Classification and Security Policies for Twauiq Academy

Ruba A. Almuhya, Mariam M. Albenyan, Shouq Almutairi, Manar Alahaimid, Rand Almajmaj

The Institutional Affiliation of SDAIA and NDMO

Abstract

This document describes the data classification and security policies and procedures for Twauiq Academy. It includes controls and defines the data governance operating model.Twauiq Academy classifies data into three categories: public, secrt and restricted. It has implemented a number of security policies and procedures to protect its data, including access control, data encryption, auditing, and incident response.

Introduction

The purpose of this project is to develop a comprehensive data classification and security policies and procedures document for Twauiq Academy. In today's digital landscape, data security is of utmost importance, and educational institutions like Twauiq Academy need robust measures in place to protect sensitive information. This document will outline the necessary controls, guidelines, and best practices to ensure the confidentiality, integrity, and availability of data within the academy's systems.

Definition

Data classification refers to the process of categorizing data based on its sensitivity, importance, and potential impact. It involves assigning appropriate levels of protection and access controls to different types of data. Security policies and procedures, on the other hand, are a set of guidelines and rules that define how data should be handled, stored, accessed, and protected within an organization. These policies and procedures provide a framework for data security practices and help mitigate risks associated with unauthorized access, data breaches, and other security threats.

Goals

The primary goals of this project are:

- Establish a Data Classification Framework:

  Develop a systematic approach to classify data based on its sensitivity and criticality. This framework will help identify and prioritize data assets for appropriate security controls.

- Define Security Policies and Procedures:

  Create a set of comprehensive security policies and procedures that outline the acceptable use, handling, and protection of data within Twauiq Academy.

Data Classification Policy and Procedure:

Policy Statement:

Twauiq Academy recognizes the importance of data as a valuable asset and is committed to ensuring the appropriate handling, protection, and classification of all data assets to maintain their confidentiality, integrity, and availability. This policy defines the data classification framework and procedures for managing and securing data within the organization.

Purpose:

The purpose of this policy is to:

- Establish a data classification framework to categorize data based on its sensitivity and criticality.
- Define data ownership and the roles and responsibilities of data stewards and data custodians.
- Ensure the appropriate protection and handling of data assets.
- Facilitate compliance with relevant data protection laws and regulations.

Scope:

This policy applies to all data assets owned, processed, or stored by Twauiq Academy, including but not limited to electronic and physical records, documents, databases, and any other data-related resources.

Data Classifications Levels:

Classification Level	Description
Secret	Data shall be classified as “Secret” if unauthorized access to or disclosure of such data or its content has a serious effect on the following: - National interests such as partial damage to the reputation of the Kingdom, diplomatic relations, operational efficiency of the security or military operations, national economy, national infrastructure or government functions; - Financial loss for organizations, leading to bankruptcy or to inability of the entities to perform their duties or major loss for competitive abilities or a combination thereof; - Significant harm or injury to the life of individuals; - Long-term damage to the environmental or natural resources; - Investigation of major cases, as defined by law, such as terrorism funding.
Public	Data shall be classified as “Public” if unauthorized access to or disclosure of such data or its content has none of the abovementioned impacts, particularly effects on: - National Interest; - Activities of entities; - Interests of individuals; - Environmental resources.
Restricted	Data shall be classified as “Restricted” if unauthorized access to or disclosure of such data or its content causes: - Limited negative effect on the functioning of public entities or economic activities in the Kingdom or on a particular individual’s business; - Limited damage to any entity’s assets and limited loss to its financial and competitive status; - Limited, short-term damage to environmental or natural resources.

Business Glossary

Business Term	Business Definition
Name	Name of Students and employees.
ID	Unique number to identify each student and employee.
Nationality	nationality of each student and employee.
University	Identify the name of the university the student is attending.
Major	describe the student's area of study or major.
Graduation Date	Identify the date of the student's graduation.
Date of Birth	Identify the date of birth of the student.
Email	Identify the email address of the student.
Phone number	Identify the phone number of the student.
Gender	Identify the gender of the students and employees.
Address	Identify the address of the student.
Department	Identify department or division the employee belongs to.
Joining Date	Identifythe date when the employee joined the organization.
Salary	Identify the salary of the employee.
Job Type	Identify the type or category of the employee's job.
Number of Students	Identify the count of students enrolled in a program.
Program Level	Identify the level or degree of the program (e.g., undergraduate, graduate).
Program Type	Identify the type or category of the program.
Program Duration	Identify the duration of the program in a numeric value (e.g., number of months or years).

Data Classifications Framework

X

Role and Responsibility (RACI)

- Data Owner:
    - Data owners are responsible for defining the classification and access controls of their data assets.
    - They ensure data is handled in accordance with this policy.
- Data Custodian:
    - Data custodians implement technical controls to protect data assets.
    - They are responsible for encryption, access controls, and other security measures.
- Data User:
    - Data users are responsible for complying with data security policies and procedures.
    - They access and handle data based on their job responsibilities and authorized access levels.

Role/Responsibility	Data Owner	Data Custodian	Data User
Define and classify data, and determine access controls	Responsible		
Ensure data processing aligns with defined policies	Responsible		
Implement technical controls to protect data		Custodian	
Comply with data security policies and procedures			User
Access and handle data based on job responsibilities and authorized access levels			User

Data Security Policy

A data security policy is a set of guidelines and procedures that outline how an organization protects its data assets from unauthorized access, use, disclosure, alteration, or destruction. It establishes the framework for ensuring the confidentiality, integrity, and availability of data throughout its lifecycle.

Policy:

- Policy Statement:
  - The organization is committed to maintaining the security and confidentiality of its data assets.
  - All employees and contractors are responsible for protecting data from unauthorized access, disclosure, alteration, or destruction.
- Data Classification:
  - Data will be classified based on its sensitivity and criticality.
  - Classification levels will include secret, public and restricted.
  - Access controls and security measures will be applied based on the data classification.
- Access Controls:
  - Access to data will be granted on a need-to-know basis.
  - User access will be authenticated through secure login credentials.
  - Access rights will be reviewed and revoked when no longer necessary.
- Data Storage and Retention:
  - Data will be stored on secure servers with appropriate access controls.
  - Backup procedures will be established to ensure data recoverability in case of system failure or data loss.
  - Data retention periods will be defined and followed in compliance with legal and regulatory requirements.

- Incident Response:
    - An incident response plan will be developed and regularly tested.
    - Security incidents, data breaches, or unauthorized access will be reported promptly.
    - Appropriate measures will be taken to mitigate the impact of incidents and prevent future occurrences.

Procedure:

- Data Access and Authorization:

Access privileges will be granted based on job responsibilities and data classification.

- Data Backup and Recovery:

Regular backups will be performed to ensure data availability and recovery in case of system failure or data loss.

- Physical Security:

Physical access to data storage facilities will be restricted to authorized personnel.

- Security Awareness and Training:

Employees will receive training on data security policies and procedures.

- Incident Reporting and Handling:

Employees will be educated on the process of reporting security incidents or suspicious activities.

Security Awareness Training

All personnel will undergo regular security awareness training to stay informed about data security best practices and potential threats.

Compliance

Twauiq Academy is committed to complying with all relevant data protection laws and regulations.

Review and Revision

This Data Security Policy will be reviewed regularly and updated as necessary to reflect changes in technology, business requirements, and regulations.

References

Include references to relevant laws, regulations, and standards that impact data security at Twauiq Academy.

Compliance Policy

Employees will be educated on the process of reporting security incidents or suspicious activities.

Review and revision Policy

This Data Classification Policy and Procedures document will be reviewed periodically to ensure its effectiveness and alignment with changing business needs, technology advancements, and regulatory requirements.

Tools and Technologies:

The project leverages various tools and technologies to facilitate development and enhance its functionality. The key tools and technologies used in this project include:

1. OpenMetadata Tool: OpenMetadata is an open-source metadata management tool that aids in organizing, documenting, and discovering metadata across various data sources and systems. It provides a centralized repository for storing and managing metadata, enabling efficient data governance and facilitating collaboration among team members.
2. Postgres: Postgres, short for PostgreSQL, is a powerful and feature-rich open-source relational database management system (RDBMS). It is known for its reliability, scalability, and extensive support for SQL standards. Postgres is widely adopted for its ability to handle large volumes of data, support complex queries, and provide advanced data management functionalities.

These tools and technologies are carefully chosen to enhance the project's development process, streamline metadata management, and ensure efficient data storage and retrieval. By leveraging the OpenMetadata tool and utilizing Postgres as the RDBMS, the project can benefit from robust metadata management capabilities and a reliable database infrastructure.

References