

NOAA Rules of Behavior for Mobile Devices

The purpose of this document is to outline the conditions NOAA requires to allow mobile devices to connect with NOAA systems including email. By signing this agreement the user agrees to abide by the NOAA IT Rules of Behavior, all other Department of Commerce, NOAA and Line Office IT Security Policies. In addition, the following will apply to any Mobile Devices configured to access NOAA systems including email. Specifically:

- NOAA and /or Line Office will install an IT Security Profile on all devices that connect to NOAA systems. The configuration may make some applications unusable. NOAA and or Line Offices are not responsible for the cost or support of such applications.
- The user understands and agrees that all data on the device may be accessed and reviewed pursuant to government investigations and / or litigation. The user further understands that they may be without access to the device as a result of the review. NOAA and / Line Office are not responsible for any cost for loss of use as a result of a review.
- Any device found to have attempted to change NOAA or Line Office installed security controls will be immediately wiped and removed from access to NOAA systems.
- NOAA and / or Line Office will not be responsible for costs or support associated with non-work related applications.
- Except for UMS data (email, calendar, contacts, and NOAA Google Documents) configured and managed by the processes published by NOAA, no government data may be stored on any device or location unless such storage is specifically authorized in the system security plan. .
- Mobile devices may not be physically connected to NOAA systems or computers. This includes the use of USB chargers connected to a NOAA computer.
- NOAA and /or Line Office reserves the right to remote wipe devices at anytime with or without notice to the user.
- NOAA and / or Line Office may install security and management related software on mobile devices.
- NOAA and / or Line Office will not be liable for any loss of data or applications resulting from a remote wipe.
- Prior to taking the mobile device outside of the United States, for either business or personal travel, the user must notify the Line Office IT Security Officer or individual designated by the Line Office:
 - Dates of travel
 - Countries of travel including stopovers and layovers
 - Identify any sensitive data that will be on the mobile device during travel
 - Comply with organizationally defined practices including maintaining possession of the device at all times, disabling WiFi and Bluetooth services, and such other controls as the Department of Commerce Office of Security (OSY), NOAA, or Line Office may impose
 - The user understands that the device will be wiped immediately upon return to the United States.
- As devices and operating systems continue to proliferate and change, NOAA and / or Line Office cannot guarantee that any specific device, operating system or application version will work or continue to work in the NOAA environment.

User Acknowledgement and Acceptance

I certify by my signature below that I have read and fully understand this document and agree to comply with its contents. I also understand that failure to comply may result in my device being immediately wiped, possibly without prior notification. I also understand and agree that as a result of this action by NOAA, personal data and applications may be lost.

Requester

Date

Line Office Approving Official

Date