Aircrew Student Information Management System (ASIMS) Mobile Device Use Policy

This policy applies to all Salesforce's employees, including full and part-time staff, contractors, freelancers, and other agents (including members of the 97th Training Squadron [97TRS]) who use any mobile device to access, store, backup, or relocate any organization or client-specific data. The 97TRS will maintain an auditable storage of these policy letters signed by squadron members.

The policy addresses a range of threats to enterprise data, or related to its use, such as Device loss, Data theft, Malware, and Compliance.

Usage Restrictions

In order to enforce security and remote device management, only devices that meet the following criteria are allowed to access corporate resources:

- Smartphones, tablets, and other devices running Android version 2.3 or iOS 5.0 and higher
- Smartphones and tablets running OKTA Authentication Software
- Laptops running Windows 7 and higher or Mac OS X Cheetah (10.0) and higher

Addition of new hardware, software, and/or related components to provide additional mobile device connectivity will be managed at the sole discretion of our IT group. Unauthorized use of mobile devices to back up, store, and otherwise access any company-related data is strictly forbidden.

Implementation Guidance

Connectivity of all mobile devices will be centrally managed by Salesforce's IT department and will use authentication and strong encryption measures. Although IT will not directly manage personal devices purchased by employees, end users are expected to adhere to the same security protocols (outlined in this memo) when connected to non-corporate equipment. Failure to do so will result in immediate suspension of all network access privileges so as to protect the company's infrastructure.

Connection Requirements

The 97TRS reserves the right to refuse, by physical and non-physical means, the ability to connect mobile devices to corporate and corporate-connected infrastructure.

- Prior to initial use on the corporate network or related infrastructure, all mobile devices must be approved by the ISSO. The 97TRS will maintain a list of approved mobile devices and related software applications and utilities. Devices that are not on this list may not be connected to corporate infrastructure. If your preferred device does not appear on this list, contact the ISSO at adrian.perry-rountree@us.af.mil. Although IT currently only allows listed devices to be connected to enterprise infrastructure, it reserves the right to update this list in the future.
- End users who wish to connect such devices to non-corporate network infrastructure to gain access to enterprise data must employ, for their devices and related infrastructure, security measures deemed necessary by the IT department. Enterprise data is not to be accessed on any hardware that fails to meet Salesforce's established enterprise IT security standards.
- All personal mobile devices attempting to connect to the corporate network through the Internet will be inspected by Salesforce's IT department. Devices that are not approved by IT, are not in compliance with IT's security policies, or represent any threat to the corporate network or data will not be allowed to connect. Devices may only access the corporate network and data through the Internet using a Secure Socket Layer (SSL) Virtual Private Network (VPN) connection. The SSL VPN portal web address will be provided to users as required. Smart mobile devices such as smartphones, tablets, and laptops will access the corporate network and data using mobile VPN software installed on the device by IT.
- Employees using mobile devices and related software for network and data access will, without exception, use secure data management procedures. All mobile devices must be protected by a strong password (a

PIN is not sufficient) and Two Factor Authentication (2FA) using OKTA. All data stored on the device must be encrypted using strong encryption. Employees agree never to disclose their passwords to anyone.

- All users of mobile devices must employ reasonable physical security measures. End users are expected to secure all such devices against being lost or stolen, whether or not they are actually in use and/or being carried.
- Passwords and other confidential data, as defined by Salesforce's IT department, are not to be stored unencrypted on mobile devices.
- Any mobile device that is being used to store or access 97TRS data must adhere to the authentication requirements (OKTA) of the Salesforce's IT department.
- IT will manage security policies, network, application, and data access centrally using whatever technology solutions it deems suitable. Any attempt to contravene or bypass that security implementation will be deemed an intrusion attempt and will be dealt with in accordance with Salesforce's overarching security policy.
- Students accessing 97TRS internet resources from a smartphone or tablet will NOT save their user credentials or internet sessions when logging in or accessing company resources of any kind.
- In the event of a lost or stolen mobile device, the user is required to report the incident to the 97TRS ISSO immediately.
- Usage of location-based services and mobile check-in services, which use GPS capabilities to share real-time user location with external parties, is prohibited within the workplace.
- Usage of a mobile device to capture images, video, or audio, whether native to the device or through third-party applications, is prohibited within the workplace.

IT can and will establish audit trails, which will be accessed, published, and used without notice. The end user agrees to and accepts that his or her access and/or connection to Salesforce's networks may be monitored to record dates, times, duration of access, etc. in order to identify unusual usage patterns or other suspicious activity. The status of the device, including location, IP address, Serial Number, IMEI, may also be monitored. This monitoring is necessary in order to identify accounts/computers that may have been compromised by external parties or users who are not complying with Salesforce's policies.
Any questions relating to this policy should be directed to Mr. Adrian Perry-Rountree in the 97TRS, at adrian.perry-rountree@us.af.mil.

Failure to comply with the *Mobile Device Use Policy* may, at the full discretion of the organization, result in the suspension of any or all technology use and connectivity privileges, disciplinary action, and possibly termination of employment.

Approved by:

SCHENK.ADDISON.WESLEY.1283425890

Digitally signed by SCHENK.ADDISON.WESLEY.1283425890
Date: 2025.07.08 09:42:00 -05'00'

ADDISON W. SCHENK, Lt Col,
USAF 97TRS DO/ASIMS PM

I, _____, have read and understand the above *Mobile Device Use Policy* and consent to adhere to the rules outlined therein.

Employee Signature

DOD ID#