Student Name: Abdurrehman Syed
Student ID: 2308546

Task 1

In order to protect myself from cyber attacks I have used different passwords for different accounts. The websites or logins I use frequently have two-factor authentication enabled for them. Additionally, I try to keep my firewall, browser and such softwares up to date to minimize the risk and avoid going to fishy websites and clicking on links or ads especially on social media.

I have never been a victim myself of cyber crime since I take the necessary measures to protect myself. But I would suggest that one should have necessary files already backed up so that even if you're attacked you dont lose anything. Stay vigilant and assume everything to be a scam on the first sight (kinda works).

Task 2

Password Policy

1. Issue Statement

This policy addresses the security concerns about passwords that are used across the company's systems and accounts. It is intended to ensure that all staff adopt good password creation, storage, and management practices in order to minimize the risk of sensitive data being accessed without authorization.

2. Organization Statement

All staff are required to create and manage secure passwords for all accounts with the company and/or with any system for which they have access. Poor passwords, password proliferation, and poor password management leave the Company vulnerable to numerous cyber security threats. These range from account compromise to data breach incidents, therefore, forcing the need for this policy to ensure strong and unique password usage for all accounts, together with MFA.

3. Applicability

It targets all employees who access the systems or applications of the company, whether it be email, cloud platforms, database, or any other work-related system.

4. Roles and Responsibilities

Employees: They shall create and manage strong passwords based on the requirements of the policy. In any suspicious activity or compromise, employees should immediately report to the IT department.

IT Department: This department is responsible for ensuring the enforcement of the password policies, supporting any password-related issues, and providing automated tools for detecting weak passwords. The IT department will also assist in password resets.

5. Compliance

Non-compliance with this policy may result in warnings and, in repeated incidences, will lead to disciplinary action. The actions may range from temporary withdrawal of access to specific systems, compulsive password training to even more severe measures depending upon the nature of the offense. All Employees are to change their passwords every 90 days. Failure to do so shall, by default, result in account lockout until passwords are updated.

6. Points of Contact

Employees must consult the IT Department or immediate supervisor for any questions about this policy. The IT helpdesk is always ready to address password recoveries and account access problems.

BYOD Policy: Bring Your Own Device

Problem Statement

A policy to deal with personal devices (such as smartphones, tablets, and laptops) in connection with work-related activities; usage of personal devices connected to the network and data of the company has to be done in a secure and responsible manner, reducing the risks of data breaches, malware, and unauthorized accesses.

Organization Statement

The organization authorizes the utilization of a personal device for official purposes once the following are met. All personnel are expected to exercise the security measures outlined in this policy to prevent the divulgence of sensitive company data. Noncompliance with the guidelines set in this policy could lead to security vulnerabilities and the potential for unauthorized access to company resources.

Applicability

This policy applies to all employees who use personal devices to access company resources such as email, cloud platforms, databases, and network services.

Roles and Responsibilities

Employees: Ensure all personal devices maintain the minimum security requirements as specified within this policy, including antivirus software, encryption, and device lock mechanisms.

Report any device loss or theft to the IT department without any delay to avoid potential associated risks.

Allow remote monitoring and management of the device in case of incidents involving security or unauthorized access of the device.

IT Department: Provide technical assistance for securing the personal devices. Device Connected to the company network will be monitored; there shall be enforcement of security patches and updates.

Security Requirements

All devices must be password-protected, encrypted, and updated to their latest operating system and security patches. Staff will access company systems using MFA. Malware prevention and unauthorized access shall be installed with the security software approved by the Company.

Compliance

Failure to follow this policy can result in immediate revocation of access to information systems and data. Repeated violations will be subject to disciplinary action, such as termination of employment, depending on the severity.

Data Privacy

The company is committed to the privacy of employees' personal information. Monitoring of devices will be limited to work-related functions, and personal information will not be accessed or monitored by the IT department.

Contact Points

Also, employees should not hesitate to contact the IT Department or their immediate supervisor if they have questions or concerns regarding the BYOD policy.

Note: I took help from AI with formatting and some ideas.