**Protecting Company Employees and Information: A comprehensive Cyber Security Approach**

**Prepared by: Reniel Villahermosa**

**Position: Cyber Security Manager**

**Company: ABC Company**

**Date: Tuesday May 21st, 2024**

**Executive Summary**

This report details a range of essential cyber security measures tailored to protect our company’s employees and safeguard sensitive information from potential cyber threats. As the newly appointed Cyber Security Manager at ABC Company, I am responsible for establishing robust security protocols to strengthen our digital defenses.

We begin with fundamental security strategies such as strong password requirements and a rigorous password expiration policy, and further enhance security through Multi-Factor Authentication (MFA). These measures are supported by additional layers including encrypted email communications, VPN usage, and data encryption on portable devices.

To secure communications, we utilise personal certificates for email, ensuring that all sent and received emails are encrypted and authenticated, thus safeguarding our internal communications from interception or misuse. Additionally, we deploy VPN IPSec on company laptops to protect data transmitted over public or unsecured networks, providing a secure and encrypted conduit for our remote and mobile workforce.

We also emphasize the importance of protecting data stored on portable devices. To this end, cryptographic hard and flash disks are used to encrypt data at rest, ensuring that sensitive information remains secure, even if physical devices are lost or stolen.

The proactive management of software through regular updates and patching is another critical aspect of our cyber defense strategy. By keeping our software and systems up-to-date, we mitigate vulnerabilities that could be exploited by cyber threats, thereby enhancing our overall security posture.

By adopting these practices, ABC Company not only protects its operational integrity but also reinforces its commitment to security, ensuring that both employees and company data are protected against emerging cyber risks.

**Introduction**

As the newly appointed Cyber Security Manager at ABC Company, my role embraces the strategic enhancement of or cybersecurity measures to protect our employees and safeguard sensitive company information. This involves a comprehensive review and upgrade of our existing cybersecurity protocols in alignment with the latest industry standards, including NIST and ISO 27001 guidelines.

This report outlines a series of foundational yet powerful security practices that form the core of our proactive cybersecurity strategy. These include the implementation of strong, regularly updated passwords, the use of multi-factor authentication (MFA) to secure access, encrypted email communications via personal certificates, and the deployment of VPN IPSec on all company laptops to ensure secure remote connections. Additionally, we focus on encrypting data on portable storage devices to prevent data breaches from lost or stolen media.

Moreover, the significance of regular software updates cannot be overstated, as they play a critical role in protecting against vulnerabilities that could be exploited by cyber threats. Each of these measures is explained with a focus on their implementation and the practical benefits they bring, ensuring that all employees, regardless of their technical background, can understand and adhere to our enhanced security protocols.

The objective of this report is to provide clear, actionable information that will guide both technical and non-technical staff in adopting these measures to create a more secure and resilient digital environment at ABC Company.

**Techniques and Approaches**

**1. Strong Passwords**

**Definition and Importance**: A strong password acts as the first barrier against unauthorized access. According to NIST guidelines, a robust password combines length and complexity to minimize breach risks.

**Implementation**:

* **Characteristics**: Passwords should be at least 12 characters long, including a mix of upper and lower case letters, numbers, and symbols. This recommendation aligns with NIST's latest publications.
* **Examples of Strong Passwords**:
* Good: P@ssw0rd!234
* Better: Th!sIsAStr0ngP@ss!
* Best: A complex phrase or sentence that you can remember but others can't guess.
* **Password Management:** Use of a password manager is recommended to maintain the integrity of password security without compromising ease of access.
* **Regular Updates**: Change your passwords regularly, at least every 60-90 days. This reduces the risk of someone using an old password to access your account.

**Why It Matters**:

* **Security**: Weak passwords can be easily guessed or cracked by hackers, putting our data at risk. Strong passwords provide a solid defense against unauthorized access.
* **Protection**: Protects not just your work accounts but also personal information that might be stored or accessed through those accounts.
* **Compliance**: Helps us meet security standards and regulations that require strong password policies.

**Steps to Create and Maintain Strong Passwords**:

1. **Create a Strong Password**: Use a mix of letters, numbers, and special characters. Avoid using the same password for multiple accounts.

2. **Use a Password Manager**: If you have trouble remembering your passwords, use a password manager to keep track of them securely.

3. **Change Passwords Regularly**: Update your passwords every 60-90 days to enhance security.

4. **Avoid Sharing Passwords**: Never share your passwords with anyone. If you need to grant access, use secure methods provided by our IT team.

By following these guidelines, you can create strong passwords that significantly enhance our company's security. If you have any questions or need help creating or managing your passwords, our IT team is here to assist you.

**2. Password Expiration Policy**

**Importance:** Regularly changing your password helps prevent unauthorized access. If a password is used for too long, there's a higher risk that it could be compromised through various means, such as hacking or phishing. By updating passwords periodically, we reduce this risk and keep our accounts more secure.

**Definition and Importance**: Regularly updating passwords reduces the risk of prolonged exposure from potentially compromised credentials, as stipulated by cybersecurity frameworks like ISO 27001.

**Implementation Guidelines**:

* **Expiration Timeline**: Passwords should be updated every 90 days, a practice supported by empirical data from various cybersecurity studies indicating reduced risk of data breaches.

**Steps to Follow for Password Expiration Policy**:

1. **Pay Attention to Notifications:** Watch for reminders to change your password and act promptly.

2. **Change Your Password**: Follow the instructions provided in the notification to change your password.

3. **Create a Strong New Password**: Use a mix of upper and lower case letters, numbers, and special characters. Avoid reusing old passwords.

4. **Seek Assistance if Needed:** Contact the IT team if you encounter any issues or need help with changing your password.

By adhering to our password expiration policy, we can better protect our systems and data from unauthorized access. Regular password updates are a simple but effective way to enhance our overall security..

### **3. Multi-Factor Authentication (MFA)**

**Definition and Importance**: Multi-Factor Authentication (MFA) significantly enhances the security of user accounts and sensitive data by requiring more than one method of verification before granting access. This method is essential in protecting against unauthorized access and is highly recommended by security frameworks such as ISO/IEC 27001 and NIST.

**The Three Factors of Authentication**: MFA relies on three distinct categories of credentials, enhancing security by combining different forms of evidence, thus making unauthorized access considerably more challenging:

1. **Something You Know** (Knowledge): This factor includes anything that the user must mentally know to log in, such as a password, PIN, or a pattern.
2. **Something You Have** (Possession): This involves something the user physically possesses, such as a security token, a smartphone app (authenticator app), or a smart card, which generates or receives a verification code.
3. **Something You Are** (Inherence): These are the biometric factors such as fingerprints, facial recognition, or voice recognition that uniquely identify the user.

**Implementation Guidelines**:

* **Setup Process**: Begin by assessing which systems and data require the highest level of security and implement MFA on these channels first. IT support will assist in setting up the necessary tools and tokens for each employee, ensuring that they have the required devices and knowledge to use them effectively.
* **User Education**: Conduct training sessions for all employees to explain how MFA works and why it’s essential for protecting both their personal and company data. Clear instructions on how to use each authentication factor will be provided.
* **Continuous Monitoring and Support**: Monitor the effectiveness of MFA implementations and provide ongoing support to address any user issues or updates in MFA technology.

**Why It Matters**: Implementing MFA provides a robust layer of security by ensuring that the theft or compromise of one credential alone is not enough for an intruder to gain unauthorized access. This is particularly crucial in an era where single-factor authentication, like passwords alone, no longer offers adequate protection against sophisticated cyber threats.

By incorporating these detailed explanations and professional terminologies, this section aims to demystify MFA and emphasize its importance within our cybersecurity strategy, making it accessible and understandable for every member of the company.

### **Encryption Techniques**

**Definition and Importance**: Encryption is the process of converting data into a coded format that can only be accessed by authorized individuals with the decryption key. This fundamental security measure protects the confidentiality and integrity of data both at rest and in transit, a critical component in complying with standards such as NIST and ISO 27001.

#### **A. Data Encryption at Rest**

**Implementation Guidelines**:

* **Whole Disk Encryption**: Use cryptographic solutions that encrypt the entire hard drive of a device. This ensures that all data stored on the device is inaccessible without the proper credentials.
* **Database Encryption**: Specific databases that store sensitive information should use field-level encryption to protect particular data elements independently.

**Standards Reference**: NIST Special Publication 800-111 provides guidelines for storage encryption technologies for protecting data at rest.

#### **B. Data Encryption in Transit**

**Implementation Guidelines**:

* **VPN IPSec**: Implement VPN IPSec to securely encrypt data transmitted between remote users and the network. It ensures that data sent over less secure networks, like the internet, is protected against eavesdropping and man-in-the-middle attacks.
* **TLS for Emails and Web Applications**: Use TLS (Transport Layer Security) to secure communications between clients and servers. This is essential for protecting sensitive data in emails and during transactions on web applications.

**Standards Reference**: ISO/IEC 27002 provides best practices for the encryption of data in transit, recommending the use of strong encryption algorithms and proper key management.

#### **C. Mobile Device Encryption**

**Implementation Guidelines**:

* **Encrypted Storage on Mobile Devices**: Ensure that all mobile devices used within the organization are equipped with default encryption settings enabled to protect data stored on these devices.
* **App Data Encryption**: Applications developed for internal use should employ data encryption to secure user data stored within the app, especially when the data is synchronized to a cloud service.

**Standards Reference**: NIST SP 800-124 provides guidance on securing mobile devices within enterprise environments, highlighting the importance of encryption to mitigate the risk of data loss or exposure.

.

**4. Secure Email with Personal Certificate**

**Importance**: Securing our email communications is crucial because emails can contain sensitive information that we don't want to fall into the wrong hands. By using a personal certificate, we can ensure that our emails are both encrypted and authenticated. This means that only the intended recipient can read the email, and they can be sure it really came from you.

**Implementation:**

* **What is a Personal Certificate?:** A personal certificate is a digital file that acts like a virtual ID card. It verifies your identity and encrypts your emails so that only the intended recipient can open and read them.
* **How It Works**: When you send an email with a personal certificate, the email is encrypted before it leaves your computer. This encryption ensures that if anyone intercepts the email, they won't be able to read it. The recipient will use their own certificate to decrypt and read the email.
* **Setting It Up:** We will help you set up your personal certificate. This involves installing the certificate on your email client (like Outlook) and configuring it to automatically encrypt and sign your emails. Don’t worry; we will guide you through each step.
* **Why It Matters**: Without encryption, anyone who intercepts your email can read its contents. With encryption, only the person you sent the email to can decrypt and read it. This keeps our communications private and secure.

**Benefits**:

* **Confidentiality:** Ensures that only the intended recipient can read your emails.
* **Authentication**: Verifies that the emails you receive are genuinely from the sender and haven't been tampered with.
* **Trust:** Builds trust with our clients and partners, knowing that their information is protected when they communicate with us.

**Steps to Use Secure Email**:

1. **Installation:** Our IT team will install your personal certificate on your email client.

2. **Sending Secure Emails**: After setup, your emails will be automatically encrypted and signed. You don’t need to do anything extra.

3. **Receiving Secure Emails**: When you receive an encrypted email, your email client will use your personal certificate to decrypt it.

By using personal certificates to secure our emails, we ensure that our communications remain private and trustworthy. This protects not only our company's information but also the sensitive data of our clients and partners.

**5. VPN IPSec on Laptops**

**Importance:** A Virtual Private Network (VPN) with Internet Protocol Security (IPSec) is essential for securing our online activities, especially when we are working remotely or using public Wi-Fi. It ensures that all data sent and received on our laptops is encrypted, making it much harder for hackers to intercept and read.

**Implementation**:

* **What is a VPN?**: A VPN is a secure connection between your laptop and the internet. Think of it as a private tunnel that protects everything you do online from prying eyes.
* **What is IPSec?:** IPSec is a suite of protocols used to secure Internet communications by authenticating and encrypting each IP packet of a communication session.
* **How It Works**: When you connect to the internet through a VPN, all your internet traffic is routed through a secure server. IPSec adds an extra layer of security by encrypting your data, ensuring that it remains private and secure.
* **Setting It Up**: We will help you set up the VPN IPSec on your laptops. This involves installing VPN software and configuring it to connect to our secure servers. Our IT team will provide detailed instructions and support to ensure everyone is set up correctly.
* **Why It Matters**: Without a VPN, your internet traffic can be easily intercepted, especially on public Wi-Fi networks. With a VPN, even if someone intercepts your data, they won't be able to read it because it's encrypted.

**Benefits**:

* **Security**: Protects sensitive data by encrypting all internet traffic.
* **Privacy**: Hides your online activities from potential eavesdroppers.
* **Remote Access**: Allows you to securely access company resources from anywhere.

**Steps to Use VPN IPSec**:

1. **Installation**: Our IT team will install the VPN software on your laptop.

2. **Connecting to the VPN:** You’ll open the VPN software and log in with your credentials. Once connected, all your internet traffic will be secure.

3. **Using Public Wi-Fi**: Always connect to the VPN when using public Wi-Fi to ensure your data remains protected.

By using VPN IPSec on our laptops, we can secure our online activities and protect sensitive company information, especially when working remotely or from public places. This simple step is crucial in keeping our data safe from cyber threats.

**6. Cryptographic Hard and Flash Disks**

**Importance**: Encrypting hard and flash disks is crucial for protecting the data stored on these devices. If a laptop or flash drive is lost or stolen, encryption ensures that the information cannot be accessed by unauthorized individuals.

**Implementation**:

* **What is Encryption**?: Encryption is a process that converts data into a code to prevent unauthorized access. Only someone with the correct key (like a password) can decrypt and read the data.
* **Why Use Cryptographic Disks?**: Cryptographic disks automatically encrypt all data stored on them. This means that if someone tries to access the data without the proper key, all they will see is gibberish.
* **How It Works**: When you save a file to an encrypted hard or flash disk, the encryption software scrambles the data. When you need to access the file, you use your password to decrypt it, making it readable again.
* **Setting It Up**: Our IT team will provide encrypted hard disks and flash drives. We will help you set them up and show you how to use them. The process is straightforward and won't change the way you normally save and access files.
* **Why It Matters**: Without encryption, anyone who gets hold of a lost or stolen device can easily access the data stored on it. With encryption, your data is protected, and only you can access it.

**Benefits**:

* **Data Security**: Ensures that sensitive information remains confidential, even if the device is lost or stolen.
* **Peace of Mind:** Knowing that your data is secure reduces the worry about potential data breaches.
* **Compliance**: Helps our company meet data protection regulations and standards.

**Steps to Use Encrypted Hard and Flash Disks**:

1. **Receiving Your Device**: The IT team will issue encrypted hard disks and flash drives to those who need them.

2. **Setting Up Your Device**: We will help you set up your device and create a strong password for encryption.

3. **Using Your Device**: Save and access files on the encrypted device just as you normally would. The encryption process runs in the background and won’t interfere with your work.

By using cryptographic hard and flash disks, we ensure that our sensitive data is protected, even if a device is lost or stolen. This simple yet effective security measure helps keep our information safe and secure.

**Other Techniques**

**7. Regular Software Updates and Patch Management**

**Importance**: Regular software updates and patch management are essential for keeping our systems secure. Software updates often include patches that fix security vulnerabilities. If these are not applied, our systems can be exposed to cyber attacks.

**Implementation**:

* **What are Software Updates?**: Software updates are new versions of software that include improvements, new features, and importantly, security fixes.
* **What are Patches?**: Patches are pieces of code designed to fix specific issues, including security vulnerabilities, in software.
* **Why Update Regularly?**: Cyber attackers often exploit known vulnerabilities in software. By keeping our software up to date, we close these security gaps and protect our systems.
* **How It Works**: When a software update or patch is released, it needs to be installed on our systems. This can usually be done automatically or manually, depending on the setup.
* **Setting It Up**: Our IT team will configure systems to automatically download and install updates whenever possible. For software that requires manual updates, we will provide instructions and assistance to ensure everyone keeps their software up to date.
* **Why It Matters**: Without regular updates, our systems can become vulnerable to attacks that exploit outdated software. Keeping software updated is a simple yet highly effective way to enhance security.

**Benefits**:

* **Security**: Fixes vulnerabilities that could be exploited by cyber attackers.
* **Performance**: Updates often include performance improvements and new features.
* **Compliance:** Ensures we meet industry standards and regulations for software security.

**Steps to Ensure Regular Updates:**

1. **Automatic Updates:** Our IT team will enable automatic updates for software that supports it.

2. **Manual Updates:** For software that requires manual updates, we will notify you when an update is available and provide instructions on how to install it.

3. **Regular Checks**: Make it a habit to regularly check for software updates and install them promptly.

By regularly updating software and applying patches, we can protect our systems from known vulnerabilities and improve overall performance. This proactive approach helps keep our company’s data secure. Again, we I would like to stress that our IT department is here to help so reach out any time you are having trouble.

**Citations**

1. **NIST Special Publication 800-111**: Guide to Storage Encryption Technologies for End User Devices. NIST. Provides guidelines for encrypting data at rest and best practices for implementing such technologies within an organizational context. Available at: [NIST SP 800-111](https://csrc.nist.gov/publications/detail/sp/800-111/final).
2. **ISO/IEC 27002**: Information technology — Security techniques — Code of practice for information security controls. It offers best practices for the implementation of data encryption in transit, including the use of TLS and secure management of cryptographic keys. Available from ISO Catalogue: ISO/IEC 27002.
3. **NIST Special Publication 800-124**: Guidelines on Cell Phone and PDA Security. NIST. Provides comprehensive guidance on securing mobile devices within enterprise environments, emphasizing the importance of encryption to protect data stored on mobile platforms. Available at: [NIST SP 800-124](https://csrc.nist.gov/publications/detail/sp/800-124/rev-1/final).
4. **ISO/IEC 27001**: Information technology — Security techniques — Information security management systems — Requirements. Specifies requirements for establishing, implementing, maintaining, and continually improving an information security management system (ISMS). It includes provisions for MFA to enhance access control security. Available from ISO Catalogue: ISO/IEC 27001.
5. **NIST Special Publication 800-63B**: Digital Identity Guidelines: Authentication and Lifecycle Management. Provides detailed guidance on implementing digital identity services, including the use of MFA. Available at: [NIST SP 800-63B](https://csrc.nist.gov/publications/detail/sp/800-63b/final).
6. **The Internet Engineering Task Force (IETF) RFC 5246**: The Transport Layer Security (TLS) Protocol Version 1.2. Describes the protocol and its implementation details for securely transmitting data over the internet. Available at: RFC 5246.