**Chase Mobile Standards Document**

**STANDARD FOR AGENCY POLICIES**

1. Require periodic audits of device to ensure:
   1. Settings have not been changed.
   2. Antivirus is running and cannot be disabled.
   3. Application updates are occurring when released.
   4. No new applications have been installed.
2. Assigned person to configure devices.
3. Periodic training on proper device usage for authorized users.
4. Use only Apple, LG and Samsung (v. 2 and later) devices.

**DEVICE HARDENING STANDARD**

1. Device must be dedicated to payment acceptance.
2. Install antivirus application that runs automatic scans (N/A for iOS).
3. Set to limit ad tracking.
4. Set to do not send diagnostic data (N/A on android)
5. Register with MDM (https://dts.utah.gov/mdm-mobile-device-management).
6. Install Chase Mobile Checkout application.
7. Password Manager/ Auto-fill must be disabled.
8. Security controls must be turned on.
9. Unnecessary applications and widgets must be disabled/ uninstalled.
10. Internet browser must restrict access to only necessary functions.
11. App store must be configured for automatic updates.
12. Establish PIN or Password. Different than security PIN/password.

**CHASE MOBILE HARDENING PROCEDURE**

**On iOS:**

1. From the home screen, click and hold any application🡪 when the applications start wobbling, click the X on each application that is not necessary for payment functions. (Note iOS native applications cannot be deleted.)
2. Go to: Settings application 🡪 select Privacy 🡪 select Analytics 🡪 Turn off “Share iPhone Analytics”
3. Go back to Privacy 🡪 Select Advertising🡪 Turn on “Limit Ad Tracking” then select “Reset Advertising Identifier…”
4. Go to App Store application🡪 Search for “Chase Mobile Checkout” 🡪 select “Get”
5. On Desktop computer, go to: https://dts.utah.gov/mdm-mobile-device-management🡪 Click iOS Device 🡪 Follow instructions in guide.
6. Go to: Settings 🡪 select General 🡪 select Keyboard 🡪 disable “Auto-Correction” and “Predictive”
7. From Settings, General 🡪 Select Handoff 🡪 Disable “Handoff”
8. From Settings, General 🡪 Select Background App Refresh 🡪 Disable “Background App Refresh”
9. From Settings, Select Screen Time 🡪 Select “Turn on Screen Time”, “Continue” and “This is my iPhone.” When Screen Time populates, select “Use Screen Time Passcode” and create a security passcode that is different from the screen passcode that was created in the MDM steps.
10. From Settings, Screen Time 🡪 Select “Content & Privacy Restrictions”. Select “iTunes & App Purchases” 🡪 Change “Deleting Apps” and “In App Purchases” to “Don’t Allow.” Leave “Installing Apps” set to “Allow”.
11. Go back to “Content & Privacy Restrictions” and select “Allowed Apps”. Disable “FaceTime”, “Camera”, “Siri & Dictation”, “Wallet”, “AirDrop” and “CarPlay.” If “Safari” and “Mail” are not required, disable these as well.
12. Go back to “Content & Privacy Restrictions” and select “Content Restrictions”. Change “Movies” and “TV Shows” to “Don’t Allow.” Turn “Music Profiles & Posts” to “off”. If “Safari” was left enabled in the previous step, select “Web Content” and change to “Allowed Websites Only”. Enter *only* the sites that are required for business dealings. Select and remove all other sites.
13. From Settings, Go to: iTunes & App Store 🡪 Disable: “Music” and “Apps”. 🡪 Enable “Updates”

**On Android (Only LG and Samsung Galaxy S2 and later allowed):**

1. Go to Settings 🡪 Select “Apps”🡪 Select each downloaded apps🡪 Uninstall each app that is not necessary (if uninstall is not available, disable and/or force stop).
2. Go to Play Store 🡪 Search for “Chase Mobile Checkout” 🡪 select install
3. From Play Store 🡪 Search for “antivirus” 🡪 select an antivirus that can run automatically. Preferred applications are: Avast! Mobile Security & Antivirus (Free) or Symantec Mobile Security Agent ($1.00/month fee)
4. Configure Antivirus App to run scheduled scans and to protect device from uninstall.
5. On Android Device From Settings 🡪 Select “Security”🡪 Disable: “Widgets”, “Unknown Sources”: enable “Verify Apps”
6. From Settings, Security🡪 select “Auto-Start Management”🡪Deny all
7. From Settings: disable any network connections not required for connectivity (i.e. Near-field communications)
8. From Home, go to Google Settings 🡪 Select Ads 🡪 Select “Opt out of interest based ads” and reset advertising ID.
9. From Home, select Browser🡪 select Settings🡪 select General 🡪 disable autofill
10. From Browser, settings🡪 select privacy & security🡪 clear cache, clear history, clear all cookie data, clear for data, clear passwords. Disable: Remember form data, Remember passwords.
11. From Home, select Google Play 🡪 select Settings 🡪 Turn on “auto-update apps”, Require authentication for all purchases.
12. From Home, remove all app shortcuts besides Chase Mobile Checkout.
13. On Desktop, go to: https://dts.utah.gov/mdm-mobile-device-management 🡪 Click Android Device 🡪 Follow instructions in guide.
14. From Home, follow the instructions on this link: <http://www.androidcentral.com/how-use-android-43-s-restricted-profile-feature>. Restrict the device to allow settings, Airwatch and the Chase Mobile Checkout.