Procedures to Accompany the Mobile Applications Implementation Policy

Introduction

The Mobile Application Implementation Policy calls for approval of all mobile application development and procurement that include data from UNLV enterprise systems; uses or collects protected data; requires UNLV infrastructure; or uses the UNLV brand.

The procedures outlined below describe:

- How the approval process works
- Special security concerns related to mobile applications
- Information about the Mobile Applications Group
- Frequently asked questions

Information about Seeking Approval to Procure or Develop a Mobile Application

In accordance with the Mobile Application Implementation Policy, any campus constituent or unit planning to develop or procure a mobile application, or hire a vendor to assist in the development of a mobile application, must seek formal approval to proceed if the application meets any one of the following criteria:

1. Accesses data from or pushes data to a UNLV enterprise system
2. Accesses or collects data that is protected by federal or state laws/regulations, or NSHE/UNLV regulations or policies
3. Requires infrastructure services managed by UNLV
4. Will be branded as a UNLV product which must be done to adhere to both UNLV graphic identity standards and in accordance with the UNLV Licensing Program

<u>Steps in Seeking Approval for Developing or Procuring a Mobile Application</u>

1. Complete the **Mobile Application Request Form** available at: http://oit.unlv.edu/forms/mobile-apps
2. The information provided on the request form will be reviewed within seven business days
3. You will be informed as to the next steps in the process, which could include any of the following:
   a. No further action is required.
      Based on the information you provided, the mobile application you propose to build or procure does not require formal committee approval.

   b. Completion of the **Mobile Applications Supplemental Information Form** is required. The questionnaire is available at: https://unlv.co1.qualtrics.com/jfe/form/SV_5ptQFwit96Ghljv

Based on the information you provided, the mobile application you propose to build or procure meets the criteria to require formal committee approval.

c. A meeting with the Mobile Applications Group.
Based on the information provided, a discussion with the full Mobile Application Group is warranted.

Complying with UNLV Security Policies and Procedures

All applications developed or purchased for use at UNLV must be designed to protect the confidentiality, integrity, and availability of university data and the privacy of members of the university community as well as the users of the application.

Mobile devices present a number of special security vulnerabilities:

- Because of their nature, mobile devices travel outside of the workplace and outside of the UNLV protected network. Moreover, they can be easily lost or stolen, potentially exposing university data to the finder or thief.
- Mobile devices rely on wireless communication and are sometimes used on public, unsecured wireless networks.
- Because mobile devices are often personal property, university applications often coexist with personal applications that may provide security vulnerabilities.
- Although biometric and other strong authentication to mobile devices is available, it is difficult to enforce authentication standards on personal devices. Many users employ weak authentication or none at all.
- Location-aware programs can provide data on the location of the mobile device and its user, information potentially useful to employers, thieves, and stalkers.

A number of precautions must be taken to minimize the impact of these vulnerabilities:

- Access to any potentially sensitive information requires authentication that meets UNLV password standards.
- All potentially sensitive, personal information must be encrypted in transit and when cached for use on the mobile device.
- Any downloaded data must be protected against access by other programs.
- No sensitive data should be stored on the mobile device once the application is terminated.
- Applications must not expose location information without the explicit consent of the user.

Related Documents

Those developing or procuring mobile applications must ensure compliance with the following policies and related procedures:

- Acceptable Use of Computing and Information Technology Resources
- Password Policy

Those providing the infrastructure for delivering mobile services and/or those who serve as the university liaison for vendors who are providing the infrastructure for delivering mobile services must ensure compliance with the following policy and related procedures:

- Technical System Administration Policy
- OIT Security Standards and Procedures for the Technical System Administration Policy

Exceptions to the Policy

- There are no predefined exceptions to the Mobile Application Implementation Policy.
- Exceptions will be made on a case-by-case basis

To request an exception, please complete the OIT Policy Exception Form.

Exception requests will be processed within 10 business days of receipt of the request. If an exception is created, the exception will be audited on an annual basis. The developer of the application or the contact for the third party developer must respond to the annual audit and verify that the exception is still required.

Changes to the exception may only be requested by the developer of the application or the contact for the third party developer.

The Mobile Application Group

Members

Area Represented	Position
Chair	Chosen from Committee by the Committee
Advancement	Assistant Director of Web Development
Executive Vice President & Provost	Associate Provost for Information Technology
Finance & Business	Appointed by Senior Vice President of Finance and Business
Office of Information Technology	Software Engineering Services Manager
Student Affairs	Executive Director of Enterprise Application Services
Technology Review Board Liaison	Representative Appointed by Technology Review Board
Ex-Officio	MyUNLV Mobile Application Developer

Logistics

The Mobile Application Group meets on a schedule determined by the group.

One member, selected by the group on a rotating basis, manages the mobile applications development or procurement requests and any additional questions received regarding mobile applications.

Contact Information

The Mobile Application Group can be reached via email at mobileappsgroup@unlv.edu.

Charges

The Mobile Application Group charges include:

- Serve as the formal approval body referenced in the UNLV Mobile Application Implementation Policy
- Ensure mobile applications comply with UNLV security policies and procedures
- Monitor use of the UNLV brand in mobile applications
- Manage mobile application developer programs including developer licenses available through those programs (e.g., Apple Developer Program)
- Develop and sustain a mobile strategy for providing enterprise mobile application services by:
    - Recommending the infrastructure architecture and support services for the development and use of mobile applications
    - Including mobility initiatives to connect future students, alumni, and community members to UNLV
    - Supporting mobile application development or acquisition and deployment to provide access to needed information and increase productivity for all major UNLV stakeholders
    - Including the unique security requirements associated with mobility (e.g., device security, application security, content security)
    - Providing incentives for innovation in mobile applications development and usages by students, faculty, and staff
- Keep the UNLV Mobile Application website current

Definitions

Mobile application - A software application designed to be installed and run on mobile devices such as smartphones or tablets.

Enterprise system - A large-scale application software package that supports business processes, information flows, reporting, and data analytics in complex organizations. Examples at UNLV include but are not limited to: student information system, human resources system, finance system, course management system, identity management system, space management system, etc.

Infrastructure services - Information technology services including but not limited to hardware, software, database, and/or cloud systems.

Sensitive, personal information - Any information about the individual maintained by the university, including the following: (a) Education, financial transactions, medical history, and criminal or employment history; and, (b) Information that can be used to distinguish or trace the individual's identity, including name, social security number, date and place of birth, mother's maiden name, or biometric records. [38 USCS § 5727(19)] Sensitive, personal information does not include publicly available directory information that may be lawfully disclosed. *(Definition taken from Breach of Information Notification Policy available at: https://oit.unlv.edu/about-oit/policies/breach-information-notification-policy)*.