#### **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.**

Users with work information on their personal devices can have many risks. Some can be mitigated to a tolerable level but some things cannot have the risk lowered enough to justify the ease of access to have corporate information on hand at all times. A compromised device with important company documents could result in financial risk, the risk of violation of law for PII, and damage to the companies reputation which could result in the business closing.

One risk is the potential of having malicious software on their devices that the employee might not be aware of. Their children may have downloaded a program that promised to give them a new Ipad, but instead has added a script that could gather the information on the machine weather it be a keylogger, trojan, malware, or many others.

If the data is on a mobile device then wherever the employee goes could have possible agents waiting to attack. They could stop by a public restaurant such as a coffee shop and connect to the public wifi. There are so many attacks that can take place on public networks such as this that they would likely have full access to the phone. Since most people do not encrypt their phone, the attacker would have to use very little effort in an attack like a honeypot.

If the person has a mobile device that gets stolen, unless they have a secure password (which they likely do not) then an attacker could just brute force the password on the machine and have full access to it. Since the device is not managed and the password requirements for the device are not set to a standard for a secure password or passcode many people would have an easy time unlocking the device.

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

One possibility if the company has the resources is to create a hub location for authorized downloads on the devices. If there is an internal corporate site where they can view what programs can be installed on the machine and a link to a verified source.   
For email attachments such as PDF or Office based files it would be more difficult to monitor. If they are logging in to a corporate email on a personal device it would need to be secured at the mail server. Possibly scanning all attachments before they arrive in the users mailbox if they come from an outside source and mark the email for the user as potentially harmful so it may act as an alarm that will catch their attention and make them think before clicking on the message. It will also ask if they are sure that they want to open unknown information on the email.

For the work related applications and tools, I would have a login access set up for accessing the program on all devices. It would run a system check to verify that the device that is currently running the program is a company owned asset.

In total it would be better to choose where files are downloaded from, and not give the users the option on where or what to download. And alert the user when an email is received from an unknown source.

1. **What methods would you use to measure how often employees are currently *not* behaving according to the preferred behavior?**

I would implement a series of emails to be sent out with different attachments from emails that are not known by the employees. I would record how many view the email after the warning and how many download the file(s) while knowing the risk.   
I would also run regular scans for not only unwanted software, but software that is not on the approved list.

For personal devices, I would try to track the information of the devices that are trying to access certain things within the network. What devices are accessing programs and what is the ID of the device. The company can have the IT team record the information of each asset that is put into production for the company.

Any device that is not company owned that is attempting to access the corporate network and data should have a prompt for login, so you can verify who is trying to log in and from where.

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

The goal would ideally be less than 1% for all logins from unauthorized devices to company applications and programs. This is attainable by putting out a policy where no company data or programs can be run on personal devices.

For the access of data from users sending out company files to personal emails or bringing data outside of the company network or devices, it would be closer to 2% for sensitive data such as PII or financial information. And 10% for lower risk data, like bookmarks or schedules for meetings that are not confidential (ex: meeting for a holiday party).

#### **Step 2: Involve the Right People**

**Now that you have a goal in mind, who needs to be involved?**

The main people that need to be persuaded to agree to implement the policy and to assist with it would be the CEO/CIO/CSO, HR, IT, legal team, and the mail server administrators.

The executive that would be in charge of the security of the company depending on the hierarchy would need to be briefed and swayed to the side that the implementation is worth the cost and time for the project.

The HR team would need to be involved to verify that this policy and the process does not violate any restrictions to the employees rights and that they allow the new policy to go into place.

The IT team to assist with implementing the process and to monitor and enforce the rules set in the policy. Such as monitoring the device logins as talked about in section 1 question 3.

The legal team would need to ensure that the law is being followed with no overreach into the employees devices and create an acceptable use policy regarding the company assets.

Mail server administrators would need to create the rule set to filter and monitor the different attachments and set up the flags for potentially harmful messages.

#### **Step 3: Training Plan**

**Training is part of any security culture framework plan. How will you train your employees on this security concern? In one page, indicate the following:**

Employees will be trained annually, and bi-annually if their knowledge does not meet a certain threshold. There will be training developed for them regarding the acceptable use of the devices and programs provided by the company. They will also be taught about personal devices within the workplace.

An online training would take place for an overarching version of the training for all employees. The training would include the policies and procedures regarding security in the workplace and what personal devices can be used for when accessing anything work related. There will be a short test going over the policy and the passing grade for no remediation would be 95% and above. For users that get between 70% and 94% would need to take a scaled down version of the training or possibly have a security 2 hour seminar lead by a member of the security team where they will go over the policies and reiterate possible risks, this could be used to minimize the cost of two professionally created learning modules with exams. Any user that gets below a 70% on the test will need to retake the initial course and test to receive a better score.

One thing that will be covered in the training is the use of company tools/programs, as the company owns the license to the software the employee has no right to misuse it or use it for personal things.

There will be a section on how employees are not to use personal devices for work related material. If the employee has an actual need to get email on their phone for example, they can submit a request through their manager to get an approved and managed company phone where all the data on it is subject to the acceptable use policy.

For company devices, the rules will be laid out that they are not to be used for personal use. They will be checked for unauthorised software on the machines and the training will follow with the correct path on how to get software if it is needed like in submitting a request to IT for a program that is not in the pre-approved list.

The training will explain how the policies, rules and regulations all are enforceable and can have repercussions for violating the instructions for the use of these devices and programs that could even lead to termination.

The training will be measured by checking the logs of the software scans of the company assets looking for unauthorized programs on the computers. It will be calculated by the amount of computers that are in compliance and those out of compliance as a percentage. If it meets the previously set threshold it will be a success. For the personal devices used at the company, they will cross reference the devices connected to the network and filter out the known company assets. If there is a device that is not listed as a company asset on the network (not the guest network) then it will be blocked.

The best way to record the use of company programs on personal devices will be to record the device that is logging in to the programs or trying to access internal sites. If it is an outside source it could be determined to be someone trying to gain access at home. But it would not be an extremely accurate number to go off of since there could be non-employees attempting to gain access. Either way it would not be good for the company.

#### **Bonus: Other Solutions**

**Training alone often isn't the entire solution to a security concern.**

One option is to not allow any personal devices in the building. Or at least no access while on the clock. The company could provide secure storage for their employees to have their devices in a secure location to use when they are not working such as on break or during lunch. This is not ideal but it is secure.

Having them keep their phones away from their desks during working hours is an administrative control that would have an enforced policy with disciplinary actions if it was not followed. This preventive measure would not only assist with keeping employees from getting distracted while at work. But also remove any temptation to put anything work related on their devices since they cannot use them while at work. Although, many employees would refuse this if it is a new policy and likely quit because it would need to be strict to be effective.

Another option would be to require a key to access any account, such as a yubikey. They could have all the yubikeys be stored at the office so that employees could not log in to any device that is not at their workstation. This two factor authentication would be a technical control as it utilizes technology to restrict unauthorized access to the company accounts and programs.

This would be considered a preventive measure since it would refuse access to any system where the person logging in does not have the correct key to authenticate the login.

This would make sure that no employee can access a company device while away as the keys would be stored in the office. A downside to this would be keeping track of the keys. It would be a tedious time consuming process.