**Step 1 : Measure and Set Goals**

1. Some security risks of employees using personal devices to access work information include :
   1. Packet sniffing could be used to collect data going from more secure work servers to less secure personal devices outside of the network.
   2. Physical data loss due to loss of personal devices.
   3. Malware attacks are also a major threat when devices are connected to networks outside of the company’s network.
2. Prefered employee behavior for each of the above scenarios would be :
   1. If employees must access or retrieve work information while using personal devices it would be preferred that they use SSH, or a VPN to connect to the network and SFTP to retrieve said information.
   2. To mitigate potential data leaks employees should be aware of what makes a strong password and possibly use a password manager that randomly generates passwords and uses two factor authentication to enter said passwords for work activities on personal devices.
   3. Employees would be requested to not download extensions from emails unless it is from a trusted source. Another important request would be that employees avoid clicking/following ads (especially on NSFW sites) to avoid infection through that avenue. (It’s awkward, but if they are able to access sensitive information on their personal devices outside of the company network NSFW sites will likely be visited by at least a small percentage of employees)
3. The following are examples of how to measure how often employees are *not* behaving according to the preferred behavior :
   1. Assuming employees must log into the network in some way before accessing information, connections could be monitored to determine if the connection is through SSH or a VPN.
   2. A survey could be used to see if employees use a reputable password manager to secure access to work data on personal devices.
   3. Emails could be sent out with “malicious” attachments that could report back who opened and downloaded the attachment. Unfortunately the only way to track employees' tendencies to click on ads would be to conduct a survey, even though they are generally not very reliable.
4. The behavioral goals for this organization are as follows :
   1. To prevent packet sniffing employees would be required to have all off site connections be through SSH or VPN and any file transfers should use SFTP tools. I believe it would be doable by not blocking off network connections without those tools.
   2. Because business data is important my goal would be to have all employees using password managers capable of generating strong passwords for work applications on personal devices as well as two factor authentication when accessing data from outside of the business network.
   3. My goal for lowering the risk of document injected malware would be to have less than 5% of employees download email attachments from insecure sources.

**Step 2 : Involve the Right People**

In order to enact a security plan the Chief Information Security Officer (CISO), CEO, SilverCorp’s security team, director of HR, and whoever is in charge of training and communication need to be involved in making and executing said plan.

The CEO and CISO will have ultimate say in how plans are executed and or budget for the plan. If they feel your recommendations are too strict, work with them to find something that will increase security but still allow employees the freedom the CEO and CISO feel they need.

SilverCorp’s security team will be in charge of implementing some of the tests, such as fake malicious emails/attachments to test employees. They will also be responsible for maintaining the right tools for employees to use when accessing the network from their personal devices.

The director of HR will be important to this task to ensure employees’ rights are maintained through the design and implementation of the plan. Since we are working with employees’ personal devices as the focus of this security plan their privacy should be protected.

The person in charge of training and communication will be vital to implementing this plan. They will be responsible for distributing and collecting review data from in person training sessions. They will also provide important insight on how the employees respond to different training techniques.

**Step 3 : Training Plan**

Depending on the type of training (described below) it will either be continuous or on a semi monthly basis. The majority of the training will be online, with a few in person courses to help employees obtain and set up the proper applications for their personal devices.

The topics covered in training will include the following :

* **Email safety** - Because so many malicious attacks are carried out using emails as the method of infection employees need to be aware/careful of what emails they open and what attachments they download. This is especially important if they are using their personal devices as they will have more email traffic on top of their standard email. The training for this would involve a regular MEMO as well as test emails sent out at random times to each employee to test if they are downloading attachments.
* **Ad/phishing training -** Because employees are using their personal devices they need to be aware of the things that could be lurking behind Ads on websites or phone calls. The training could also be done by regular reminders sent through MEMOS and possibly in person training a few times a year. Effectiveness would be measured by survey to see how often employees recognized received phishing calls and malicious ads
* **SSH/VPN training -** SSH/VPN training would happen at least once a year with updates if there are any major changes to the system. The training would be mostly involved with how to properly use SSH and/or VPN clients and the importance of using them when outside the work network. Success of the training would not be measured by hard metrics, rather by the ease with which employees adopt to using SSH/VPN protocols. If more than 5% of employees struggle with using the new protocols new training methods would be developed and implemented as soon as possible.
* **Password management and tools -** Training for password strength and tools should be done about 4 times a year because it is easy to become complacent with passwords without frequent reminders or tools that will update them for the user. Topics will cover what makes a strong password and some common weaknesses to avoid. The company will also host, or endorse a password management system for employees to use to aid in strong passwords. After training a survey would be used to measure general understanding since it is difficult to safely track the strength of passwords outside of having strict requirements