, Malta
+356 2328 7100
idpc.info@idpc.org.mt

For questions, concerns, or reporting of data breaches, contact the designated Data Protection Officer (DPO) :

ICT Services Ltd.

228 Constitution street,
Mosta MST9053, Malta
+356 21420881
dpo@ictservices.com.mt

This document was last reviewed on the 11th November 2023