

NOAA Mobile Device Security Policy

Introduction

Mobile computing devices, smart phones and tablet computers, are important tools for the organization and their use is supported to achieve business goals. However, mobile devices also represent a significant risk to sensitive data and systems if appropriate controls are not applied.

NOAA and its component Line Offices have a requirement to protect its information assets in order to safeguard sensitive data including Personally and Business Identifiable Information, and other sensitive data. This document outlines a set of practices and requirements for the use of mobile devices.

Scope

1. This policy applies to all mobile devices that have access to Government networks, data and systems. This includes smart phones and tablet computers except as noted below.
 - a. This policy does not apply to laptops encrypted, maintained and used in accordance with applicable NOAA policy and requirements
 - b. Devices that access government data exclusively through an official web portal and do not otherwise store or retain government data on the device.
2. Exemptions from this policy may be granted by the NOAA CIO or designee, on a case by case basis, after:
 - a. Demonstration of sufficient business need and;
 - b. Completion of a risk assessment by security management.

Policy

Effective January 1, 2012:

1. Unless otherwise specifically stated in this policy, all Department of Commerce and NOAA IT security policies apply to mobile devices used to access NOAA systems.
2. Line Offices may require and enforce additional enhanced security controls.
3. Devices that connect to NOAA systems, except as specified as excluded in the Scope Section of this document, must be managed by a NOAA and / or Line Office mobile device management system. The management system may do or enforce the following:
 - a. Devices covered by this policy may not be used to access or store classified data.
 - b. All Government data on devices that connect to NOAA systems must be encrypted to a level approved by the NOAA CIO. This will be at least AES 256 encryption.
 - c. Devices that connect to NOAA systems must be configured with a password that complies with NOAA password policy.
 - d. Require the installation of security- and/or management-related software on mobile devices.
 - e. Perform an inventory of applications and data on the device.

- f. Block the installation or remove applications.
 - g. Managed devices may be wiped without notice in the event of a security threat or violation of policy.
 - h. Applications on mobile devices covered by this policy must only be installed from approved sources and may be restricted by NOAA or Line Offices.
4. Except as required for limited technical support, mobile devices may not be physically connected to NOAA systems or computers. This includes the use of USB chargers connected to NOAA computers.
5. Mobile device users must notify Line Office IT Security Officer or individual designated by the Line Office prior to any international travel. At a minimum, the Line Office IT Security Officer or individual designated by the Line Office must document:
 - a. the dates of travel;
 - b. countries of travel, including intermediate stopover;
 - c. the nature and sensitivity of any data carried on the mobile device;
6. For International travel, the Line Office Security Officer or individual designated by the Line Office must:
 - a. Instruct the user on the proper protection of the mobile device.
 - b. Advise the user to review the Department of Commerce Office of Security (OSY) policies and to contact OSY.
 - c. Ensure that any NOAA or Line Office or Staff Office defined sensitive data is appropriately encrypted at the file level (i.e., in addition to device-wide encryption).
 - d. WiFi and Bluetooth connections are disabled for the period of travel.
 - e. Ensure that the device is wiped immediately upon return to the United States.
7. Except for accessing the Unified Messaging System, as specifically stated as an Exemption above, the Accrediting Official or the NOAA CIO must approve any mobile device that connects to any system. End users must sign a NOAA Mobile Device Rules of Behavior prior to being granted a connection to NOAA systems from a Mobile Device. The Rules of Behavior must be signed annually.
8. At such time as the training becomes available, end users must take the NOAA Mobile Device Security Training within 30 days and annually thereafter.
9. NOAA and / or Line Offices may enforce enhanced security controls based on the user's access to sensitive data with mobile devices. Enhanced controls may include, but are not limited to restrictions on installing applications, restrictions on web access, increased password complexity, and increased encryption strength.
10. Any user of a mobile device covered by this policy must report a lost or stolen device to a Line or Staff Office help desk within one hour of discovery that the device is no longer accounted for. The Line or Staff Office will coordinate with NCIRT and other units consistent with established escalation processes.
11. If a user suspects that unauthorized access to a mobile device that is covered by this policy, they must report the incident as required by NOAA's IT Security incident handling policy.

12. Failure to comply with these requirements may result in the termination of mobile device connection to NOAA systems and the wiping of the device.