National Aeronautics and Space Administration

Headquarters
Washington, DC 20546-0001

AUG 27 2013

Office of the Chief Information Officer

Reply to Attn of:

TO: Distribution

FROM: NASA Chief Information Officer

SUBJECT: Minimum Security Requirements for Personal Mobile Devices

Mobile devices like smartphones and tablets are playing an increasingly important role in our lives. Some of us have access to a mobile device provided by NASA, and many others have personal devices we would like to use to help accomplish our work. In the coming months, we will be working to develop a formal policy to govern the use of personal devices to access NASA information, also known as "Bring Your Own Device (BYOD)." Until then, I have directed the End User Services Office to enforce a minimum set of security requirements on any personal mobile device[1] that attempts to access the NASA email system, just like is currently done on NASA's government-issued devices.

This change, effective September 10th, will automatically enforce a minimum set of security requirements on your personal mobile device if you wish to access NASA's email and calendaring resources. These requirements include:

- Your personal device will be required to have an unlock code of no less than 4 characters
- Your personal device will be required to automatically lock after a period of inactivity of 15 minutes or less
- Your personal device will be required to use any available native encryption[2]
- Your personal device will be required to automatically erase/wipe itself after 10 unsuccessful login attempts
- Your personal device can be remotely wiped in the event it is lost or stolen *(NOTE: NASA will not utilize this capability unless explicitly requested by the user)*

Although most commercially available devices can accept these minimum security requirements, NASA cannot accommodate every single model, brand, and type of personal mobile device that may exist. As a result, there is a potential that some, mainly older devices

1 For the purposes of this memo, a "personal mobile device" is any device that is not provided by NASA, and which is running a mobile operating system, i.e., an operating system specifically designed to run on mobile devices such as mobile phones, smartphones, PDAs, tablet computers, and other handheld devices. Examples of mobile operating systems include Apple's iOS, Google's Android, RIM's Blackberry, etc.

2 "Native encryption" refers to the data at rest encryption provided by the device itself; this is different than the Entrust product that NASA uses to encrypt documents and emails within NASA. Beginning September 10th, NASA will enforce any native encryption capabilities that are built into and available on the device itself.

may not be able to meet these minimum security requirements, and may not be able to continue accessing NASA email once this change is applied.[3]

In addition, adherence to the following practices is expected while using personal devices to perform NASA work:

- If a personal mobile device that has been used to access NASA resources is lost or stolen, the NASA Security Operations Center[4] must be notified immediately, or as soon as practical after the device is discovered to be missing.
- All sensitive information must be fully encrypted and protected in accordance with NASA policy[5].
- Prior to separation from NASA service, or prior to disposing of a personal mobile device in any way (e.g. trading it in for an upgrade, selling or giving it to another individual, or otherwise relinquishing physical possession of the device.), all NASA information must be deleted from the device, including any removable storage media used in the device.
- If a personal mobile device is used to access or store NASA business information, neither the device nor the NASA data therein may be shared or provided to others who are not authorized to access the NASA data.
- All personal mobile devices must be maintained and kept up-to-date with security patches and updates released by the manufacturer.
- Personal mobile devices must remain configured as prescribed by the manufacturer, vendor, or service provider, and must not be configured to allow users to bypass standard, built-in security features and controls (i.e. jail-broken, 'rooted', etc.).
- Personally owned devices must not be connected to the NASA internal hardwired network or internal wireless network unless permitted and facilitated via an approved NASA Virtual Private Network (VPN). (Connection to a NASA guest network is permitted.)
- The owner of the personally owned mobile device may be requested to provide access to the device for forensic examination if it or data contained within it is suspected of being involved in a security incident.

I ask that you take a moment to review and familiarize yourself with these requirements. Please keep in mind that any use of personal devices to access NASA data is purely optional. You should refrain from using a personal mobile device to access NASA information and systems if you are uncomfortable or unwilling to comply with these minimum security requirements. Individuals are solely responsible for the operation and maintenance of their personally owned devices. At this time, NASA does not provide any form of stipend or reimbursement for any cost incurred to meet the requirements of this memo or for any cost incurred as a result of using a personally owned device to conduct official business.

---

3 This capability is supported by most current mobile operating systems. To truly ensure compatibility, though, employees should maintain their device to the standards provided in NASA-STD-2804P. Additional details can be found in the FAQs at http://inside.nasa.gov/ocio/ under "Resources".

4 The NASA Security Operations Center can be reached at soc@nasa.gov or 1-877-NASA-SEC (1-877-627-2732)

5 Sensitive information is defined in NID 1600.55 (Sensitive But Unclassified (SBU) information) and includes personally identifiable information (PII), information in identifiable form (IIF), Privacy Act information, proprietary information, pre-decisional information, export controlled information (ITAR/EAR) and all other SBU. Encryption of sensitive data must be FIPS 140-2 Validated. Additional information can be found in the FAQs at http://inside.nasa.gov/ocio/ under "Resources".

Additional information and Frequently Asked Questions (FAQs) can be found at http://inside.nasa.gov/ocio/ under "Resources."

Thank you for all the work you do every day to help us achieve NASA's mission.

Larry Sweet
NASA Chief Information Officer

Distribution:

Deborah Diaz
Gary Cox
Valarie Burks
Jerry Davis
Lawrence C. Freudinger
Randy Humphries
Adrian Gardner
Jim Rinaldi
Jeff Seaton
Jonathan Pettus
Bruce O'Dell
Dinna Cottrell
Beverly Hamilton
Vanessa Stromer (Acting)
Annette Moore (Acting)
Victor Thompson (Acting)