Overview

This policy sets forth the rules surrounding development and distribution of mobile applications (mobile apps).

Applicability

This policy applies to anyone who develops mobile applications at Emory or on behalf of Emory.

Policy Details

I. Mobile Applications Developed for Internal Distribution and Use

Emory requires a review of all internal mobile applications at Emory (developed at Emory or vended) prior to distribution to end users for production use. Internal mobile applications are those intended for use by Emory people and Emory affiliates only and not segments of the general public. This process is initiated by Library and Information Technology Services (LITS) in consultation with Legal Counsel and the Emory Healthcare and Emory University Compliance Officers. To begin this process, please visit https://wiki.service.emory.edu/x/7ILaB. Although internally distributed mobile applications do not have the same business and branding requirements as publicly distributed mobile apps, internal mobile applications have many of the same legal, compliance, and security implications. For this reason, Emory must perform a technical review, compliance and regulatory review, and a security review for internal mobile apps. If the mobile application involves cross-institutional collaboration, an intellectual property analysis by the Office of Technology Transfer (OTT) may be required to generate the necessary copyright notices and disclaimers. In addition, if the mobile application will be employed in research with human subjects, LITS may decline to distribute the mobile application for production use until authorization for the protocol is obtained from the appropriate Institutional Review Board (IRB). Mobile applications may be distributed internally to a limited user base for development and testing purposes prior to this review, but the reviews must be completed satisfactorily prior to distributing apps for production use.

Emory requires that all internal mobile applications developed at Emory, both native apps and mobile web apps, be distributed for production use using the Emory Mobile App Catalog. Mobile web apps may also be distributed by communicating a uniform resource locator (URL) or a launch web page in addition to listing them in the Emory Mobile App Catalog. This practice helps ensure that Emory can track mobile app usage, apply security policies, manage application updates, and otherwise support the applications. Some vended mobile apps may require distribution by the vendor or distribution through a public marketplace. These practices for vended applications are allowed when they do...
II. Mobile Applications Developed for Public Distribution and Use

Emory requires an internal review of all mobile applications developed at Emory prior to submission for distribution in public marketplaces, including but not limited to the Apple App Store and Google Play. This process is initiated by the Office of Technology Transfer in consultation with Legal Counsel, Marketing & Communications, and Library and Information Technology Services (LITS). To begin the process, please visit https://wiki.service.emory.edu/x/FqMIAw. As part of the Apple and Google submission processes for public distribution of mobile applications, parties distributing mobile applications must affirm their ownership of the intellectual property and accept marketplace terms and conditions, which include assuming some liability and accepting business obligations. Although Apple spends considerable effort tracking the ever-changing tax landscape, it is possible that errors and miscalculations can happen. If there is an underpayment assessment, the funding for that liability is not covered from a central source of funds. It will be up to the department, unit, or school to fund that expense in the unlikely event it were to arise. For these reasons, reviews of the intellectual property ownership status, marketability, and potential liability to Emory are essential.

Public distribution of mobile applications requires approval of four distinct Emory offices: Technology Transfer, Compliance, LITS Security, and Communications & Public Affairs. These reviews include an intellectual property analysis to generate copyright notices and disclaimers, as well as compliance and security analyses to ensure proper safeguards for user data and records. As necessary, the approval process may also involve the Office of General Counsel or Emory’s Institutional Review Board (IRB). In the event that the mobile application is to be used in research with human subjects, LITS may decline to publicly distribute the mobile application pending authorization from the appropriate Institutional Review Board. Upon the conclusion of the review process, remediations may be required to bring the application into alignment with Emory standards prior to distribution.

All mobile applications containing Emory intellectual property should be distributed through Emory’s public app store accounts unless other arrangements have been made and approved by the relevant mobile app approval groups. In addition, unless a compelling business reason can be provided, it is expected that Emory intellectual property meet Emory branding standards.

III. Mobile Applications Developed by Consultants or Vendors for Public Distribution and Use

If an app is not developed by Emory, but is developed and maintained by an external vendor on behalf of Emory and contains Emory intellectual property or is otherwise determined to be owned by Emory, the app should still be distributed through Emory’s public marketplace accounts unless other arrangements have been made and approved by the relevant mobile app approval groups. Specifically, if the app contains Emory’s name, marks, and branding, and if the app is intended to represent Emory to the public as an Emory-specific app, then it should be distributed through Emory’s official marketplace accounts. This is necessary for Emory to maintain the ability to coordinate its mobile marketplace presence and, most importantly, to disclaim any unauthorized rogue apps, which purport to be Emory apps and are not. Such apps can put Emory faculty, staff, students, and patients at risk. If external entities are allowed to distribute Emory-branded, public facing mobile apps, Emory users have no way of knowing which apps are legitimate and Emory has no effective way of disclaiming and shutting down unauthorized apps.

IV. Listing Publicly Available Mobile Apps in the Emory Mobile App Catalog

Emory requires a review of all apps available in public marketplaces that are listed for download in the Emory Mobile App Catalog. The process for reviewing mobile apps endorsed by Emory and listed in the Emory Mobile App Catalog is initiated by Library and Information Technology Services in consultation with Emory Healthcare and Emory University Compliance Officers and other groups depending on the particular nature or requirements of the mobile application. To begin this process, please visit https://wiki.service.emory.edu/x/suGBQ. These mobile apps are endorsed in some way by Emory when they appear in the Emory Mobile App Catalog and they should be reviewed and documented to indicate the nature of their review and recommended or endorsed use.

Sanctions: Failure to comply with this policy may have legal consequences and may result in:

- Suspension or termination of access;
- Disciplinary actions (up to and including termination of employment) in accordance with applicable university policy.

Related Links

- Current Version of This Policy: http://policies.emory.edu/5.16
- Emory Mobile App Review and Submission Process for Internal Emory Distribution (https://wiki.service.emory.edu/x/7ILaB)
- Emory Mobile App Review and Submission Process for Public App Marketplaces Distribution
Emory University policies are subject to change at any time. If you are reading this policy in paper or PDF format, you are strongly encouraged to visit policies.emory.edu to ensure that you are relying on the current version.