Office of the Chief Information Security Officer
Risk Advisory: Smartphone Configuration

BACKGROUND

When University of Washington (University) employees use their smartphones to respond to work emails, download files with institutional information, and access University applications, it represents a potential risk to the confidentiality, integrity, and availability of institutional information where much of the risk management is the responsibility of the individual employee.

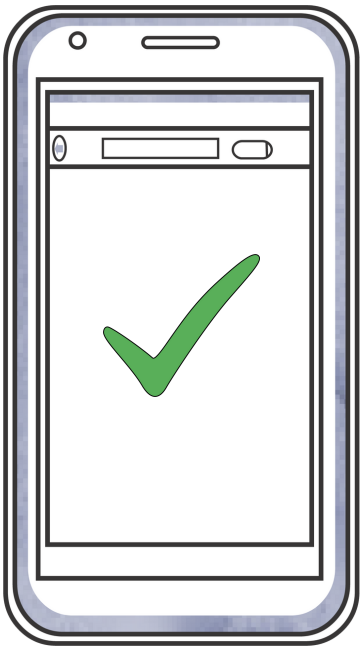
BEST PRACTICES

If you use a University or personally owned smartphone to conduct University business, the Office of the CISO encourages you to consider the following settings to help protect the information and secure the smartphone.

- **Encrypt the device** to help protect the information from being accessed by unauthorized individuals if the device is lost or stolen
- **Select an alpha-numeric pass code or PIN** to limit unauthorized access to the smartphone. Do not share your pass code or PIN with other individuals.
- **Lock automatically after a few minutes of inactivity** (for example between one and five minutes). The pass code or PIN should be required to be entered in order to unlock the smartphone.
- Configure the smartphone to completely erase itself or **"wipe" after multiple consecutive incorrect attempts** (for example 10 invalid pass codes or PINs)
- **Configure remote wipe for your device.** This can be accomplished through functionality in current versions of Microsoft Exchange, or through your cellular provider or phone manufacturer
- If the smartphone uses a SIM card, then **configure SIM PIN** and configure the smartphone to require the SIM PIN whenever the SIM card has been replaced.

- **Back up the information stored on the smartphone** on a regular basis to help recover the information in the event that the smartphone is lost or stolen and you initiated a remote wipe, you forget the pass code or PIN, or the pass code or PIN is accidentally entered incorrectly multiple times in a row and you have set the above wipe or erase feature.

This list represents its examples of configuration settings that can help to secure the smartphone and protect the information stored on it. This list is not exhaustive. Other information security settings may apply to the particular smartphone you are using. For additional information, consult with your department IT support person or University smartphone support contact.



For instructions on how to implement these settings, please refer to the user manual for the smartphone or consult with the cellular provider or manufacturer.