

VIA University College
Software Technology Engineering

Security Policy - Learnify

Semester Project - Group 3
3rd Semester

December 15, 2025

Date: 2025-12-15

Version: 1.5

1 Introduction

This document outlines the security policy for **Learnify** within **SEP3**. The system is an e-learning platform and requires appropriate security measures to protect data, ensure proper access control, and maintain system availability.

2 Purpose

The purpose of this policy is to define the necessary security measures to protect **Learnify** from unauthorized access, data breaches, disruptions, or misuse. These measures ensure the **confidentiality, integrity, and availability** of the system.

3 Scope

This policy applies to all users, administrators, contractors, and third-party service providers who access or interact with **Learnify**.

4 Roles and Responsibilities

Product Owner: Responsible for ensuring the system operates securely and this policy is implemented to the extent feasible.

System Administrators: Responsible for maintenance, patching, account management, and monitoring.

Users: Responsible for adhering to the policy and reporting suspicious activity.

5 Access Control

5.1 User Authentication

All users must authenticate using a unique username and password.

Requirement:

- Strong passwords (min 8 chars) required. MFA recommended for admins. **Rotation:** Passwords should be changed every 180 days.

5.2 Role-Based Access Control (RBAC)

Access permissions are assigned based on the user's roles.

Requirement:

- Simple RBAC with regular access reviews.

5.3 Account Management

Inactive Accounts:

- Accounts will not be disabled automatically but will be a subject to periodic review.
- Roles removed immediately after administrator or teacher exit.

6 Data Protection

6.1 Data Classification

Data is classified into categories - Public, Internal, and Sensitive.

Requirement:

- Internal data must be protected; Sensitive data requires encryption.

6.2 Data Encryption

Requirement:

- Encrypt in transit (HTTPS); rest encryption optional.

6.3 Data Backup

Requirement:

- Weekly backups. Retention: 30 days.

6.4 Data Retention

Requirement:

- Retain and dispose of data per legal requirements.

7 System Security

7.1 Patch Management

Critical Patches:

- Apply within 24-48 hours.

7.2 Firewall and Network Security

Requirement:

- Firewall with IDS/IPS and regular monitoring.

7.3 Antivirus and Malware Protection

Requirement:

- Automatically updated antivirus and anti-malware on all systems.

7.4 Physical Security

Requirement:

- Secure server locations with restricted access. (outsourced to cloud provider)

8 Monitoring and Logging

8.1 User Activity Logging

Requirement:

- Basic logging. Retain 90 days.

8.2 System Monitoring

Requirement:

- Monthly review of basic metrics.

8.3 Audit

Requirement:

- Annual security audit or after major changes.

9 Incident Response

9.1 Reporting

All users must report suspected incidents within 24 hours.

9.2 Incident Response Plan

Requirement:

- Basic procedures (identify, notify, restore).

9.3 Data Breach Notification

Requirement:

- Internal notification; external as legally required.

10 Disaster Recovery and Business Continuity

10.1 Disaster Recovery Plan (DRP)

Target Restoration:

- Within 14 days unless critical or legally mandated.

10.2 Business Continuity

Requirement:

- Redundancy to minimize downtime.

11 Compliance and Training

11.1 Regulatory Compliance

Requirement:

- Basic legal compliance based on the system's operational regions.

11.2 User Training

Frequency:

- Onboarding as needed; periodic optional refreshers.

12 Policy Review and Approval

This policy will be reviewed **quarterly** or upon significant system changes.

Last Reviewed: 2025-12-15

Approved By: Eduard Fekete

Next Review Date: 2026-03-15

13 Glossary

- **MFA:** Multi-Factor Authentication
- **RBAC:** Role-Based Access Control
- **IDS/IPS:** Intrusion Detection/Prevention System
- **DRP:** Disaster Recovery Plan
- **HTTPS:** Hypertext Transfer Protocol Secure