

# Exercise: Initial protective measures

## Introduction

So far, you've learned about the importance of securing physical machines and user data within a business enterprise, as well as various encryption methods that can be used to protect sensitive information.

Businesses face a growing number of cyber threats that can jeopardize their sensitive data and operations. It is essential for companies to regularly assess and update their security policies, infrastructure, and physical machines to ensure they are protected. In this activity, you will apply your knowledge by determining the initial protective measures required to secure Sam's physical machines and user data.

By completing this activity, you'll be able to assess a business's security needs and recommend suitable protective measures.

## How to complete this exercise

To complete this exercise, you will need access to Microsoft Word. If you do not have the Microsoft Word application, you can use [Free Office for the web](#). This version of Office allows you to view and edit files in apps like Word, Excel, and PowerPoint. This free service is available to anyone with a Microsoft account.

## Scenario

Imagine yourself as a cybersecurity consultant for Sam's Scoops. Your role involves evaluating the company's current security infrastructure and identifying vulnerabilities.

Let's say that during your assessment of Sam's business security infrastructure, you discovered several areas where improvements are necessary:

### Security policies

- The existing password policy requires employees to create passwords with a minimum length of only six characters. Additionally, periodic password changes are not enforced.
- There is no policy in place for regularly backing up data or recovering lost data in case of a disaster or system failure.
- The enforcement of access controls is inconsistent, allowing some employees to access sensitive information without proper authorization.

### Infrastructure

- Sam's Scoops uses outdated operating systems that are no longer supported by the manufacturer.
- Firewalls are not properly configured or maintained, leaving the network susceptible to cyber-attacks.
- The current system relies solely on usernames and passwords for access, lacking strong authentication methods.

### Physical machines

- The physical machines within the company are not adequately secured.
- Remote access to physical machines lacks proper security measures.

Now, your task is to recommend initial protective measures based on your findings to secure Sam's Scoops physical machines and user data.

## Instructions

Based on your findings from the scenario, create a comprehensive security plan that includes recommended protective measures for the following areas:

- Security policies: Provide recommendations to strengthen the password policy, establish a data backup and recovery plan, and enforce consistent access controls.
- Infrastructure: Outline measures to address the use of outdated operating systems, improve firewall configuration and maintenance, and enhance authentication methods.
- Physical machines: Recommend security measures to secure physical machines and secure remote access.

Ensure that the recommended measures are justified and supported by the potential benefits it offers to Sam's Scoops, considering the protection of sensitive data and operations.

## Conclusion

The review of Sam's Scoops' current security policies, infrastructure, and physical machines reveals several vulnerabilities that pose risks to the company's sensitive data and operations. The exercise provides an opportunity to develop a comprehensive security plan that addresses these vulnerabilities and recommends protective measures to mitigate potential risks. By implementing the recommended measures, Sam's Scoops can significantly enhance its security posture and protect against potential threats.