HARVARD
UNIVERSITY
Information Technology

Mobile Device Security Requirements

Overview

The following requirements were recommended by the Mobile Device Security work group and endorsed by the CIO Council. These requirements apply to all mobile devices that may store or process Harvard confidential information, regardless of whether they belong to or are paid for by Harvard.

Requirements

All mobile devices that may store or process Harvard confidential information must:

- Have a passcode of at least 4 digits
- Have device encryption enabled
- Be configured to self-erase after 10 consecutive bad passcode attempts
- Have remote-wipe capability enabled
- Have a screen lock with maximum of 5 minute inactivity period