Step 1: Measure and Set Goals

1. Three risks that could come up from having employees access work information on their personal devices are: Man in the Middle attacks, Malware attacks and the possibility of the device being stolen, and sensitive data being taken and/or sold.
2. For man in the middle attacks, a good encryption on data being sent and received would help prevent that. For Malware, making sure there is a good anti-malware software on the personal device would help keep malware from being an issue. Lastly, for devices being stolen, keep any sensitive data and passwords off of personal devices, and keep track of personal devices at all times.
3. Two ways I would use to measure on how employees are behaving is one through surveys about what they do for work on their personal devices, and lastly would be monitoring any data that comes to and from personal devices, and making sure that all data is encrypted.
4. An ideal goal to reach would be less than 5% of people leaving any sort of passwords or sensitive data on their personal devices, and having up to date anti-malware services. Lastly, less than 10% having a way to encrypt data on their personal devices.

Step 2: Ivolve the Right People

1. The first and most obvious person would be the CEO. The CEO’s job is to make sure the company as a whole is running smoothly, so informing them of something like this, which would involve anyone in the company, is a must.
2. The second person who needs to know is the CISO. This is another obvious one, as they are in charge of all information and data security, thus they will have a key word in this process.
3. The third is the HR department. This is less obvious, but due to it also potentially conflicting with employee’s privacy, they need to be informed so they can also aid in anything that might arise during this monitoring and questioning process.
4. The fourth is the COO. Due to the COO overseeing the daily operations of the company, they are essential in this process, as it can help with both the efficiency and security of the company.
5. The last is the CIO. This is because while the CISO is responsible for the security of information, the CIO is responsible for the information itself. They will also play a key role in making sure that all data can and will be encrypted at all times.

Step 3: Training Plan

1. Training should take place at least once a week, with recurring sessions annually afterwards. It can be done online, but having it recurring annually will help keep both newer and older employees from laxing on security, and it will help keep employees who aren’t as tech savvy up to date on good software to have.
2. The main things that would be covered are, why they need to have data encrypted, why they need to keep security software up to date, and lastly, why not to keep sensitive data and passwords on the computer. On top of that, more than just why, it will also include potential solutions or suggestions for those exact issues.
3. After the training, other than continuing to monitor the amount of incoming data that is encrypted, another survey will be asked every few months to see how much of a difference the training is making, and if it lasts.