Mobile Applications Approval Procedure

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

Steps in Seeking Approval for Developing or Procuring a Mobile Application

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_5ptQFwit96GhIjv
    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.