UNIVERSITY OF ILLINOIS ADVANCEMENT INFORMATION ACCESS MANUAL EXECUTIVE SUMMARY

Access to Advancement information maintained by the University of Illinois Foundation and University of Illinois Alumni Association will be managed in accordance with a hierarchical information security classification scheme and corresponding access groups based on Advancement-related job functions and reporting lines. Highlights of the manual are provided below.

Advancement information is classified into four general categories:

- **Public** – Information in this category is available to the public and is limited to published materials. Examples: alumni magazines, publications for general distribution, published donor recognition, and external video productions. Storage: Protection is unnecessary. Use: This information may be freely circulated. Destruction: This information may be recycled directly and has no retention requirements beyond the useful life of the document.
- **Internal** – Information classified in this category is for internal use by University of Illinois and URO employees. This level of data is protected and can be transmitted to anyone within the university's Advancement community without encryption. Examples: General information given with consent to share, advancement summary, basic constituent information in regard to directory-level educational history, volunteer information, and relationships. Storage: This information requires minimal protection and can be shared within the Advancement community. Use: This information may not be released to the public without the permission of the custodians. Destruction: This information should be destroyed securely after the retention period has been reached.
- **Confidential (Sensitive)** – Confidential information is defined as proprietary and privileged with restrictions on access. Disclosure of this information would cause reputation and competitive harm to the University of Illinois, the Foundation, and/or the Alumni Association. Examples: Contact information collected with the understanding that it is not to be shared, pledges, deferred gifts, donation amounts, and advancement activities (contacts, relationship management details). Storage: This information is to be protected using appropriate measures such as encryption, physical protection, and secure destruction. Use: Confidential information may not be released internally or externally without the direct permission of the custodians. Destruction: This information should be destroyed securely and not retained beyond the records retention schedule.
- **High Risk (Restricted)** – High risk information is defined as data restricted by custodians, policies, regulations, and/or statutes. Examples: Records containing credit card numbers, bank account numbers, social security numbers, or other identifiers that can be used for identity theft. Storage: Information in this category requires protection with the use of firewalls and access restrictions. Use: Custodians exercise their prerogative in granting access to those employees requiring the information for business use. Destruction: This

information must be destroyed securely and within the times required by the records retention schedule.

Access to Advancement information systems is granted based on an individual's role within the Advancement community. Requests for new accounts and changes are handled through designated Security Contacts in one of the following offices:

- University of Illinois Alumni Association – Security Contact: President (or designee)
- University of Illinois Foundation – Security Contact: Vice President for Advancement Services (or designee)
- UIS Office for Advancement – Security Contact: Vice Chancellor for Advancement (or designee)
- UIC Office for Advancement – Security Contact: Vice Chancellor for Advancement (or designee)
- UIUC Office for Institutional Advancement – Security Contact: Vice Chancellor for Institutional Advancement (or designee)

In order to obtain access to systems, UI employees are required to complete the UIF System Access Request Form (see Appendix B) indicating their unit affiliation, title, and functional job role. Applicants for access must read the confidentiality agreement (see Appendix A for full language) and check the box indicating they understand the nature of advancement information and agree to use it only for university-related purposes. Once the online form is completed, a paper copy is generated that the employee signs, along with her/his supervisor, and forwards to the appropriate office for approval.

Access to Advancement information is administered in a manner consistent with Advancement organizational structures at the University of Illinois and its related organizations. Access to systems is restricted largely to employees in Advancement reporting lines, along with Academic executives such as Deans, Department Heads, and their assistants.

Departments requesting access to systems are responsible for ensuring employees complete certain training to obtain or maintain access to Advancement systems. After submitting the access request form, users are required to attend the Welcome to Advancement course in UIF iLEARN Advancement online system prior to receiving access to TED.

Accountability guidelines are specified based on the nature of information misuse. Occurrences can range from minor to severe, and disciplinary actions can range from formal notification with a recommendation for further training to removal of access with a recommendation for termination of employment. Security contacts have initial authority to investigate, assess, and refer misuses of information to Advancement leadership.

The following general security groups form the basis for access to Advancement information:

Advancement Reporting Lines

- Advancement Support – Functional Roles: Human Resources/Professional Development, Support Staff for Advancement/Development, Student Worker for Advancement/Development. Information Security Class: Confidential II. Available Information: Constituent information (Limited)—Personal Info, Advancement Employment (Directory) Information, Relationships, Contact Information (Full), Constituent Documentation, Volunteer.
- Advancement Constituent Relationship Management (CRM) – Functional Roles: Events, Marketing/Communications. Information Security Class: Confidential III. Available Information: Constituent Information (Full), Revenue, Gift/Funding Agreement, Marketing and Communications.
- Advancement Officer – Functional Roles: Academic Executive (University President, Chancellors, Deans), Advancement Executive (UIF President and VPs, Advancement VCs, UIAA President), Unit Chief Advancement Officer/Director of Advancement, Major Gifts/Principal Gifts/Gift Planning, Corporate/Foundation Relations, Annual Giving, Alumni Relations, Donor Research and Analysis, Advancement Administrator, Stewardship/Donor Relations. Information Security Class: Confidential IV. Available Information: Full Prospect Information, Wealth and Ratings, Prospect Plans, Interactions, Opportunities.
- Specialized Roles – Functional Roles: Donor Research and Analysis, Gift Administration, Trust Relations, Information Technology, Alumni Memberships. Information Security Class: Confidential V. Available Information: Trust accounts, prospect analysis, gift acceptance, receipts function, training and support, records management and confidential agreements.

Non-Advancement Reporting Lines

- Advancement Constituent – Functional Roles: Alumni and Friends who use UIAA Directory and the UI Alumni Network. Information Security Class: Public. Available Information: Education (Directory), Contact (Limited).
- Business Manager – Functional Roles: Business Operations. Information Security Class: Confidential I. Available Information: Fund/Designation, Revenue (Limited).

Within Advancement report lines, security groups are hierarchical—access to Confidential III information implies access to Confidential II, Confidential I, etc. With approval of Advancement leadership, individuals may be granted access to higher security groups as their job responsibilities require. For example, an events administrator (Confidential III) who needs to create stewardship plans in TED can request access to Confidential IV information, and an Advancement officer's assistant (Confidential II) may be granted access to Confidential IV information in order to update and/or print plan information on behalf of his or her supervisor. Other than the Business Manager group, access to Confidential Advancement information is limited to Advancement reporting lines, defined as Alumni Relations, Development, and Marketing/Communications offices that report to Advancement. The only exception to that are Chancellors, Deans, and other Academic Executives who may request access at the Confidential IV level. Business managers are granted access (subject to approval) because, while often

not in Advancement reporting lines, they play important Advancement roles in gift acknowledgement and funds management.

Access to advancement information is authorized as appropriate and sufficient to secure private support for the University of Illinois in the areas of alumni relations, fundraising, marketing/ communications, and related business functions. The advancement security groups outlined above refer to broad categories of related information (i.e., gifts, pledges, trusts, and associated documents) and do not necessarily authorize access to specific information items or applications. University, UIAA, and UIF Advancement leadership retain authority to approve or deny access to specific types of information and/or applications.

Should any action that violates the confidentiality policy or protocols occur, the supervisor, the Foundation President, the Vice Chancellors for Advancement, or the Alumni Association President may use the following disciplinary guidelines:

- A *minor occurrence* is generally an unintentional or inadvertent misuse of information that causes minimal or no damage or potential damage to any constituent, the University of Illinois, or a University-Related Organization (URO).
- A *serious occurrence* is generally an intentional misuse of information that causes some damage or potential damage to any constituent, the University of Illinois, or a URO, or an unintentional or inadvertent misuse of information causing some damage that stems from negligence or casual disregard for confidentiality practices and principles.
- A *severe occurrence* is an intentional misuse of information that causes significant damage or potential damage to any constituent, the University of Illinois, or a URO, or an unintentional or inadvertent misuse of information causing significant damage that stems from negligence or casual disregard for confidentiality practices and principles outlined in this document, including appendices.

Severe violations will be handled by the Foundation President, a Vice Chancellor for Advancement, or the Alumni Association President and may result in immediate revocation of systems access, termination of employment where possible, or a recommendation for termination of employment where direct termination is not possible.

Alumni clubs and other volunteer organizations wishing to establish and operate nodes on the UI Alumni Network must sign and abide by the terms of the Participation Guidelines and Policies (PGP) document. The UIAA reserves the right to assume control of, or shut down completely, any Alumni Network nodes that violate the terms and conditions of the PGP.

This document is reviewed annually, and revisions must be approved by the UIF Executive Operations Team, consisting of the Foundation President, Executive and Senior Vice Presidents, Secretary to the UIF Board, and University Vice Chancellors for Advancement.

UPDATED - 11/02/2018