**Cyber Security Policy Review Report**

James Kuzhilaparambil

Contents

[Executive Summary 3](#_heading=h.gjdgxs)

[Introduction 3](#_heading=h.30j0zll)

[Basic Cyber Security Concepts 3](#_heading=h.1fob9te)

[Common Cyber Security Threats 3](#_heading=h.3znysh7)

[Recommended Cyber Security Practices 4](#_heading=h.2et92p0)

[Strong Passwords 4](#_heading=h.tyjcwt)

[Password Expiration Policy 4](#_heading=h.3dy6vkm)

[Multi-Factor Authentication (MFA) 4](#_heading=h.1t3h5sf)

[Secure Email with Personal Certificate 4](#_heading=h.4d34og8)

[VPN IPSec on Laptops 4](#_heading=h.2s8eyo1)

[Encrypted Hard Drives/Flash Disks 4](#_heading=h.17dp8vu)

[Implementation and Monitoring 5](#_heading=h.3rdcrjn)

[Conclusion 5](#_heading=h.26in1rg)

[References 5](#_heading=h.lnxbz9)

## Executive Summary

This report provides a comprehensive review of the company’s Cyber Security policy, focusing on essential security approaches and practices to protect employees, information, and resources. As the new Cyber Security manager, the goal is to ensure robust protection against potential breaches by implementing strong passwords, a password expiration policy, Multi-Factor Authentication (MFA), secure email with personal certificates, VPN IPSec on laptops, and encrypted hard drives/flash disks. This report is designed to be understood by both technical and non-technical readers, ensuring a unified approach to Cyber Security across the organization.

## Introduction

* **Purpose**: To review and explain the company’s Cyber Security policy, focusing on basic concepts and practices to protect users and information.
* **Scope**: This report will cover essential Cyber Security principles, common threats, and recommended practices for employees and tech teams.

## Basic Cyber Security Concepts

* **Confidentiality**: Ensuring that sensitive information is accessible only to those authorized to have access.
* **Integrity**: Protecting information from being altered by unauthorized parties.
* **Availability**: Ensuring that information and resources are available to authorized users when needed.
* **Authentication**: Verifying the identity of users before granting access to systems and data.
* **Authorization**: Granting permissions to users based on their roles and responsibilities.
* **Non-repudiation**: Ensuring that actions or transactions cannot be denied after they have been performed.

## Common Cyber Security Threats

* **Phishing**: Deceptive attempts to obtain sensitive information by pretending to be a trustworthy entity.
* **Malware**: Malicious software designed to damage, disrupt, or gain unauthorized access to computer systems.
* **Ransomware**: A type of malware that encrypts data and demands payment for its release.
* **Social Engineering**: Manipulating individuals into divulging confidential information.

## Recommended Cyber Security Practices

### Strong Passwords

* **Explanation**: Strong passwords are essential for protecting user accounts from unauthorized access. A strong password typically includes a mix of uppercase and lowercase letters, numbers, and special characters.
* **Implementation**: Encourage employees to create complex passwords and use password managers to store them securely.

### Password Expiration Policy

* **Explanation**: Regularly changing passwords reduces the risk of compromised credentials being used over a long period.
* **Implementation**: Set a policy requiring employees to change their passwords every 60-90 days.

### Multi-Factor Authentication (MFA)

* **Explanation**: MFA adds an extra layer of security by requiring multiple forms of verification, such as a password and a one-time code sent to a mobile device.
* **Implementation**: Implement MFA for all critical systems and applications to enhance security.

### Secure Email with Personal Certificate

* **Explanation**: Using personal certificates to encrypt and digitally sign emails ensures the authenticity and confidentiality of communications.
* **Implementation**: Provide employees with personal certificates and train them on how to use them for secure email communication.

### VPN IPSec on Laptops

* **Explanation**: VPN IPSec creates secure, encrypted connections for remote access, protecting data transmitted over public networks.
* **Implementation**: Require employees to use VPN IPSec when accessing company resources remotely.

### Encrypted Hard Drives/Flash Disks

* **Explanation**: Encrypting portable and mobile devices protects sensitive data in case of loss or theft.
* **Implementation**: Mandate the use of encryption software for all company-issued laptops and portable storage devices.

## Implementation and Monitoring

* **Policy Enforcement**: Ensure that all employees adhere to the Cyber Security policy.
* **Regular Audits**: Conduct regular security audits to identify and address vulnerabilities.
* **Incident Response Plan**: Develop and maintain an incident response plan to quickly address and mitigate security breaches.

## Conclusion

In summary, Cyber Security is crucial for protecting the company’s information and infrastructure from potential threats. Implementing strong passwords, a password expiration policy, Multi-Factor Authentication (MFA), secure email with personal certificates, VPN IPSec on laptops, and encrypted hard drives/flash disks are key practices that enhance security. These measures help ensure confidentiality, integrity, and availability of data, safeguarding the company against cyber-attacks.

As a call to action, it is essential for all employees and tech teams to remain vigilant and proactive in maintaining Cyber Security. Continuous education, adherence to policies, and prompt response to incidents are vital in creating a secure environment. Together, we can protect our company’s assets and maintain a robust Cyber Security posture.

## References

*Cyber Security Training | SANS courses, certifications & research*. (n.d.). https://www.sans.org/?ref=195285

*Department of Home Affairs website*. (n.d.). Department of Home Affairs Website. https://www.homeaffairs.gov.au/about-us/our-portfolios/cyber-security/strategy

*Enhancing the cybersecurity workforce*. (2011, February 1). IEEE Journals & Magazine | IEEE Xplore. https://ieeexplore.ieee.org/document/5708280

*Reference List | NIST*. (2024, January 3). NIST. https://www.nist.gov/itl/applied-cybersecurity/nice/resources/executive-order-13800/reference-list

U.S. Department of Defense. (2022). *Overview of useful references to support security cooperation* (p. 3). https://dodcio.defense.gov/Portals/0/Documents/Library/CSResourceReferenceGuide.pdf

CSRC Content Editor. (n.d.). *Home | CSRC*. https://csrc.nist.gov/

Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology, U.S. Department of Commerce. (n.d.). *Cybersecurity and Privacy Reference Tool | CSRC | CSRC*. https://csrc.nist.gov/Projects/cprt