Step 1: Measure and set goals:

Answer the following questions:

1. Using outside research, indicate the potential security risks of allowing employees to access work information on their personal devices. Identify at least three potential attacks that can be carried out.

1. Data Theft:
   1. Personal applications on a device may collect more data than is needed for the app to function. This can include information about other apps, photos, contacts, network traffic, GPS location data, audio, video, or stored documents.
   2. Backing up a personal device on a personal pc may also allow the device owner to restore company data after the device has been wiped by the company IT department and returned to the user.
2. Shadow IT:
   1. Employees may bring their own solutions to accomplish their work. These can include using their personal storage service (Google, Dropbox, OneDrive) to host, store, or disseminate data outside the approved confines of the corporate control methods.
   2. This may also include servicing devices without the consent or knowledge of the corporate IT team. When upgrading devices or getting repairs, some may choose to take their device loaded with company data to a third party repair shop. This allows that repair shop to potentially access and steal that data in a way that is unobservable to the device user or the company.
3. Poor Mobile Access Management:
   1. A BYOD user may have numerous apps, a network configuration, like a virtual private network (VPN) tunnel, certificates, or other access mechanisms that allow them to authenticate or access their companies internal data and systems. Revoking all certificates, app logins, and network access rights. Leaves a lot of work to do when an employee terminates. This work may not be dealt with as fast as necessary or properly to prevent the access from being abused.
   2. An attacker may take synchronized emails on the device, use installed apps to steal data, or use the device to act as a backdoor to their corporate network.

2. Based on the above scenario, what is the preferred employee behavior?

- For example, if employees were downloading suspicious email attachments, the preferred behavior would be that employees only download attachments from trusted sources.

1. Data Theft:
   1. The desired behavior in this case is for staff to only download reputable apps from reputable app stores. This may decrease the likelihood that they will download malicious apps from 3rd party stores. Staff may also be told to refrain from opening any other applications that are not approved during their work on their personal devices. Internal business applications should also be designed securely to prevent security issues, memory leaks, or unauthenticated access.
   2. Ensuring backups only contain personal information and not company information. Do not store company passwords, scans of documents, pdf files, etc locally to the device.
2. Shadow IT:
   1. Employees should use only company approved services like a Corporate Sharepoint site, Company controlled Dropbox account, or Google workspace.
   2. Notify IT of device loss, theft, damage, replacement, and upgrades. IT should work with the employee to sanitize the device in the case of damage, replacement, or before upgrades. IT should also have a way to identify the device and remotely wipe it in the case of loss or theft.
3. Poor Mobile Access Management:
   * 1. In the case of apps, employees should remove all company apps upon the termination of their authorization to access them. Internal IT should revoke credentials to these apps and programs.
     2. Network access through a virtual private network (VPNs) should be disabled. If credential based, revoke the credentials in a timely manner.
     3. Certificates are often long lasting and hard to change across large and diverse systems. If certificates are used to provide authentication or access, the curators of those certificates should revoke them as soon as authorization ceases. Certificates being generated should have shorter lifespans to ensure that they expire in a timely manner if forgotten about.
   1. 1. Do not synchronize data to your devices. For email, use official mail service apps that require a login before presenting data.Use device passcodes to lock the device.

3. What methods would you use to measure how often employees are currently *\_not\_* behaving according to the preferred behavior?

- For example, conduct a survey to see how often people download email attachments from unknown senders.

1. Data Theft:
   1. Using an mobile device management system (MDM) to monitor applications running on the device. This can see what the applications are, how long they run for, and what connections they make.
2. Shadow IT:
   1. Use an MDM to locate local files on the device and monitor system logs for file downloads.
   2. Inspect devices for damage periodically, use taper tags to identify devices that are approved to be used, base application install and access on only devices that are approved.
3. Poor Mobile Access Management:
   1. Section A:
      1. Use a mobile device management software to verify the company apps are removed from the device. This software should help you quickly find which devices have unapproved apps installed.
      2. Monitor network access logs to identify access by virtual private network (VPN) connections.
      3. Check logs for invalid certificates or credentials used in authentication attempts.
   2. Section B:
      1. Check email security logs to verify connection type and method.

4. What is the goal that you would like the organization to reach regarding this behavior?

- For example, to have less than 5% of employees downloading suspicious email attachments.

1. Data theft:
   1. Have 100% of BYOD devices approved and enrolled with a mobile device management system (MDM).
2. Shadow IT:
   1. Have less than 5% of employees using personally managed 3rd party programs, services and personal accounts for work purposes.
3. Poor Mobile Access Management:
   1. Terminate remote access within 2 hours of termination notice. Have 100% of accounts and access methods documented for every user.

Step 2: Involve The Right People

Indicate at least five employees or departments that need to be involved. For each person or department, indicate in 2-3 sentences what their role and responsibilities will be.

1. CEO: This individual will need to be involved to help shape the culture in which the company supports and fosters a security culture. Their authority will help immensely in gaining buy-in from other tiers of management to adapt the security minded company culture.
2. Chief information security officer (CISO): This position will be needed to direct the security culture, advise the C-suite level staff like the CEO, advise the board, and direct the teams below them. They will facilitate the security culture and lead the direction of design for the company’s security needs.
3. Network Operations Center (NOC): The network operations center will need to be involved in maintaining network accessibility and ensuring the network infrastructure can support the personal devices in use. They will do this by verifying wifi standards and compatibility, configuring virtual private network (VPN) access, and verifying devices are authorized to access the network infrastructure.
4. Security Operations Center (SOC): This team will be responsible for going over the network access logs, Software as a Service (SaaS) logs (E.g. Sharepoint), and MDM logs for anomalies. They will be required to collate the logs from the other departments and monitor them to ensure no lapse in security occurs from the adoption and continued use of the Bring Your Own Device (BYOD) policy.
5. Systems Administration/Help Desk: This team will be in charge of applications access, account creation and deactivation, managing the mobile device management (MDM) system, and general communications with the other teams to support the documentation and functionality of the BYOD policy in practice. This team is also likely to be the first point of contact when issues arise on the end user side.

Step 3: Training Plan

1. How frequently will you run training? What format will it take? (i.e. in-person, online, a combination of both)
   1. A combination of in-person and online training will be conducted. Training will be run at hiring, semi-annually or quarterly depending on staff size, and as needed to correct behavior throughout employment.
2. What topics will you cover in your training and why? (This should be the bulk of the deliverable.)
   1. The online training will consist of a course of short videos covering data privacy, mobile device management and professionalism in the workplace in regards to personal devices, guidance on choosing safe app stores, company apps, policy for loss, theft, or replacement of devices, and an overview of who to contact for issues.
   2. This in-person training will be a basic/cut down supplement to online training. As the IT team under the System Administrator tags and documents devices, they can cover the policies about loss, theft, and replacement once more. They may also cover how to reach out to them and the separation of responsibility regarding support for personal devices issues vs issues the company supports.
3. After you’ve run your training, how will you measure its effectiveness?
   1. The measurements will be done through log reports, hands on appraisals, and account access audits.

* + 1. Data Theft:
       1. Using the mobile device management system, you can view the installed applications on a device or the presence of unauthorized apps. You can enforce a standard that requires an Antivirus (AV) software be installed on the device. This will allow you to measure if employees may be utilizing dangerous apps that may compromise their devices or if their device meets security baselines.
    2. Shadow IT:
       1. This can be measured by observing logs of approved tools and services. You should see consistent access by all staff for common services. If someone stops using Sharepoint entirely or begins moving/copying massive amounts of files, this is a red flag.
    3. Poor Mobile Access Management:
       1. This measurement will be made by examining the access logs of a terminated user to verify no access occurs after termination of the user. This will also be measured by auditing accounts and access methods to ensure all terminated users have had their accounts properly archived, deleted, or disabled.

Bonus: Other Solutions

- Indicate at least two other potential solutions. For each one, indicate the following:

1. Provide users with secured company owned mobile devices.
2. Provide a stipend to pay for an Antivirus software and policy requirement to have this installed their mobile device.

\* What type of control is it? Administrative, technical, or physical?

1. This would fall into Administrative and Technical
2. Administrative

\* What goal does this control have? Is it preventive, deterrent, detective, corrective, or compensating?

1. Preventative: Prevents the risks associated with personal devices accessing corporate data and services.
2. Deterrent: This deters some risks by hardening the device with an antivirus service which will help prevent some attacks and malware.

\* What is one advantage of each solution?

1. The company can ensure the devices are uniform in control and security standards.
2. This will help harden their device without a lot of company-side overhead or involvement.

\* What is one disadvantage of each solution?

1. This is an expensive policy due to the procurement and provision of the devices.
2. This is not a guarantee of security. Ensuring software updates and continued use of the antivirus service will be difficult to measure without other detective supports in place.