YouTestMe

YTM System Access Policies

Table of Contents

1 Introduction

The purpose of this document is to outline the access control measures and procedures for the examination and learning software provided by YouTestMe. The system access control is designed to ensure the confidentiality, integrity, and availability of the software and its associated data. This document provides an overview of user roles, access levels, and the processes for granting and revoking system access.

2 System Overview

The examination and learning software provided by YouTestMe is a comprehensive platform designed to facilitate examination management and online learning. It includes features for creating and administering exams, delivering educational content, and tracking student progress. The software is hosted and maintained by YouTestMe to ensure optimal performance, security, and data protection.

3 User Roles and Responsibilities

The following user roles and their associated responsibilities have been defined:
a. System Administrator:
- Responsible for the overall management and administration of the system.
- Granting and revoking access rights.

- Configuring system settings and performing system maintenance tasks.
- Responsible for defining data access levels and permissions.
- Ensuring data integrity and accuracy.
- Approving access requests for their specific data sets.

c. Support Access:

- Individuals who require access to the system to provide technical support and assistance to clients.
- Limited to application access in accordance with the client's level of agreement.
- Adhering to the system's security policies and procedures.
- Protecting their login credentials and reporting any suspicious activity.

4 Access Control Procedures

The following procedures will be followed for granting and revoking system access:

1. Access Request:

Users must submit an access request form to their respective supervisor or system administrator.

The form should include the user's name, job title, department, reason for access, and the level of access required.

The supervisor or system administrator will review and approve access requests based on the principle of least privilege.

2. User Provisioning:

Upon approval of the access request, the system administrator will create a user account for the user.

User accounts will be assigned appropriate access levels and privileges based on the approved request.

3. Access Review:

Periodic access reviews will be conducted to ensure that user access is still necessary and appropriate.

System administrators will review user access and make adjustments as required.

4. Access Revocation:

When an employee leaves the organization or changes job roles, their access rights will be promptly revoked.

Access revocation will be performed by the system administrator or the user's supervisor.

5 Remote Access Policy

This addendum applies to all employees, contractors, and third-party vendors who require remote access to company resources. It emphasizes the use of company-provided computers and VPN connections to ensure a secure and controlled remote access environment.

5.1 Remote Access Methods

Remote access to company resources is only permitted through company computers provided to employees.
Remote access must be established using the Office VPN or other VPN connections provided within the company network.

5.2 Security Requirements

All remote access connections must be secured using company-approved VPN solutions that provide encryption and secure tunneling.
Users must connect to the company network via the designated VPN entry points provided by the system administrators.
Virtual private networks (VPNs) must be configured to enforce strong authentication, encryption, and integrity controls.

5.3 Endpoint Security

Company-provided computers used for remote access must comply with the company's endpoint security policies, including up-to-date antivirus software, host-based firewalls, and security patches.
Users must ensure that their company computers are protected against unauthorized physical access and properly secured when not in use.

5.4 User Authentication and Access Control

Users accessing company resources remotely must use their designated company computer and login credentials.
Passwords for company computers and VPN accounts must adhere to the company's password policy, including complexity requirements and regular password changes.
Remote access privileges must be promptly revoked when an employee leaves the company or no longer requires remote access.

5.5 Prohibited Activities

Remote access users must not attempt to use personal devices or computers that are not provided by the company for remote access purposes.
Users are prohibited from sharing their VPN credentials or allowing others to use their remote access privileges.
Users must not attempt to bypass or disable security controls or engage in any activity that could compromise the security of company resources.

6 Security Measures

To enhance the security of the examination and learning software, the following measures will be implemented:
1. Strong Password Policy:

Users will be required to create strong passwords.
Passwords must be regularly changed, and password reuse will not be allowed.

2. Audit Logs:
   System access and activity will be logged and monitored.
   Logs will be regularly reviewed.