Guidelines for Business Use of User Owned Devices (Bring Your Own Device - BYOD)

Business Units (BU) may authorize access to state systems for business purposes utilizing User Owned Devices (UOD). Employees accessing state systems from UODs are subject to the following::

1. Have agency approval to use UOD to access agency and/or state systems.
    a. Storage or access of Confidential information on UODs or User Owned Cloud Storage is prohibited unless approved by agency Privacy Officer and Information Security Officer.
2. Ensure UODs meet minimum hardware and software specifications;
    a. UOD must run the operating system (OS) provided by the Original Equipment Manufacturer (OEM) and service provider and be currently supported by the OEM/ service provider (e.g., non-rooted, non-jail-broken).
    b. UOD OS and applications shall be patched and kept up to date.
3. Users must not:
    a. Allow anyone else to use UOD when logged into agency or state systems.
    b. Give anyone else your agency or state login information and password.
4. All agency and statewide policies and standards apply to UODs and access to state systems from UODs including, but not limited to:
    a. Software to ensure policies and standards are followed may be installed on your UOD. State personnel may request access to UODs to install and configure required policies.
    b. Access to the UOD will be protected with a password.
    c. After 5 minutes of inactivity on the UOD and some UOD connected devices (smart watches, etc.), password reentry is required to unlock the device.
    d. After ten failed login attempts, the device is locked. The device will remain locked until a system administrator unlocks the device.
    e. A remote wipe may be performed as deemed necessary by the State. Examples of when a remote wipe may be necessary include, but are not limited to: employee termination, malicious code infection, lost or stolen device, or prolonged absence from the State. The State will attempt to selectively wipe only State content unless you request a full wipe or a selective wipe is not technically

feasible. However, the State is not responsible for any non- information lost as the result of a remote wipe.

f. Users must not disable or alter the settings for information security software or enforcement functions on UODs.

5. UODs and non-state information on UODs are the responsibility of the device owner. The State is not responsible for technical or other issues, including information loss, occurring on UODs.
6. Individuals using UODs for business use shall notify the State of UOD loss or suspected security compromise, and what actions have been taken, immediately but no later than twenty four (24) hours from the time of the loss or suspected security compromise. Notification can be done by contacting your agency Service Desk, either via email or phone.
7. The State will respect the privacy of your personal device and will only request access to the device by technicians for the following purposes:
    a. To implement security controls, as outlined above; or
    b. To respond to public records requests or legitimate discovery requests arising out of administrative, civil, or criminal proceedings.
8. When possible, separate information from non- information on UODs.
9. Know and comply with agency data retention policies for data or information created when conducting business (text messages, photos, documents, emails, etc.).
10. Hourly or non-exempt employees opting-in to using UODs for business use are discouraged from accesing agency or systems outside their work hours.