YouTestMe

YTM Security Policies

Table of Contents

1 Introduction

List of policies that has to provide rules and guidelines to be followed by people accessing company IT resources. Policies can help improve an organization’s overall security posture. This program defines baseline control measures in a program of information security everyone who connects to the YouTestMe network is expected to be familiar with and consistently follow.

2 General Policies

This chapter is covering policies for using company networks, computers, documentation, etc.

2.1 Company computers

Computers are provided with a predefined user with local privileges (non-administrator). Members don't have permission to access administrative account
Programs required for work are preinstalled. Additional programs could be requested from the system administrator but not installed by any other member.
Company laptops should be connected only to safe, known networks. VPN is required n case of using them on unknown public networks (parks, coffees, conferences, etc.)

2.2 Antivirus

Company computers come with antivirus software preinstalled.
Member using the computer must run a full system scan once a week and commit a scan report.
The antivirus program had to be on the last update and active all the time

2.3 Password Policies

Passwords are stored and shared using the password manager application
Passwords could not be shared using chat, emails, and similar communication systems
Passwords could not be saved on paper or text files

2.4 Remote Access

Remote access to the office network is done using exclusively by SSH tunneling and VPN
Every member uses his personal access accounts. Personal accounts couldn't be shared between members.

2.4.1 SSH Access

The password should be complex and 16 characters long (minimal)
Minimum one uppercase and lowercase and minimum one special character
The password is forcibly changed every three months
If it is not used for more than two months, the password expires, and the user is locked
SSH access is provided only for networks that members have permission to access

2.4.2 Database Access

The password should be complex, random, and 16 characters long (at a minimum).
There should be a minimum of two uppercase and two lowercase letters in the password.
There should also be a minimum of two special characters in the password.
Access to the database is restricted to administrators only.
The access to the database can be done locally, combined with SSH proxy access.

3 Production Security Policies

3.1 Access Roles

Access to clients' data, applications, and servers is defined for different company roles. Existing roles are:

- Support – has minimum access privileges to the client's application and servers to help the client with occurring issues.
- Developer – limited data access. The role is to use scrambled data to protect PII.
- System Administrator – has unlimited access to all properties. This role is used when it is required in tasks such as an upgrade, migration, etc. Lower access roles are used in any other case.

3.2 Production Data

3.2.1 Database Backup

Backup is stored in multiple locations. Access is limited by policies: to the System Administration role and limited:

Backup files are accessible only from the company office network.
Backup files are encrypted
Files are manipulated using secure protocols SCP or SFTP
Files are used in cases of migration, disaster recovery, and testing fixes(scrambled)

3.2.2 Scrambling Data

Scrambling data has to remove PII, access to third-party services, exam questions, results, training courses, etc. It is applied to:

User information
Mail Server
SSO access
Webex access

3.3 Production Server Access

Production servers are located in the network separated from the office networks.
Servers are accessible only from the office network and company servers. Access from other locations is done by using an office VPN or by tunneling to an office proxy

3.3.1 VM Access

VM (Virtual Machines) access defines accessibility to the proxy, application, database, and backup servers.

Support access

Access is done by using SSH with the personal account on the proxy server. Personal user has only access permission. It is used for tunneling to other VMs.

Support roles have minimum privileges:

Checking active services
Reading log files
Monitoring server load

System Administration roles have full access to servers. These roles are used only in cases of:

Disaster recovery
Upgrade
Maintenance

3.3.2 Database Access

Polices defining access to the database in production. Access to databases is given only to the System Administration role:

Use read-only database roles to access limited parts of the database. Only tables with parameters and other system-relevant data are accessible

Use predefined scripts for accessing data. This measure is required to reduce the risk of corrupting data in the database

Changing database is allowed only with scripts that are tested and approved by the development department

4 Development Policies

Code or a significant part of it could not be shared with people out of the company
Coders have to follow all standard rules from YouTestMe Developer Manual
Code must be scanned with automated tools and comply with OWASP tests. Every issue found has to be resolved to release the new version of the application
Software used to deploy, host and test application must be continuously followed for changes, patched, and updated

5 Encryption in transit

SSL/TLS uses both asymmetric and symmetric encryption to protect the confidentiality and integrity of data in transit. Asymmetric encryption is used to establish a secure session between a client and a server, while symmetric encryption is used to exchange data within the secured session.
Transport Layer Security (TLS) is the successor protocol to SSL. TLS is an improved version of SSL. It works in much the same way as SSL, using encryption to protect the transfer of data and information. The two terms are often used interchangeably in the industry, although SSL is still widely used.
YouTestMe is using certificates provided by the domain provider and enforcing the latest TLS version.
HTTP access is the only available access point to the application over the public network.