



URBANA-CHAMPAIGN



CHICAGO



SPRINGFIELD

# UNIVERSITY OF ILLINOIS ADVANCEMENT INFORMATION ACCESS MANUAL

# Contents

Confidentiality of Information.....	1
Advancement Information Systems .....	2
Data Classification.....	2
Access to Advancement Information.....	3
Training on Advancement Systems.....	4
Accountability.....	5
Destruction of Data.....	5
Use of Copyrighted Content in Advancement.....	6
Third Parties .....	6
Contact Updates .....	6
Information Security Groups.....	6
Advancement Reporting Lines.....	6
Non-Advancement Reporting Lines.....	7
Specific Access for UI Employees.....	8
Interruption of Access for Inactivity .....	8
Annual Review .....	9
Appendix A: University of Illinois Advancement Confidentiality Protocol Statement.....	10
Introduction.....	10
Purpose .....	10
Information Classification .....	11
Collection.....	11
Personal Use of Information .....	11
Retention of Advancement Information .....	12
Destruction of Information.....	12
Loss of Information .....	12
Release .....	12
Conclusion .....	12
Appendix B: UIF Systems Access Request Form and Confidentiality Agreement.....	14
Advancement Information Confidentiality Agreement .....	14

Use of Content.....	15
Agreement.....	15
Appendix C: Confidentiality Agreement for Volunteers .....	17
Introduction.....	17
Agreement.....	17
Appendix D: Vendor/Third Party Data Privacy and Security Agreement.....	18
Appendix E: Confidentiality Agreement for Club/Group .....	28
Appendix F: Advancement Data Access Plan .....	29
Information Security Classification .....	29
Add Advancement Administrator .....	29
Appendix G: Advancement Information Systems Reference Guide .....	34
UI Functional Job Roles .....	34
Confidential I: Business Manager.....	34
Confidential II: Advancement Support .....	34
Confidential III: Advancement Constituent Relationship Management (CRM) .....	34
Confidential IV: Advancement Officer.....	35
Confidential V: Specialized UIF/UIAA Roles.....	36
Data and Systems Inventory.....	38

## Confidentiality of Information

Two University-Related Organizations (UROs)—the University of Illinois Foundation (UIF) and the University of Illinois Alumni Association (UIAA)—maintain information on alumni, friends, prospects, and donors for the University of Illinois system for the purposes of Advancement. Access to the main Advancement information system for users is provided by UIF, and the UIAA maintains an Alumni Directory and IlliniLink alumni-student mentoring system that alumni and current students can access. In addition, the Gies College of Business and the Grainger College of Engineering maintain an alumni-student mentoring system similar to the UIAA's. Both of the UIAA databases and the Gies and the Grainger databases use data from the main UIF database.

The University of Illinois Foundation is responsible for training, security, and the integrity of the information contained in Advancement information systems for which it serves as custodian. In an effort to eliminate the need for separate databases and duplicate effort across universities, departments are strongly advised to use Advancement information systems for their constituent data needs. Units are strongly discouraged from maintaining local information systems.

The Foundation, the University of Illinois, and the Alumni Association are committed to responsible and appropriate collection and use of information in pursuit of legitimate institutional goals. Each organization supports the individual's fundamental right to privacy and subscribes to the following basic principles regarding ethics and confidentiality:

- The *principle of the right to privacy*. Every individual has the right to privacy. Consequently, information that is not available from public sources should not be disclosed except to the appropriate individual or department.
- The *principle of information necessity*. Only information that pertains to the capacity or inclination of an individual to become more fully engaged with the University of Illinois and related organizations is the proper subject for information collection.
- The *principle of individual ethical responsibility*. Any individual—whether an employee of this institution, a volunteer, or an outside consultant—is responsible for the ethical ramifications of his or her individual acts.
- The *principle of protection of confidential material*. Records about individuals and organizations are confidential should be used only by those staff members and volunteers who need to use them to further the legitimate missions of the institution.
- The *principle of record sensitivity*. Records have an enduring power and may improve or damage individual lives. Since records might become available to their subjects or to others who do not understand appropriate use of sensitive materials, everyone must ensure that records are not used in a harmful manner.
- The *principle of ethical collection*. Collection of data for Advancement systems is limited to public sources, correspondence, and constituent relationships. However, Foundation, University, and Alumni Association staff, agents, and volunteers shall not seek out or report public information of a personal nature such as that contained in documents related to

divorce, child custody, probate, or bankruptcy. Information collected should be stated in an objective and factual manner and attributed to the source. Information solicited from external or university sources shall be in accordance with state and federal laws.

## Advancement Information Systems

Advancement information is maintained in centralized systems including but not limited to:

Tracking and Engagement Database (TED) – The main database containing information on alumni, students, friends and donors (individual, corporations and foundations) to the University of Illinois.

- BBIS – Blackbaud Internet Solutions is a management system for web content that integrates with TED.
- Hyland OnBase – The document management system maintaining documents relating to transactions, correspondence and documentation supporting the business of Advancement.
- Blackbaud Data Warehouse – The data warehouse consists of a nightly download of data from TED with additional tables and calculated data elements for reports that are distributed to the Advancement community.
- UIF Online – A web portal to a variety of Advancement content including forms, fund content, and other Advancement information.
- UIF iLEARN Advancement – An online Learning Management system through which advancement employees can access training curricula, as well as the history of training they have completed.
- University of Illinois Alumni Network – Web access to alumni directory information and alumni club activities from around the world.

The Foundation is the custodian of data contained in TED for use by Advancement staff throughout the University, the Foundation, and the Alumni Association. The database contains development, stewardship, solicitation, gift transactions, research, communications, and biographical data. Users access the database and the content via a secure internet connection.

UIF Online is an intranet portal providing access to the Fund Database, Accounting information, and telemarketing reports.

## Data Classification

Information for University of Illinois Advancement is outlined in the Confidentiality Protocol Statement (Appendix A) and is classified into four 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

---

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 Advancement systems is restricted largely to University, UIAA, and UIF employees who report directly to Alumni Relations, Development, or Institutional Advancement, along with Academic executives such as Deans, Department Heads, and their assistants. Licensing requirements and/or resource constraints may limit the number of users outside of Advancement reporting lines who can be supported. However, the Advancement Data Access Plan (ADAP) (Appendix F) provides flexibility for expansion of access should reporting lines change and resources be identified to support increased numbers of users.

*Denial of Access and Appeals* – Access requests will be denied if deemed inconsistent with the ADAP outlined in Appendix F. Appeals will be made to the Security Contact at the appropriate University, who will refer the appeal to University Advancement, UIAA, and/or UIF leadership, as appropriate, for final disposition.

*Termination of Employment* – Units provided with access to Advancement systems are responsible for notifying UIF Advancement Information Management and Support (AIMS) ([aims@uif.uillinois.edu](mailto:aims@uif.uillinois.edu)) of all employee terminations or role reassignments.

## Training on Advancement Systems

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 and other Advancement systems. Additional training is required prior to being granted access to add or edit Volunteer or Committee records in TED.

UIF Learning and Development offers a variety of training courses and tutorials through the iLEARN online system. The Alumni Association provides training and user support for the Alumni Network and support for the Alumni Directory.

For a complete list of Advancement training courses offered by the Foundation, visit UIF iLEARN Advancement at <https://ilearn.uif.uillinois.edu/#/dashboard>.



## Accountability

---

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. Advancement information systems usage is monitored, and possible security violations are investigated as they become known. The Security Contact for the employee's university or URO has initial authority to characterize a violation as potentially minor, serious, or severe, and to initiate the notifications process in consultation with Advancement leadership. Depending on the nature of each occurrence, the Security Contact may recommend that two or more minor occurrences by the same individual constitute a serious occurrence, or that any number of serious and/or minor occurrences together constitute a severe occurrence.

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.

## Destruction of Data

---

Destruction of data is an important part of good information management practice. Hard copies of reports should be stored securely and shredded after use. Most information obtained from Advancement systems diminishes in value over time as updates are continuously added. Keeping such reports for extended periods of time increases the chances of loss. Information is most secure when stored within protected systems. Such information when held locally must be maintained separately from university information.



## Use of Copyrighted Content in Advancement

---

The University of Illinois and the Advancement community have policies about the capture, storage, and redistribution of copyrighted content such as news articles, obituaries, photographs and web content. Copyrighted materials belonging to entities other than Advancement and the University of Illinois may not be stored or transmitted by users via the computing resources provided. Failure to observe copyright or license agreements may result in disciplinary action from University of Illinois Advancement and/or legal action by the copyright owner.

## Third Parties

---

Volunteers, faculty, donors, clubs, and others partnering with the University of Illinois Foundation and the University of Illinois Alumni Association are required to sign Confidentiality agreements. Vendors with whom the UIF shares data are required to sign a Data Privacy and Security Agreement on which they agree to neither repurpose nor sell personal information and maintain numerous safeguards. Partners also agree to destroy all copies of the information after the conclusion of their engagement.

## Contact Updates

---

University of Illinois Advancement adheres to all applicable laws with regard to the use of telemarketing, email, and other methods of contact. University of Illinois Advancement provides individuals with the means to opt-out of receiving communications from the University, the Alumni Association, the Foundation, and partners. Users in areas subject to Europe's General Data Protection Regulation (GDPR) must specifically opt in to begin receiving communications.

## Information Security Groups

---

Appendix F shows the University of Illinois Advancement Data Access Plan (ADAP). Individuals in the Advancement community, academic executives, and staff outside of Advancement who perform vital Advancement functions such as stewardship and gift/funds management can access and/or update information within the Internal and Confidential security classification groups based on job functions. Advancement constituents themselves can directly access very limited Advancement information through the UIAA Directory and the UI Alumni Network. The following 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 Agreements, 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 and 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.

Appendix F also outlines several Confidential V and High Risk security groups that are specific to UIAA and/or UIF. Confidential V groups can access specialized screens and other applications used in

Advancement business processes that are not conducted in University units, including UIF Research, Technology Services, Cash Receipts, Gift Processing, Gift Administration, and Trust Services. High Risk groups consist of a small number of individuals who require access to bank information, credit card information, Social Security numbers, and the like, in order to conduct business transactions.

Appendix G provides an overview of advancement information systems and resources, including the security classification and host system(s) of all major advancement information resources.

## Specific Access for UI Employees

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.

In August 2020, the UIF, in consultation with the Universities and the UIAA, concluded an exhaustive review of access security roles pertaining to Revenue (Gift Transactions), Marketing and Communications (Solicitations and Mass Communications), and Prospects (Plans, Opportunities, and Interactions). As a result, fewer persons than before have access to add or edit Interactions (records of personal visits and other contacts between fundraisers and other advancement staff and constituents), Prospect Plans (sets of related planned and completed steps involved in maintaining relationships), and Opportunities (aspects of Plans that detail personal solicitations). The intent was to provide further protection for sensitive information within the information security groups described above.

## Interruption of Access for Inactivity

Also in August 2020, the UIF instituted the following protocols for inactive user accounts:

- For all TED and OnBase Users—Failure to take the mandatory Welcome to Advancement course (which includes Information Privacy and Security) in iLearn within 90 days of being enrolled will result in the account being deleted and require submission of a new Access Request Form if access is still needed. Inactive users (those who have not yet taken the required training after 90 days of enrollment) will receive email notices of impending deletion, two weeks, one week, and one day before deletion.
- For Student Employees—Accounts will be deleted at the end of each semester unless the student's supervisor (the person who signed his/her Access Request Form) indicates access should continue. The supervisor will receive emails asking if access should continue on the 15th and 30th day of the month before the end of each semester, and on the 5th day of the month in which the semester will end. If access is deleted, submission of a new Access Request Form will be required if access is still needed.

- For Business Managers—Accounts will be deleted after 18 months of inactivity. (Many Business Managers only log in once a year.) Submission of a new Access Request Form will be required if access is still needed. Inactive users (those who have not logged in to TED or OnBase after 18 months) will receive email notifications of impending deletion, two weeks, one week, and one day before deletion.
- For All Other Users—Accounts will be disabled after 90 days of inactivity. Accounts will be reactivated by email request within 90 days of being disabled. Accounts will be deleted entirely after those 90 days. If access is deleted, submission of a new Access Request Form will be required if access is still needed. Inactive users (those who still have not logged in to TED or OnBase 90 days after being disabled) will receive email notifications of impending deletion two weeks, one week, and one day before being disabled, and again two weeks, one week, and one day before deletion.

## Annual Review

---

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 – 7/20/2020

## Appendix A: University of Illinois Advancement Confidentiality Protocol Statement

Revised 6/27/2018

### Introduction

The University of Illinois Foundation, the University of Illinois, and the University of Illinois Alumni Association are committed to the ethical collection and use of information in the pursuit of legitimate institutional goals. We shall support and further the individual's fundamental right to privacy and subscribe to the following basic principles regarding ethics and confidentiality:

- The *principle of the right to privacy*. Every individual has the right to privacy. Consequently, information that is not available from public sources should not be disclosed except to the appropriate individual or department.
- The *principle of information necessity*. Only information that pertains to the capacity or inclination of an individual to become more fully engaged with the University of Illinois and related organizations is the proper subject to research.
- The *principle of individual ethical responsibility*. Any individual whether an employee of this institution, a volunteer, or an outside consultant is responsible for the ethical ramifications of his or her individual acts.
- The *principle of protection of confidential material*. Records about individuals and organizations are confidential and are to be used only by those staff members who need to use them to further the legitimate mission of the institution.
- The *principle of record sensitivity*. Records have an enduring power and may improve or ruin individual lives. Since records might become available to their subjects or to others who do not understand appropriate use of sensitive materials, everyone must ensure that records are not used in a harmful manner.
- The *principle of ethical collection*. Collection of data for Advancement systems is limited to public sources, correspondence, and constituent relationships. Foundation, University of Illinois, and Alumni Association staff, agents and volunteers shall not seek out or report public information of a personal nature such as that contained in documents related to divorce, child custody, probate, or bankruptcy. Information collected should be stated in an objective and factual manner and attributed to the source. Information solicited from external or university sources shall be in accordance with state and federal laws.

### Purpose

These protocols will protect our members and donors and guide our staff by providing general principles and practices related to all aspects of confidentiality. The protocol applies to all types of confidential information, regardless of format; including but not limited to, hard copy, electronic, film, or any other medium. It applies not only to Foundation and Alumni Association employees, but also to University employees who are engaged in alumni relations or fundraising, along with volunteers, consultants, or

others outside of the Foundation, the University, and the Alumni Association, who work to further Advancement efforts.

## Information Classification

Advancement information is divided into four categories: Public, Internal, Confidential and High Risk.

- *Public* – Information in this category is available for public distribution. This includes publications, published contact and degree data, public websites and external video productions.
- *Internal* – Information in this category is for internal Advancement use. This includes Advancement summaries, limited constituent information, events, volunteer, and department memos and policies.
- *Confidential* – Confidential information is proprietary and access is restricted depending on job roles. Disclosure of this information would cause reputation and competitive harm to University of Illinois Advancement. This category includes contact information, donation amounts, call reports, and relationship management details.
- *High Risk* – High risk information is data restricted by custodians, policies, regulations, or statute. Examples of this data are social security numbers, bank account numbers, credit card numbers or other identifiers that can be used for identity theft.

## Collection

Collection of information as it relates to the Advancement systems is limited to sources available to the public and information collected by Advancement personnel. Information should be stated in an objective and factual manner and attributed to the source.

Foundation, University, and Alumni Association staff, agents and volunteers shall not seek out or report public information of a personal nature such as that contained in documents related to divorce, child custody, probate, or bankruptcy. Letters and communications received disparaging or slandering others will not be collected. Information not relevant to University of Illinois Advancement shall not be collected.

Collection and use of information shall be done lawfully and openly. Therefore, written requests for public information shall be made on institutional stationery or by official University or University-related email clearly identifying the sender and the proposed use for the information. Also, when requesting information in person or by telephone, neither individual nor institutional identity shall be concealed.

## Personal Use of Information

Advancement information is for maintained solely for the benefit of the University of Illinois. As such personal use is prohibited, and transfer of Advancement downloads to unauthorized individuals is prohibited. Prior to receiving access, all users of Advancement data must take an introductory course that includes content regarding protection of sensitive information.

## Retention of Advancement Information

Advancement information is continuously updated and a download or printed information has a short life span. Information should be used and destroyed after use. Storage of Advancement data in shared drives where others who are not trained have access to the data is prohibited. Storage of data on CDs, DVDs, USB drives and other external portable media is prohibited.

## Destruction of Information

Advancement information is to be securely destroyed. Shredding of paper and electronic erasure are required of discarded data. Information stored on hard disk drives, USB drives or other media are to be erased before destruction or sending to surplus.

## Loss of Information

Should Advancement information be misplaced, lost or stolen, it is required of all personnel to report that loss. This requirement relates to all media and information systems. Loss may be reported to supervisors, to the Foundation or the Alumni Association.

## Release

Confidential information is collected and maintained for the purpose of furthering the membership or fundraising operations of the Foundation or the Alumni Association, respectively, and the University. Therefore, any confidential information is released for those purposes only. All information, confidential or not, may be subject to subpoena or other legal action.

When an employee of the Foundation, the University, or the Alumni Association must share confidential information about a member, donor or prospect in order to perform his or her duties, the volunteer or agent must execute a written confidentiality agreement before the information is transferred. Nonetheless, the employee is ultimately responsible for the release of the confidential information.

Confidential information is not available to groups or individuals for any other uses, such as for vendor usage, for political mailing lists or for locating old friends. Therefore, addresses or telephone numbers are not to be released to third parties.

Questions about the appropriate release of information should be referred to the Foundation President, a Vice Chancellor for Advancement, or the Alumni Association President, or their designees, depending on the type of information.

## Conclusion

It is critical to the mission of the Foundation, the University, and the Alumni Association that confidentiality be respected and maintained. All employees are required to sign a confidentiality agreement and abide by its terms. The executed agreement shall be kept in the employee's permanent personnel file. Since supervisors are responsible for their staff, they shall provide proper orientation, obtain the agreement, make sure the employee attends required information security training, and monitor employees to ensure compliance.



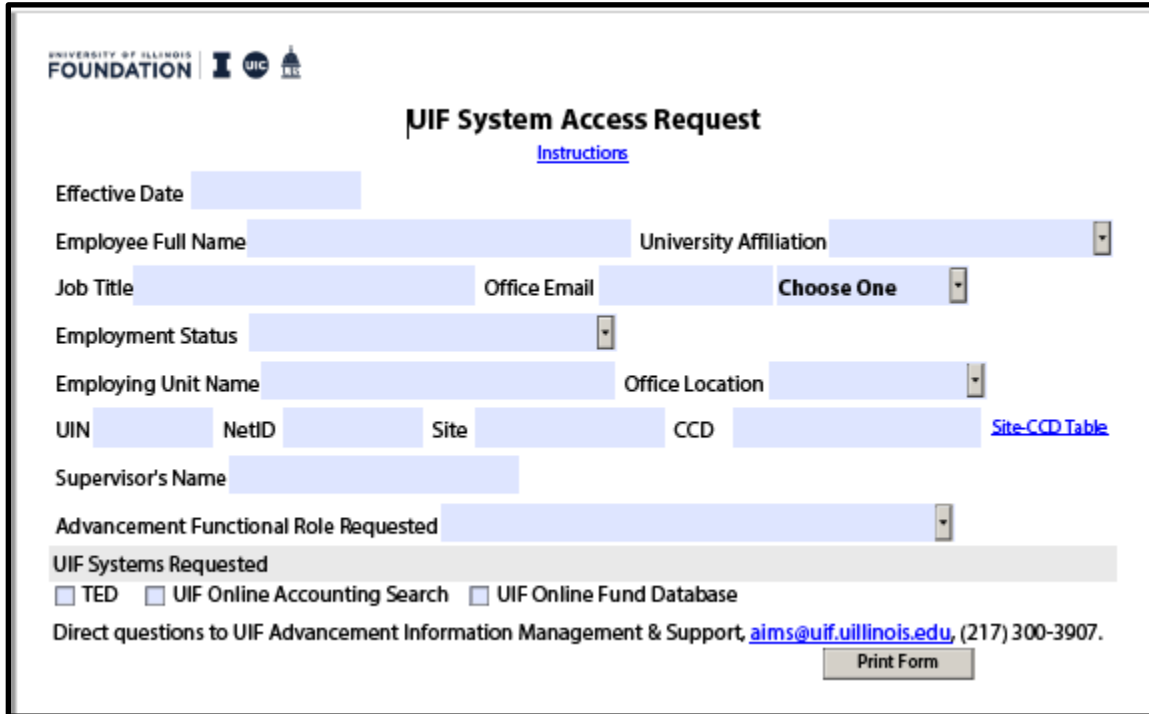
Should any action that violates the confidentiality policy or protocols occur, the supervisor, the Foundation President, the Vice Chancellors for Advancement, or the Alumni Association President may use the following disciplinary guidelines:

- 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 or termination of employment.

## Appendix B: UIF Systems Access Request Form and Confidentiality Agreement

Updated 6/27/2018



The form is titled "UIF System Access Request" and includes the University of Illinois Foundation logo. It contains the following fields and options:

- Effective Date:** Text input field.
- Employee Full Name:** Text input field.
- University Affiliation:** Dropdown menu.
- Job Title:** Text input field.
- Office Email:** Text input field.
- Choose One:** Dropdown menu.
- Employment Status:** Dropdown menu.
- Employing Unit Name:** Text input field.
- Office Location:** Dropdown menu.
- UIN:** Text input field.
- NetID:** Text input field.
- Site:** Text input field.
- CCD:** Text input field.
- Site-CCD Table:** Link.
- Supervisor's Name:** Text input field.
- Advancement Functional Role Requested:** Dropdown menu.
- UIF Systems Requested:** Section with checkboxes for:
  - ☐ TED
  - ☐ UIF Online Accounting Search
  - ☐ UIF Online Fund Database
- Direct questions to UIF Advancement Information Management & Support:** [aims@uif.uillinois.edu](mailto:aims@uif.uillinois.edu), (217) 300-3907.
- Print Form:** Button.

## Advancement Information Confidentiality Agreement

Updated 04/30/18

The Alumni Association, the Foundation, and the University of Illinois are committed to the ethical collection and use of information in pursuit of legitimate institutional goals. We shall support and further the individual's fundamental right to privacy. Consequently, information not available from public sources should not be disclosed. Records about individuals and organizations are confidential and are to be used only to advance the mission of the institution.

I acknowledge that in the course of my work activities I may have access to documents, data, or other information that may be confidential and/or privileged from disclosure, whether labeled or identified as "confidential."

Except as required by my activities, I shall never, either during or after my employment with the Alumni Association, the Foundation or the University of Illinois, directly or indirectly use, publish, disseminate or otherwise disclose to any third party, or use for personal gain, any information acquired in the course of my activities without the prior written consent of the University of Illinois Alumni Association and /or University of Illinois Foundation.

I have read the Confidentiality Protocol Statement and understand that violation of any of the policies and practices described therein may be grounds for dismissal or disciplinary action, including loss of access to all Advancement information systems.

## Use of Content

Access to Advancement information is made available in centralized systems including but not limited to: ADD iLEARN Advancement to this list

- The Tracking and Engagement Database (TED) – The database containing information on alumni, students, friends and donors (individual, corporations and foundations) to the University of Illinois system.
- BBIS – Blackbaud Internet Solutions is a management system for web content that integrates with the Blackbaud CRM database.
- Hyland OnBase – The document management system maintaining documents relating to transactions, correspondence and documentation supporting the business of advancement.
- Blackbaud Data Warehouse (BBDW) – The data warehouse consists of a nightly download of data from the Blackbaud CRM database with additional tables and calculated data elements for reports that are distributed to the advancement community.
- UIF Online – A web portal to a variety of Advancement content including forms, fund content and other Advancement information.
- UIF iLEARN Advancement – An online Learning Management system through which advancement employees can access training curricula, as well as the history of training they have completed.
- University of Illinois Alumni Network – Web access to the alumni directory information and alumni club activities from around the world, as well as the IlliniLink mentoring system.

Advancement information is governed by the Advancement data access manual available on UIF Online.

Users of Advancement systems will download, and receive reports and other content from Advancement systems in the course of their work. This content contains confidential data and alumni/donor contact information and should not be redistributed using email or any other form of electronic transmission except to authorized Advancement and University of Illinois employees. All content downloaded from systems should be handled with utmost care. Virus protection software and firewalls must be in use on systems where content is used to safeguard confidential Advancement information.

## Agreement

I acknowledge that in the course of my advancement activities I may have access to documents, data, or other information, some or all of which may be confidential and/or privileged from disclosure whether or not labeled or identified as "confidential." Therefore, except as required by my activities, I shall never, either during or after my association with the University of Illinois Alumni Association, the University of Illinois Foundation, or the University of Illinois directly or indirectly use, publish, disseminate or

otherwise disclose to any third party, or use for personal gain, any information acquired in the course of my activities without prior written consent of the University of Illinois Alumni Association and/or University of Illinois Foundation.

Finally, I acknowledge that I have read and understand the University of Illinois Advancement Information Confidentiality Agreement and agree to abide by it.

Signature: \_\_\_\_\_ Unit: \_\_\_\_\_

Name: \_\_\_\_\_ Date: \_\_\_\_\_

## Appendix C: Confidentiality Agreement for Volunteers

---

**Updated 8/27/2018**

### Introduction

The University of Illinois Foundation, the University of Illinois, and the University of Illinois Alumni Association are committed to the ethical collection and use of information in the pursuit of legitimate institutional goals. We support and further the individual's fundamental right to privacy. Consequently, information not available from public sources should not be disclosed. Records about individuals and organizations are confidential and are to be used only to further the mission of the institution.

### Agreement

I acknowledge that in the course of my volunteer activities I may have access to documents, data, or other information, some or all of which may be confidential and/or privileged from disclosure whether or not labeled or identified as "confidential." Therefore, except as required by my activities, I shall never, either during or after my association with the University of Illinois Foundation, the University of Illinois, or the University of Illinois Alumni Association, directly or indirectly use, publish, disseminate or otherwise disclose to any third party, or use for personal gain, any information acquired in the course of my activities without prior written consent of the University of Illinois Foundation or the University of Illinois Alumni Association.

Finally, I acknowledge that I have read and understand the University of Illinois Advancement Confidentiality Protocol Statement and agree to abide by it.

Signature: \_\_\_\_\_ Date: \_\_\_\_\_

\_\_\_\_\_

Name

## Appendix D: Vendor/Third Party Data Privacy and Security Agreement

Updated 6/9/2020

### DATA PRIVACY AND SECURITY AGREEMENT

This Data Privacy and Security Agreement ("DPSA") is entered into by and between \_\_\_\_\_ ("Company") a(n) \_\_\_\_\_ company, incorporated in \_\_\_\_\_, with offices located at \_\_\_\_\_ and University of Illinois Foundation, 1305 West Green Street, Urbana, Illinois 61802, ("Foundation").

**WHEREAS**, Company has or may be engaged to perform certain services or functions on behalf of Foundation pursuant to separate contractual arrangements; Company performs or may perform work on behalf of Foundation which may require Company to have access to, create, receive, maintain, or transmit Personal Data (as defined below) of Foundation's donors, employees, or agents which is or may be protected under Applicable Law; Applicable Law may require Foundation to have protective measures to protect such Personal Data, including but not limited to written agreements with third parties to ensure the confidentiality and security of such information.

**NOW, THEREFORE**, the parties agree as follows:

#### 1. Definitions. For purposes of this DPSA:

- a. "GDPR" - means the EU General Data Protection Regulation (Regulation (EU) 2016/679).
- b. "Special categories of data," "process/processing," "controller," "processor," "data subject," "personal data breach," "supervisory authority," "Union," and "Member State" have the same meaning as in GDPR
- c. "Personal Data" - Personal Data as used in this DPSA has the same meaning as GDPR, including without limitation, any personally identifiable information, in whatever form or medium, Company accesses, creates, receives, maintains or transmits on behalf of Foundation about an individual, including but not limited to (1) an individual's name or other personal identifier in connection with one or more of following; Social Security number; driver's license number or state identification card number; financial or billing account number; policy number of any insurance contract having a cash value; health insurance information; credit card number; debit card number; tax identification number; any required security code, access code, or password that would permit access to an individual's financial account; professional, occupational, recreational or governmental license, certificate, permit, or membership number; date of birth; mother's maiden name; medical information; biometric information; electronic, voice, or digital signature; (2) a user name or email address, in combination with a password or security question and answer that would permit access to an online account; or (3) other information subject to Security Breach notification obligations under any Applicable Law.

- d. "Sub-processor" means any processor engaged by Company or by any other sub-processor of Company who agrees to receive from Company or from any other sub-processor of Company Personal Data exclusively intended for processing activities to be carried out on behalf of Foundation after the transfer in accordance with Foundation's instructions and the terms of this DPSA.
- e. "Technical and organizational security measures" means those measures aimed at protecting Personal Data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure, or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, taking into account the nature, scope, context, and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons.

**2. Security Breach.** Security Breach means any unlawful or unauthorized access, acquisition or use of data or information that is capable of compromising the security, confidentiality, availability or integrity of Personal Data. Good faith acquisition of Personal Data by an employee or agent of Company is not a Security Breach, provided that the information is not used for a purpose unrelated to work performed by Company for Foundation and is not subject to further unlawful or unauthorized use.

**3. Applicable Law.** Applicable Law means those laws, regulations, bulletins, or other legal authority having the force of law, including but not limited to obligations imposed by GDPR and private, quasi-governmental and governmental agencies, relating to services provided under any agreement between Company and Foundation.

**4. Confidentiality of Personal Data.** Notwithstanding any contrary provisions of any agreement between Company and Foundation, it is understood and agreed that all Personal Data will be held by Company in strict confidence and will be used only as necessary to perform work for Foundation. The scope and details of the processing (as well as the personal data covered) are specified either or both in Annex 1, attached to this DPSA, which forms an integral part of this DPSA, and the separate written agreement covering the contracted services or functions performed.

**5. Obligations of Company.** The Company shall have the following obligations:

5.1. Company shall process the Personal Data only (i) on behalf of Foundation and in compliance with Foundation's instructions, this DPSA, and the principles of GDPR; (ii) for the purpose(s) described in Annex 1; and (iii) for the duration of the DPSA. If Company cannot provide such compliance for whatever reason, it will promptly inform Foundation of its inability to comply, in which case Foundation may either or both suspend the transfer of data and terminate the DPSA.

5.2. Company shall not transfer the Personal Data to a third country outside the European Economic Area ("EEA") without Foundation's prior written consent and, if applicable, will do so only in compliance with Paragraph 7, below.



5.3. Company represents that it has in place procedures so that any person authorized to process the Personal Data is committed to binding obligations of confidentiality when processing such Personal Data.

5.4. Company shall have and maintain appropriate technical and organizational security measures, including the measures referred to in Article 32(1) of GDPR, to protect the Personal Data against accidental or unlawful destruction, loss, alteration, and unauthorized disclosure or access, and which enable Foundation to respond to requests from individuals who exercise their rights under GDPR.

5.5. Company will only appoint a sub-processor with Foundation's prior written consent and in accordance with Paragraph 26

5.6. Company will fully and in good faith cooperate and assist Foundation in fulfilling Foundation's obligations in relation to (i) any request to exercise a data subject's rights under Chapter III of GDPR, and (ii) responding to any complaint, notice, or communication that relates directly or indirectly to Contractor's processing of the Personal Data or compliance with GDPR.

5.7. Company will assist Foundation in ensuring compliance with the obligations pursuant to Articles 30 to 36 of GDPR.

5.8. Company will cooperate with the supervisory authority in the performance of the supervisory authority's tasks.

5.9. Company will notify Foundation within 24 hours of becoming aware that any Personal Data (while in Contractor's or its sub-processors' possession or control) is subject to a Personal Data breach or is lost or destroyed or becomes damaged, corrupted, or unusable. Company will provide Foundation with sufficient information to allow Foundation to meet any obligations to report or inform data subjects of the breach and will cooperate with Foundation and take such reasonable commercial steps as are directed by Foundation to assist in the investigation, mitigation, and remediation of each such a breach.

5.10. Company will provide reasonable assistance to Foundation with any data protection assessments and prior consultations with supervisory authorities or other competent data privacy authorities that Foundation reasonably considers to be required by Article 35 or 36 of GDPR.

5.11. Upon reasonable request of Foundation, Company will make available to Foundation all information and assistance necessary to demonstrate compliance with this DPSA and GDPR and will allow for and contribute to audits, including inspections, by Foundation (or an auditor selected by Foundation and not reasonably objected to by Contractor), with reasonable notice and during regular business hours.

5.12. Company will notify Foundation within 2 business days about (i) any legally binding request for disclosure of the Personal Data by a law enforcement authority unless otherwise prohibited by law; (ii) any communications between Company and the supervisory authority concerning the processing of the Personal Data; and (iii) any request received directly from a data subject, without responding to that request, unless it has been otherwise authorized to do so by Foundation.

**6. Obligations of Foundation.** The Foundation represents that:

6.1 The Personal Data has been collected, processed, and transferred in accordance with the laws applicable to Foundation. Foundation has instructed, and throughout the duration of the contractual arrangement will instruct, Company to process the Personal Data transferred only on Foundation's behalf and in accordance with the applicable data protection law and this DPSA.

6.2 Foundation has used reasonable efforts to determine that Company is able to satisfy its legal obligations under this DPSA.

6.3 Taking into account the risks for the rights and freedoms of natural persons and the nature, scope, context, and purposes of processing, Foundation has implanted appropriate technical and organizational security measures.

**7. Consent for Restricted Activities.** Company shall not subcontract, and shall prohibit its suppliers and subcontractors from subcontracting, any Restricted Activities outside of the United States of America ("U.S.") without obtaining the prior written consent of Foundation, which shall be granted or withheld in Foundation's sole discretion. If a location outside the U.S. is designated in any agreement between Company and Foundation or statement of work, Foundation shall be deemed to have consented to such location outside the U.S.

Restricted Activities means any activity that would require or permit Company's employees or permitted subcontractor's employees to (a) have direct phone, face-to-face, email or other real-time communications with Foundation or Foundation personnel involving Personal Data; or (b) access, use, or transmit to any local storage device, or print, any Personal Data.

**8. Security and Safeguards of Personal Data.** Notwithstanding any contrary provisions of any agreement between Company and Foundation, Company has implemented and will continue to implement and maintain administrative, physical and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, security, and availability of Personal Data that Company accesses, creates, receives, maintains or transmits on behalf of Foundation. Such measures shall include protection of Personal Data with at least the same degree of care that Company uses to protect its own confidential information, but in no event less than compliance with Applicable Law. Company will ensure that any employee, contractor, subcontractor and agent to whom Company provides such information agrees to comply with the requirements set forth in this Paragraph 8.

Access to Personal Data will be limited to those persons who need such information to provide contracted services or functions to Foundation, pursuant to reasonable business practices adopted to limit access and unauthorized disclosure, or as otherwise required by Applicable Law. Company agrees to use reasonable and appropriate safeguards to prevent the use or disclosure of Personal Data other than as specifically authorized by Foundation. Company will maintain, and will require that its employees, contractors, subcontractors and agents maintain the confidentiality of all Personal Data and will require its employees, contractors, subcontractors and agents, to comply with the provisions of this DPSA, and as necessary, with Applicable Law.

**9. Notification.** Company agrees that Foundation is considered to be the owner of any data to the extent it contains Personal Data, and that Company will comply with the requirements of Applicable Law concerning data security breaches and any third party duties thereunder to the owners of data containing personally identifiable information. Company shall not disclose to any third party the existence of any actual or suspected unauthorized access, possession, use or knowledge, or attempt thereof, of any Personal Data or actual or suspected Security Breach, without Foundation's express written consent, unless Company is otherwise prohibited by Applicable Law from doing so, in which case, Company shall nevertheless provide as much advance notice to Foundation as permitted by law of such planned disclosure of such event.

Notwithstanding the preceding paragraph, Company will promptly notify Foundation of any Security Breach, if such information was, or is reasonably believed to have been, accessed or acquired by any unauthorized person or entity. Company's notice to Foundation will, to the maximum extent possible, include a detailed description of the Personal Data acquired or reasonably believed to have been acquired.

**10. Security Incidents.** Company has implemented and will continue to implement and maintain policies and procedures to address security incidents, including Security Breaches, concerning Personal Data that Company or its employees, contractors, subcontractors or agents access, create, receive, maintain or transmit on behalf of Foundation. Company will mitigate to the extent practicable any harmful effects of such incidents and document security incidents and their outcomes.

**11. Identity Theft.** If Company is engaged to perform an activity in connection with Personal Data, Company shall ensure that its own activity with respect to such Personal Data is conducted in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft. Company shall have policies and procedures in place to detect relevant patterns, practices, or specific activities that indicate identity theft with respect to Personal Data, and which may arise in the performance of Company's activities under any agreement between Company and Foundation. Company shall either report such patterns, practices, or specific activities to Foundation or take appropriate steps to prevent or mitigate identity theft. Third party audits of Company's policies and procedures shall be made available to Foundation in a reasonably timely manner.

**12. Foundation and Regulatory Access.** At Foundation's reasonable discretion, Company will make its internal practices, books and records relating to the use, security, and disclosure of Personal Data available to relevant governmental authorities or to Foundation at Foundation's request and in a time and manner

designated by Foundation for purposes of determining Company's compliance with Applicable Law, or as otherwise required by law.

**13. Return and/or Destruction of Personal Data.** Unless otherwise required by law, within ten (10) days of Foundation's request, Company will return and/or certify to Foundation the destruction of all Personal Data in its possession. In the case of destruction of the Personal Data, Company shall destroy the Personal Data in a manner that will render non-retrievable all documents, memoranda, notes or other writings prepared by or retained by Company which are based in part or reference the Personal Data. If return or destruction is not feasible, Company shall notify Foundation of the reasons that such return or destruction is not feasible and identify the Personal Data that has not been returned or destroyed (the "Retained Information"). Company further agrees that any Retained Information retained after the termination of the term of this DPSA shall remain subject to this DPSA until Company returns or destroys such Retained Information. This Paragraph 13 and Paragraphs 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 14, 15, 17, 18, 19, 21, 22 and 26 of this DPSA shall survive the ending of the term of this DPSA described in Paragraph 16 below.

**14. Injunctive and Other Relief.** Company acknowledges that any breach of the covenants contained in this DPSA may result in irreparable injury to Foundation, for which money damages are not available to or otherwise do not adequately compensate Foundation. In the event of any such breach or any threatened breach, Foundation shall be entitled to seek an injunction or restraining order issued by a competent court enjoining and restricting Company from breaching or continuing any such breach. Company agrees to waive any requirement for the securing or posting of any bond in connection with such remedy. Such remedy shall not be deemed to be the exclusive remedy, but shall be in addition to all other remedies available at law or equity to Foundation. In no event shall any party to this DPSA sue or otherwise take action against the other for lost profits or any other special, punitive, consequential or incidental damages arising out of or in any way related to this DPSA, an alleged breach of this DPSA, or any other agreement or arrangement between Foundation and Company. In the event of litigation relating to this DPSA, the non-prevailing party shall be liable and pay to the prevailing party the reasonable legal fees incurred by the prevailing party in connection with such litigation, including any appeal therefrom.

**15. Indemnification.** Company will be liable to Foundation for damages that Company causes to Foundation by Company's breach of this DPSA. Foundation will be liable to Company for damages that Foundation causes to Company by Foundation's breach of this DPSA. Liability as between the parties is limited to actual damage suffered; punitive damages are specifically excluded. Each party will be liable to data subjects for damages it causes by any breach of third party rights if applicable. Company shall not rely on a breach by a sub-processor of the sub-processor's obligations in order to avoid Company's own liabilities. For purposes of this provision, actual damage losses include but are not limited to costs, claims, damages, legal fees, liabilities, fines, penalties, and expenses.

**16. Term.** This DPSA shall and the obligations hereunder shall continue until terminated by Foundation or by mutual consent in writing by both parties, except as otherwise stated herein.

**17. Ambiguity.** Any ambiguity in this DPSA will be resolved in favor of a meaning that permits Foundation and Company to comply with Applicable Law, including those governing privacy, data security, data security breach notification, encryption, and protocol.

**18. Other Provisions.** All other provisions of any agreement between Company and Foundation, including provisions relating to the confidentiality of proprietary and confidential information remain in full force and effect. However, if a conflict exists between the provisions of any agreement between Company and Foundation, (other than a Business Associate Agreement executed in accordance with the Health Insurance Portability and Accountability Act and related regulations) and the provisions of this DPSA, the provisions of this DPSA will govern.

**19. Entire Agreement.** This DPSA supersedes all prior agreements between the parties hereto with respect to the subject matter hereof and constitutes the entire agreement of the parties with respect to the subject matter hereof, and there are no representations, warranties, covenants or agreements or commitments by the parties except as set forth herein. No modification, amendment or waiver of this DPSA shall be binding without the written consent of the parties hereto. This DPSA shall inure to the benefit of and be binding upon each of the parties hereto and their respective successors and assigns; provided, however, that neither this DPSA nor any of the rights, interest or obligations hereunder shall be assigned by either of the parties hereto without the prior written consent of the other party, which shall not be unreasonably withheld, delayed or conditioned, and no assignment of any right, interest or obligation shall release any such assigning party therefrom unless the other party shall have consented to such release in writing specifically referring to the right, interest or obligation from which such assigning party is to be released.

**20. Severability.** In the event that any provision or portion of this DPSA is determined by a competent court to be invalid or unenforceable for any reason, in whole or in part, the remaining provisions of this DPSA and shall be unaffected thereby and shall remain in full force and effect to the fullest extent permitted by applicable law.

**21. Governing Law.** This DPSA shall be governed by, and construed and enforced in accordance with, the laws of the State of Illinois, without reference to principles of conflicts of law.

**22. Jurisdiction and Venue.** The parties irrevocably and unconditionally submit to the exclusive jurisdiction of any United States federal court sitting in the Central District of Illinois or State of Illinois court sitting in Champaign, Illinois over any suit, action, or proceeding arising out of or relating to this DPSA. The parties hereby irrevocably and unconditionally waive (i) any objection to the laying of venue of any such suit, action or proceeding brought in any such court and any claim that any such suit, action, or proceeding brought in any such court has been brought in an inconvenient forum and (ii) any right a party has to a trial by jury in any action or proceeding arising out of or relating to this DPSA. The parties agree that a final judgment in any such suit, action, or proceeding brought in any such court after the exhaustion of any appeals shall be conclusive and binding upon it and may be enforced in any other court to whose jurisdiction the parties are or may be subject, by suit upon such judgment.

**23. Notice.** All notices, demands or other communications to be given or delivered under or by reason of this DPSA shall be in writing and shall be deemed to have been properly served if delivered personally; by a nationally recognized overnight delivery service (receipt requested); by fax, if a copy is sent the same day by a nationally recognized overnight delivery service (receipt requested); or by certified or registered mail, return

receipt requested and first class postage prepaid, in each case to the contact party at the addresses or fax numbers as follows:

If to Company: Name: \_\_\_\_\_

Attn: \_\_\_\_\_

Address: \_\_\_\_\_

City/State/Zip Code: \_\_\_\_\_

Fax Number: \_\_\_\_\_

If to Foundation:

Attn: \_\_\_\_\_

1305 W. Green Street

Urbana, Illinois 61802

With a copy to (which shall not constitute notice):

University of Illinois Foundation

Office of the General Counsel

1305 W. Green Street

Urbana, Illinois 61802

Fax: (217) 333-0810

**24. Headings.** The Paragraph headings set forth herein are for convenience only and do not constitute a substantive part of this DPSA.

**25. Counterparts.** This DPSA may be executed in counterparts, and signature pages exchanged by facsimile or other electronic transmission, and each counterpart shall be deemed to be an original, but all counterparts shall together constitute one and the same instrument. A signature by facsimile or other electronic transmission by any party on a counterpart of this DPSA shall be binding and effective for all purposes.

**26. Sub-processing** Company shall not subcontract any of its processing operations performed on behalf of Foundation without Foundation's prior specific or general written consent. Where Foundation has so consented, Company will subcontract such processing only by way of a written agreement with the sub-processor that imposes the same obligations on the sub-processor as are imposed on Company under this DPSA. Company will promptly send a copy of any sub-processor agreement it concludes under this DPSA to Foundation. Company will keep a list of such sub-processing agreements, which it will make available to Foundation and the appropriate supervisory authority when so requested or required by GDPR. Where the sub-processor fails to fulfill its data protection obligations under such written agreement, Company will remain fully liable to Foundation for the performance of the sub-processor's obligations under such agreement.

**27. Effective Date.** This DPSA is effective \_\_\_\_\_ ("Effective Date").

IN WITNESS WHEREOF, the parties have executed this DPSA as of the Effective Date:

By <b>University of Illinois Foundation</b>	By _____:
Name:	Name:
Signature:	Signature:
Title:	Title:
Date:	Date:



**Annex 1**

**DETAILS OF PROCESSING**

1. Subject matter of the processing:

[Briefly describe subject matter of the processing]

2. Duration of the processing:

[Briefly describe anticipated duration of the processing]

3. Nature and purpose of the processing:

[Briefly describe nature (what types of basic processing activities) and purpose of the processing]

4. Categories of data subjects concerned:

[Identify the categories of data subjects whose data is to be processed]

5. Categories of Personal Data to be processed:

[Identify the categories/types of Personal Data to be processed]

6. Special categories of data to be processed (if applicable):

[Identify the special categories of data to be processed, if any. Special categories include race, ethnic origin, political opinions, religion, philosophical beliefs, trade union memberships, genetic data, biometric data, health, sex life, and sexual orientation.]

## Appendix E: Confidentiality Agreement for Club/Group

---

### Updated 8/27/2018

Data being provided by the University of Illinois Alumni Association or University of Illinois Foundation is confidential and is to be used exclusively by \_\_\_\_\_ (club/group) for the purpose of providing the agreed upon services with the University of Illinois Alumni Association or University of Illinois Foundation. All individuals associated with handling this data/project understand the confidential nature of this agreement and will abide by this Statement of Confidentiality.

### Accepted and Agreed:

### Name/Address of club/group:

---

---

---

## Appendix F: Advancement Data Access Plan

### Information Security Classification

#### Add Advancement Administrator

Proposed Role	Description	Examples	Information Access Categories	Notes
<b>Security Class: Public</b>				
Advancement Constituent	Access to limited contact and degree information regarding individuals in UIAA Directory and Alumni Network. Individuals can opt for non-disclosure.	All UI faculty, staff, and alumni who use UIAA Gateway (Alumni Directory) and/or Network.	Education (Directory), Contact (Limited).	The most basic access category—read-only access to directory-level information, with ability to update personal information. All alumni, faculty and staff currently will continue to access this information through UIAA Gateway and/or Alumni Network.
<b>Security Class: Confidential I</b>				
Business Manager	Access to information necessary to manage pledges, gifts, gift funds, and gift acknowledgement programs.	Business Operations.	Fund/Ledger, Revenue (Limited).	This role is a non-hierarchical, stand-alone role for staff who manage gift funds and acknowledgement programs but do not report to Advancement. Staff and do not have access to most Advancement information.

# UNIVERSITY OF ILLINOIS ADVANCEMENT INFORMATION ACCESS MANUAL

Proposed Role	Description	Examples	Information Access Categories	Notes
<b>Security Class: Confidential II</b>				
Advancement Support	Access to information necessary to perform administrative duties that pertain to Advancement.	Human Resources, Support Staff for Advancement/Development, Student Worker for Advancement/Development.	Public level of access, plus Basic Constituent information—Personal Info, Advancement Employment (Directory) Information, Relationships, Contact information (Full), Documentation, Volunteer	Assistants, other office support professionals, and student employees may request higher access levels if needed to accomplish tasks for other designated persons.
<b>Security Class: Confidential III</b>				

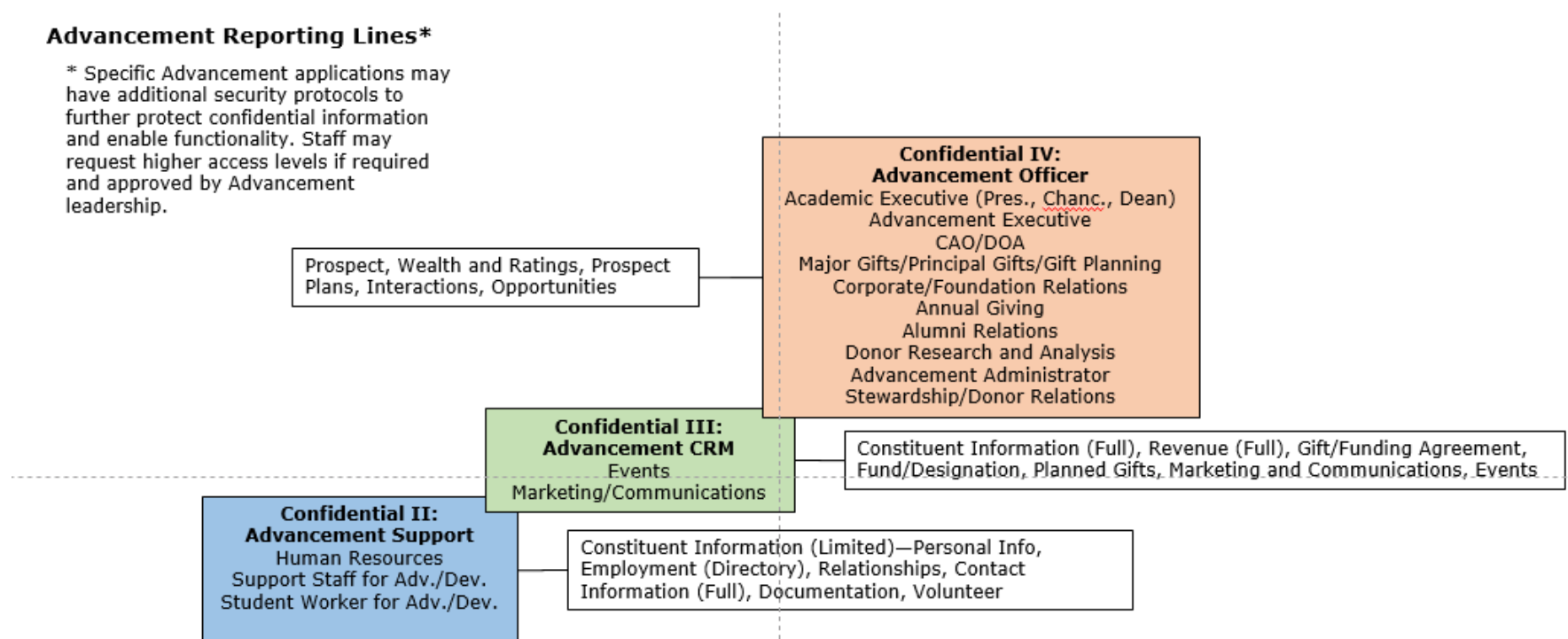
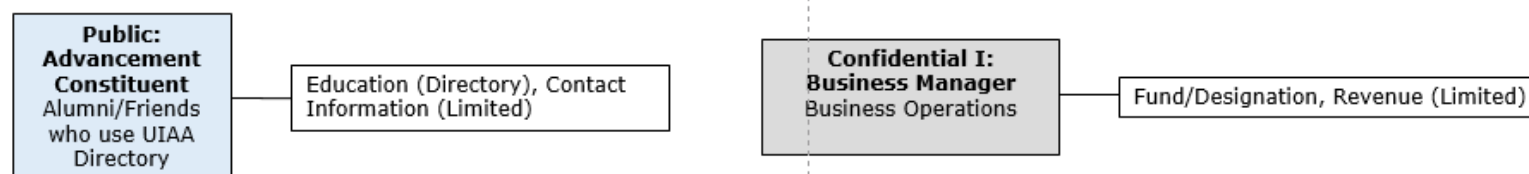
# UNIVERSITY OF ILLINOIS ADVANCEMENT INFORMATION ACCESS MANUAL

Proposed Role	Description	Examples	Information Access Categories	Notes
Advancement Constituent Relationship Management (CRM)	Access to information needed to manage constituent contacts through events, communications, and marketing.	Events, Marketing/Communications.	Internal level of access, plus Full Constituent Information, Revenue, Gift/Funding Agreements, Fund/Designation, Marketing and Communications.	The main role for most Advancement staff who are not Advancement Officers or a specialized UIAA/UIF role. Staff may request higher access levels if advancement activities information is required for events management, preparing communications materials, or managing relationships. Adherence to UIF communications tracking policies is required.
<b>Security Class: Confidential IV</b>				
Advancement Officer	Access to all appropriate information needed to solicit private support for the University, with ability to view and add solicitations, call reports, etc.	Academic Executive (University President, Chancellors, Deans), Advancement Executive (UIAA, UIF Presidents, Advancement VPs), 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.	Confidential II level access, plus Prospect, Wealth and Ratings, Prospect Plans, Interactions, Opportunities.	Access to entire database, with ability to add and update call reports, opportunities, and prospect plans. Academic Executives may request lower access levels as desired.
<b>Security Class: Confidential V</b>				

Proposed Role	Description	Examples	Information Access Categories	Notes
UIAA/UIF Specialized	Access to all appropriate information w/ ability to maintain and to modify systems as required.	Specialized functions within UIAA/UIF, including Information Technology, Research, Cash Receipts, Gift Processing, Stewardship Services, and Trust Services.	Confidential III, plus access to various screens and tables.	People in group can view the entire database, and as appropriate can enter pledges, gifts, wealth information and other data, build and modify applications, and make other changes using screens and applications not available outside of UIAA/UIF. Consists of a variety of roles and permissions for various table custodians.
<b>Security Class: High Risk</b>				
UIAA/UIF Specialized	Access to all appropriate credit card information, bank information, Social Security numbers, and the like as required to conduct business operations.	A small number of staff (< 25) within UIAA/UIF. Limited largely to Gift Administration, Trust Services, and Records	Confidential III, plus controlled access to specific personal constituent information, largely from donors.	High Risk information is held only in local systems maintained by UIAA/UIF for purposes of receiving credit card gifts and EFTs, maintaining trust funds, and the like.

**Advancement Reporting Lines\***

\* Specific Advancement applications may have additional security protocols to further protect confidential information and enable functionality. Staff may request higher access levels if required and approved by Advancement leadership.

**Non-Advancement Reporting Lines**



## Appendix G: Advancement Information Systems Reference Guide

---

### UI Functional Job Roles

#### Confidential I: Business Manager

##### *Business Operations*

UI employees who do not report to advancement but perform the related functions related of gift/fund management and/or gift acknowledgement.

#### Confidential II: Advancement Support

##### *Human Resources/Professional Development*

Responsible for employment-related services within the advancement community, including any or all of the following: training and professional development, employment processing and status changes, payroll processing, maintaining personnel records, and conducting various reporting functions related to employment.

##### *Support Staff for Advancement/Development*

Responsible for providing support for development or advancement functions. Support professionals may be assigned full-time or part-time to advancement. Responsibilities often include trip planning, report generation, and form correspondence. Support professionals may be granted higher levels of access as needed to accomplish tasks for designated persons or units. For example, an advancement officer's assistant may be granted access to development activities information (Confidential III, see below) in order to update and/or print call reports on behalf of his or her supervisor.

##### *Student Worker for Advancement/Development*

Responsible for accomplishing miscellaneous tasks for development or advancement functions. Responsibilities may vary widely among positions. Student Workers may be granted higher levels of access as needed to accomplish tasks for designated persons or units. For example, a student employee may be granted access to full contact information in order to update mailing addresses, phone numbers, email addresses, and the like (Confidential II, see below) on behalf of a unit.

#### Confidential III: Advancement Constituent Relationship Management (CRM)

##### *Events*

Plans and executes advancement events, including events related to fundraising, alumni recognition, investitures, advancement retreats, and the like.

*Marketing/Communications*

Responsible for any combination of marketing/communications activities within the advancement community, including planning, reporting, writing, editing and the production of print, web, electronic/digital communications and online communities.

*Confidential IV: Advancement Officer**Academic Executive*

The Academic Executive group includes academic leadership among the universities and the units whose duties include advancement work, including the University President, university Chancellors and Vice Presidents, Vice Chancellors, Deans, Directors, and Department Heads. Persons in this group may request lower levels of access.

*Advancement Executive*

Advancement Executives serve in senior leadership roles within the advancement community at the Universities, UIAA, or UIF. Persons in this role include the Alumni Association and the Foundation Presidents and Vice Presidents, Vice Chancellors, and Associate/Assistant Vice Chancellors. Primary responsibility is to set strategic direction for advancement programs, manage staffing and/or budgeting for university or URO, and cultivate board relationships.

*Chief Advancement Officer/Director of Advancement*

Responsible for planning and implementing a comprehensive advancement strategy for a college/unit, typically including development, alumni relations, special events and communications functions. Serves as primary liaison with university administrators and the college/unit's dean or director regarding advancement. Assists academic department heads and faculty in managing advancement initiatives. Maintains a significant travel schedule throughout the U.S. meeting with alumni, corporations and foundations to secure private support. Supervises advancement staff.

*Major/Principal Gifts/Gift Planning*

Primary responsibility is to meet with alumni and friends of the university to identify, cultivate, solicit and steward gifts of \$25,000 or more. Employees are considered Major Gift Officers if they are assigned visit goals by their Unit Chief Advancement Officer. Principal Gift Officers focus on gifts of \$5 million or more. Gift Planning Advisors work with major and principal gifts officers to provide information and advice regarding deferred giving instruments (annuities, trusts, bequests, etc.) and prepare fund agreements. May also manage a portfolio of donors and prospects.

*Corporate/Foundation Relations*

Primarily responsible for working closely with colleges, units and senior administrators to expand and steward relationships with foundations and/or corporations. Researches and develops presentations and proposals to fund university initiatives. Travels throughout the U.S., and sometimes internationally, to meet with corporate or foundation representatives. Secondary duties may include Major Gift work with individual donor prospects.

*Annual Giving*

Primary responsibility is to work with direct mail and telemarketing programs to secure gifts of \$24,999 or less from alumni and friends. Additional responsibilities may include identifying and/or personally engaging in relationships with donor prospects for Leadership Annual Giving.

*Alumni Relations*

Primary responsibility is to build life-long, mutually supportive relationships between the institution and its alumni. Typical responsibilities include event planning, volunteer recruitment and coordination, administration of awards and recognition programs, data management, strategic communications, advocacy, maintenance of institutional history and traditions, and outreach to current students as future alumni.

*Donor Research and Analysis*

Primarily responsible for developing prospect and donor lists and creating ad hoc reports for use in various University units.

*Advancement Administrator*

Responsible for management and/or oversight of non-major gift fundraising activities. Duties typically include general administration, alumni relation, events, communication, stewardship, and/or annual giving.

*Stewardship/Donor Relations*

Primary responsibilities include coordinating gift acknowledgements and donor recognition, drafting donor correspondence, tracking fund agreements, and serving as liaison with Board members and volunteers.

## Confidential V: Specialized UIF/UIAA Roles

*Donor Research and Analysis*

Responsible for identifying and profiling new sources of private support for the university's fundraising efforts by using the Foundation, University and community research libraries, archival materials and online databases to provide biographical and financial research of individuals and organizations; prospect analysis; tracking major donor prospects; associating revenue with opportunities; and helping gift officers optimize their portfolios.

*Gift Administration*

Responsible for direction and support for the acceptance and processing of gifts in support of University unit under established UIF policies and procedures. Includes the gift processing and cash receipts functions.

*Trust Services*

Maintains records and accounts of funds held in trust by the Foundation. Compiles tax returns and other associated materials.

*Information Technology Services*

Responsible for developing and maintaining Advancement information systems, including design and development of Blackbaud, UIF Online, OnBase and other software. Provides training and support to system users. Individuals in this role receive system- and table-specific access based on their job duties.

## Data and Systems Inventory

<b>Security Class</b>
<b>P = Public</b>
<b>I = Internal</b>
<b>CI = Confidential I, CII = Confidential II, CIII = Confidential III</b>
<b>H = High Risk</b>

Security Class	Information Category	Description	Host System	Category of Misuse
P	Education	Data regarding attendance at the University of Illinois, University Laboratory High School and, in some cases, other higher education institutions.	UIAA Directory, UI Alumni Network, TED	Minor
P-CI	Contact Information	Primary, secondary and tertiary contact information. Examples include home address, business address, phone number, and email address in paper or digital form. Limited contact information is available to constituents through UIAA Directory and Alumni Network. Full contact information is available at the CI level.	UIAA Directory, UI Alumni Network, TED	Severe
I-CV	Training	Information regarding training classes offered by various advancement offices,	<a href="https://ilearn.uif.uillinois.edu/#/dashboard">https://ilearn.uif.uillinois.edu/#/dashboard</a>	Serious

Security Class	Information Category	Description	Host System	Category of Misuse
		including offerings, attendance and effectiveness. Examples include attendance rosters, instructor evaluations, and summary reports.		
CI-CIII	Constituent	Data of a biographical and/or descriptive nature regarding individuals or organizational constituents. Examples include names (current and historical), constituencies, demographics, and other items that indicate age, race-ethnicity, gender, spousal and/or family information, personal interests, employment information, relationships, etc.	TED	Serious
CIII	Events	Event invitations and attendance lists.	TED, CVent	Serious
CIII	Marketing and Communications	Documents and data pertaining to mass contacts by mail, telephone, and email from advancement offices to constituents for purposes of solicitation or communication. Examples include newsletters, events invitations, solicit codes, mail preference codes, marketing efforts, and segments.	TED	Serious
CIII	Revenue	Documents and data relating to revenue transactions, including pledges, deferred gifts, outright gifts, securities, gifts-in-kind, grants, and contracts.	TED	Severe
CIII	Planned Gifts	Documents and data pertaining to planned gifts, including original amounts, adjustments, vehicles, maturity dates, and other information.	TED	Severe

Security Class	Information Category	Description	Host System	Category of Misuse
CIII	Memberships	Commitments and payments to the UI Alumni Association for membership programs.	TED	Severe
CI-CIII	Fund/Designation	Documents and data pertaining to fund balances and transactions.	TED, UIF Online (Fund, Accounting tabs)	Severe
CIV	Prospect	Documents and data pertaining to personal contacts by telephone, email, mail, or face-to-face between fundraisers and alumni relations officers and constituents. Examples include plans, interactions, opportunities, and summary activity reports.	TED	Severe
CIV	Wealth and Ratings	Wealth and giving capacity information obtained primarily from public sources.	TED	Severe
CIV	Plans	Collections of steps and solicitations planned by advancement officers for particular prospects.	TED	Severe
CIV	Interactions	Recorded personal contacts among advancement officers and prospects, including notes describing that nature of the contacts. Interactions may be part of a plan or stand-alone.	TED	Severe
CIV	Opportunities	Planned and made personal solicitations from an advancement officer to a prospect, including status and amount.	TED	Severe
H	Personal Identification Numbers	Credit Cards, SSNs, etc., stored within UIAA/UIF systems or files.	Local UIAA/UIF systems only.	Severe
All Security Groups	Records	Images of unstructured data, including but not limited to: gifts, news clippings, and correspondence among advancement staff and constituents. Examples include news articles, greeting cards,	TED, Hyland OnBase	Various, depending on the document type

# UNIVERSITY OF ILLINOIS ADVANCEMENT INFORMATION ACCESS MANUAL

Security Class	Information Category	Description	Host System	Category of Misuse
		acknowledgement letters, summary activity reports, gift related correspondence and payment data. Records are organized into document type groups, which denote the type of information contained. Access is defined at the document type group level as appropriate.		