Mobile Application Review and Distribution Processes

Quck Links: **Emory Mobile App Dashboard** | **Emory Mobile App Data Request Dashboard** | **Public Mobile Distribution Process** | **Internal Mobile Distribution Process**

Policy for Emory *Public* Mobile App Distribution (Adopted October 14, 2014, revised December 8, 2017)

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 Emory mobile application owner via ServiceNow request and facilitated by the mobile application review coordinator, in consultation with the Office of Technology Transfer, Legal Counsel, the Office of Compliance, Communications & Public Affairs, and Library and Information Technology Services (LITS). To begin the process, please visit https://wiki.service.emory.edu/x/FqMlAw. 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. All mobile apps owned by Emory are to be distributed through official Emory channels (i.e., Emory marketplace accounts) unless special dispensation for another distribution method is obtained during the review process.

Emory must also determine if mobile applications collect, transmit, or store any sensitive data and, if so, ensure that Emory's FERPA, HIPAA, PCI, or other appropriate compliance obligations are met. Distribution of mobile applications to any external (non-Emory affiliated) people without completing Emory's mobile application review process is prohibited. Distributing mobile applications that one does not personally own may also be a violation of marketplace agreements.

Policy for Emory *Internal* Mobile App Distribution (Adopted November 17, 2014, revised December 8, 2017)

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 the Emory mobile application owner via ServiceNow request and facilitated by the mobile application review coordinator, in consultation with LITS, Legal Counsel, and the Office of Compliance. To begin this process, please visit https://wiki.service.emory.edu/x/7ILaB. While 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. 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 not introduce unmanageable risk to Emory.

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 LITS in consultation with Emory Healthcare and Emory University Compliance Officers and [list other parties here]. To begin this process, please visit https://wiki.service.emory.edu/x/suIGBQ (the same process as the Vended Apps in the next section). 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.

Draft Policy for Use of Mobile *Vended* Apps at Emory for Purposes Subject to Policy Compliance (work in progress, not yet approved or adopted)

Emory requires a review of all mobile apps used for purposes subject to Emory policy and regulatory compliance. These purposes include the acquisition, storage, and transmission of data that is subject to Emory compliance policies such as student information, employee data, and

protected health information. Mobile apps developed at Emory are already covered under internal and external distribution review policies. This process applies specifically to mobile apps available on public marketplaces like the Apple App Store, Google Play, and others as well as any mobile apps available through other distribution channels or individual developers, hereafter referred to as Vended Apps.

Emory requires that all Vended Apps that are intended to acquire, store, or transmit sensitive information be reviewed for suitability and compliance by the appropriate Compliance Officer and Information Security. Once approved, all Vended Apps will be listed in the Emory Mobile App Catalog along with a description of their approved use. To begin this process visit https://wiki.service.emory.edu/x/suIGBQ.

Processes

Here are the processes for mobile app review and distribution at Emory to address the requirements for internal and external distribution. Detailed descriptions of these processes are at:

- Emory Mobile App Review and Distribution Process for *Public* App Marketplaces
- Emory Mobile App Review and Submission Process for *Internal* Emory Distribution
- Emory Mobile App Endorsement and Listing Process for Apps Available in Public Marketplaces (*Endorsed or Vended*) (under development)

These processes may be updated from time to time. For example, Emory is presently using an interim internal app distribution mechanism, which leaves much to be desired. Emory is currently evaluating enterprise app store products with the goal of finding a product to support an improved internal mobile app distribution process.