Last Updated: 09-24-2025

Data Privacy and Security for Salesforce Mobile Application Use

By downloading, installing, or using the Salesforce mobile application on your mobile phone, tablet, or Chromebook, you acknowledge and agree to the following:

Securing Mobile Devices

- Mobile devices are not currently subject to the same UCR Security Toolset requirements as computers and laptops*. However, it remains your responsibility to secure your device to protect institutional data.
- You must:
  - Use strong passwords or biometric authentication.
  - Keep operating systems and applications up to date.
  - Exercise caution when using public Wi-Fi for sensitive activities.
  - Remain vigilant against phishing attempts.
  - Maintain regular data backups.
- *Note: Microsoft Surface Tablets require installation and use of the UCR Security Toolset to access UCR resources.

Use of Personal Devices

- University-owned and managed devices should be used for University work.
- If you choose to use a personal device subject to the UCR Security Toolset requirements to access secure UCR resources (including Salesforce), the UCR Security Toolset must be installed and running on that device.
- All records related to the use and disposition of equipment used for University work are potentially subject to disclosure under the California Public Records Act. This equally applies to personal devices, potentially subjecting personal information to disclosure.

Data Privacy and User Responsibility

- Access to Salesforce may involve confidential and sensitive University data, including personal information of students, alumni, donors, community, friends, and staff. Such data must be used only for official University business, in compliance with University policies and applicable laws.
- You may not download, copy, share, or otherwise store Salesforce data outside the authorized application or secure University systems. Do not export Salesforce data and use it in a shadow system.
- Lost, stolen, or compromised devices must be reported immediately to the Director of Constituent Management & Technologies.
- Unauthorized use, disclosure, or mishandling of Salesforce data may result in disciplinary action and potential legal consequences.
- The University is not responsible for loss of personal data, device functionality, or costs associated with use of the Salesforce mobile application.