TIP ACADEMY

TELECOM INFRA PROJECT

in collaboration with accenture

TIP Academy Data & Information Security Policy

Version: January 2024

Table of Contents

© Copyright TIP Academy 2023

1. Definitions

Asset – tangible or intangible item of value to the organization and therefore requiring adequate protection. In the context of this document specifically – data and information.

Data – is an economic resource that can be owned and/or controlled and processed, and that holds or produces value. The term 'data' is predominantly used in this Policy and covers both data and information.

Information – is data with meaning. This term is added in the title and in the definitions to mark the wide scope of the Policy covering both data and information and that data shall not be associated only with the concept of data privacy (PII – Personally Identifiable Information).

Data Processing – all operations in relation to data: collecting, storing, ordering, modifying, adapting, uploading, and downloading, sharing, linking, reviewing, using, destroying.

CDP – Client Data Protection.

Data security – securing data, preserving their confidentiality, integrity, and availability (CIA triad).

The Policy – Data and Information Security Policy (this document).

TIP – Telecom Infra Project: the owner of the Organization.

The Organization – TIP Academy: the provider of learning services under TIP Academy brand.

Data Administrator – person administering data in the eLearning Platform.

DPO – Data Privacy Officer in the understanding of GDPR.

ISO 27001 – The International Organization for Standardization norm for Information Security Management System – Requirements.

ISO 22301 – The International Organization for Standardization norm for Security Resilience – Business Continuity Management Systems – Requirements.

© Copyright TIP Academy 2023

2. Goal, Context, Scope, and Applicability

1. The purpose of the Policy is to define effective rules for data protection, regardless of its form, quantity, the method, and place of processing. The scope of the Policy includes both Organization's own data and information provided by customers and business partners.
2. The Management of the Organization understands the importance of data and information security and sets the strategic context and helps in embedding the security posture.
3. The Organization aims to align their security posture with ISO 27001 and its resilience posture with ISO 22301.

3. Risk Approach

1. The implementation of initiatives and projects as well as the launch of new services is preceded by the assessment of risk and the implementation of appropriate control mechanisms. Risk assessment and security requirements foundational to the implementation of security-related activities follow the Deming cycle: Plan, Do, Check, Act.

4. Roles & Responsibilities

1. All Employees and Collaborators are responsible for data security Roles & Responsibilities. The responsibilities of individual organizational units of the Organization are indicated in Specification of Roles and Responsibilities.
2. Duties and responsibilities that pose a risk of conflict (e.g., execution and approval of activities) shall be separated from each other.

5. Asset management

1. The Organization maintains inventory of assets.
2. The level of protection measures applied to protect assets depend on their criticality.
3. Data resources shall have designated owners and be classified and marked according to their importance and criticality to the Organization.
4. Upon termination of the employment/contract, the Employee/Contractor shall return assets belonging to the Organization.
5. The use of devices that do not belong to the Organization (e.g., private computers, mobile devices) is possible only after obtaining the consent of Global Head of Engagement of TIP.

© Copyright TIP Academy 2023

6. Data Classification

1. Data classification is adopted, based on their criticality level designated by the organization. Its requirements define the method of protecting data during its processing, depending on their adopted class, regardless of the form of its recording or transmission and include operations such as: creating, storing, sharing, copying, archiving and deleting/destruction.
2. Employees are obliged to mark data in accordance with its classification and process data using organizational and technical safeguards appropriate to their level of classification.

7. Data Access Management

1. Access rights are granted to Employees and Collaborators in accordance with the principle of 'need-to-know' and 'minimum privileges', to enable work in systems with minimal exposure to threats related to privileged access.
2. Access may be granted only based on the request submitted and approved by the authorized representatives.
3. The system access users shall be required to authenticate by providing unique credentials.

8. Operations security

1. To ensure the expected level of security of computer hardware, software and networks used in the Organization, there are appropriate rules and mechanisms implemented.
2. Production, test, and development environments are separated. Data that require protection based on risk assessment, cannot be processed in test environments.
3. Users are not allowed to make unauthorized modifications to the configuration of the Organization's business equipment, uninstall software installed on company's business equipment and disable anti-virus software.

9. Secure communication

1. The Organization uses cryptographic mechanisms to ensure confidentiality, integrity, and non-repudiation of the processed information.
2. Secure methods of exchanging information with customers and the cryptographic solutions used shall be compliant with applicable security standards.

© Copyright TIP Academy 2023

3. Data stored on workstations, mobile devices and other media shall be cryptographically secured.
4. The rules for using e-mail, the Internet and instant messaging are set out in CDP rules.
5. The CDP rules specify how data is to be protected and transferred, according to its classification level.

10. Acquisition, development, and maintenance of systems

1. The Organization initiatives are analyzed in terms of data security requirements. The results of the analysis shall be considered by introducing appropriate security mechanisms (controls, measures, etc.).
2. Security requirements shall be considered in the process of software development, also in case when it is outsourced.
3. Security mechanisms that are implemented shall be tested.

11. Incident management

1. As a part of Business Continuity Plan the Organization maintains an Incident Management Procedure stating the rules of identifying incidents, responding to them, and handling them.
2. The aim of incident management process is to minimize the negative consequences of the incident in relation to the Organization's business processes.
3. The Organization's Incident Management is performed with Asset Owner's supervision and participation.
4. An incident regarding the security and privacy of personal data (PII) is recorded in the designated security incident registers. The process of its management and handling (including recording, reporting, and processing - including contact with the authorities/supervisory authorities) is handled by the Data Protection Officer (DPO).
5. Incidents that may affect business continuity or lead to a crisis shall be immediately reported to the persons designated to act in crisis situations, indicated in the Business Continuity Plan.

12. Business Continuity Management

1. Business Continuity Management (BCM) is a priority in the context of data security.
2. BCM help prioritize assets and therefore expenditures to protect them.

© Copyright TIP Academy 2023

3. The Organization aims to align its business continuity posture with ISO 22301.
4. The Organization's Business Continuity is governed by a separate Business Continuity Policy.

13. Physical and environmental security

1. Physical Security embraces human safety and physical asset security.
2. Human safety is of utmost importance to the Organization and protecting human life and health takes precedence over protecting any other asset of the Organization. The Organization follows the applicable Health and Safety and CDP rules and regulations adopted by law and choice.
3. Areas where data that need to be protected are processed shall be protected against unauthorized physical access.

14. Supplier relationship

1. The Organization's cooperation with third parties (partners, as well as other entities and institutions - including their employees and collaborators) shall be in accordance with the principles set out in the CDP plan.
2. Third parties who have access to other than public data, must sign a confidentiality agreement before data processing begins.
3. Contracts with third parties shall include provisions to ensure the security of the Organization's information.
4. Procurement is responsible for fulfilling the obligations ensuring information security in relations with third parties.
5. The Organization declares cooperation with institutions, authorities, regulatory bodies, in particular in the event of detecting information security incidents that may be related to criminal activity.

15. Compliance

1. The Organization acts in accordance with this Policy, internal regulations, as well as contractual provisions with clients and legal and regulatory requirements.
2. Compliance with this Information Security Policy is periodically verified through internal and third-party audits.
3. The initiator of a project, change, purchase, or contract shall identify contractual and external requirements at the stage of starting the initiative and, in consultation with the Global Head of Engagement of TIP and the legal department, determine whether they are consistent

© Copyright TIP Academy 2023

with this Policy, legal requirements, and whether the current state of information security allows them to be met.

4. The Data Protection Officer with the support of lawyers serving the Organization is responsible for managing personal data protection processes.

16. Exceptions management

1. All deviations from the provisions included in this Policy shall be documented and reported by the Owners of the assets to which the deviations apply. The consent of the Global Head of Engagement of TIP shall be formally obtained for each deviation.
2. All deviations shall be treated as risks and handled in accordance with the process described in the Business Impact Analysis.

© Copyright TIP Academy 2023