Step 1:

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.

**A hacker could gain access to an employee's phone through an unsecured WiFi.**

**An employee's phone can be stolen and all the company's info on that phone could be downloaded by the hacker.**

**An ex employee could have access to the company's data.**

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

**The employee should never access the work app or send important data outside the workplace.**

**Have a program that can instantly shutoff a lost device and erases important data.**

**Make sure ex employees no longer have access and phones have to be surrendered to IT and wiped.**

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

**I would create a fake malicious email and send it to all the employees. I then would wait to see who all clicked on it and downloaded it.**

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

**The goal would be 0% of malicious email download. It is important to continue to educate and remind employees on the subject.**

Step 2:

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

**CEO: Oversees the departments and makes sure jobs are being done appropriately.**

**CFO: Financial planning and gives final approval for budgets**

**IT Department: implementing the plans listed above, helping create policy and educating the employees on ways to mitigate a breach.**

**Human Resources: Keep track of employee and disciplinary actions for not following the policies.**

Step 3:

**Training will be done once every month so that the information is still fresh in the employees heads. Also with all the new ways hackers are attacking it's good to stay current. I would host a fun training course online and an in person information briefing.**

**My training would cover the risks of clicking on and downloading suspicious emails and also logging in on unsecured WiFis. I would show examples of what can happen and the destruction that can come from not being careful.**

**After the training, I will randomly send out a fake malicious email and wait to see who clicks on it, and if they download it. I then would then be able to see the numbers and how effective the training is. For those who fall into the trap I will shut their computer completely off just to scare them a little bit. Then I will sit down with them individually and actually show them that I can see everything they are doing from my computer and how dangerous it can be.**