CONTENTS

Confidentiality of Information ............................................................................................................. 1
Advancement Information Systems ........................................................................................................ 1
Data Classification .................................................................................................................................. 2
Access to Advancement Information ...................................................................................................... 3
Training on Advancement Systems ........................................................................................................ 3
Accountability ......................................................................................................................................... 4
Destruction of Data ................................................................................................................................. 4
Use of Copyrighted Content in Advancement ....................................................................................... 4
Third Parties ........................................................................................................................................... 5
Contact Updates ..................................................................................................................................... 5
Information Security Groups .................................................................................................................. 5
Specific Access for UI Employees .......................................................................................................... 6
Annual Review ....................................................................................................................................... 6

Appendix A: University of Illinois Advancement Confidentiality Protocol Statement .... 7

Introduction ............................................................................................................................................. 7
Purpose ................................................................................................................................................... 7
Information Classification ...................................................................................................................... 8
Collection ................................................................................................................................................ 8
Personal Use of Information .................................................................................................................. 8
  Retention of Advancement Information ............................................................................................... 9
  Destruction of Information .................................................................................................................... 9
  Loss of Information ............................................................................................................................... 9
Release .................................................................................................................................................... 9
Conclusion ............................................................................................................................................... 9

Appendix B: UIF Systems Access Request Form and Confidentiality Agreement ........ 11

Advancement Information Confidentiality Agreement .............................................................................. 12
Use of Content ..................................................................................................................................... 12
Agreement .............................................................................................................................................. 13

Appendix C: Confidentiality Agreement for Volunteers ........................................................................ 14

Introduction ......................................................................................................................................... 14
Agreement .............................................................................................................................................. 14

** Confidential information must be stored in a secure environment and should not be redistributed electronically except to persons authorized to receive such content. **
Appendix D: Vendor Confidentiality/Non-Disclosure Agreement ........................................... 15
Termination Clause .............................................................................................................. 15
Regulatory Matters ............................................................................................................. 15
Data Sharing ....................................................................................................................... 15
Use of Data .......................................................................................................................... 15
Intellectual Property .......................................................................................................... 15
Notification on Security Incidents ...................................................................................... 16
Access to Data ..................................................................................................................... 16
Encrypted Data Transmission .............................................................................................. 16
Encryption for Data Backups .............................................................................................. 16
Appendix E: Confidentiality Agreement for Club/Group ...................................................... 17
Appendix F: Advancement Data Access Plan ....................................................................... 18
Information Security Classification ...................................................................................... 18
Appendix G: Advancement Information Systems Reference Guide .................................... 23

UI Functional Job Roles .................................................................................................... 23
Confidential I: Business Manager ...................................................................................... 23
  Business Operations ......................................................................................................... 23
Confidential II: Advancement Support ................................................................................ 23
  Human Resources/Professional Development ................................................................ 23
  Support Staff for Advancement/Development ................................................................ 23
  Student Worker for Advancement/Development ............................................................... 23
Confidential III: Advancement Constituent Relationship Management (CRM) ..................... 24
  Events ............................................................................................................................... 24
  Marketing/Communications ........................................................................................... 24
Confidential IV: Advancement Officer ............................................................................... 24
  Academic Executive ....................................................................................................... 24
  Advancement Executive .................................................................................................. 24
  Chief Advancement Officer/Director of Advancement .................................................... 24
  Major/Principal Gifts/Gift Planning ............................................................................... 24
  Corporate/Foundation Relations ....................................................................................... 25
  Annual Giving .................................................................................................................. 25
  Alumni Relations ............................................................................................................ 25
  Donor Research and Analysis ......................................................................................... 25
  Advancement Administrator ............................................................................................ 25
  Stewardship/Donor Relations ......................................................................................... 25
Confidential V: Specialized UIF/UIAA Roles ..................................................................... 25
  Donor Research and Analysis ......................................................................................... 25
  Gift Administration ........................................................................................................ 26
  Trust Services ................................................................................................................ 26
  Information Technology Services .................................................................................... 26

Data and Systems Inventory ............................................................................................... 27

** Confidential information must be stored in a secure environment and should not be redistributed electronically except to persons authorized to receive such content. **
CONFIDENTIALITY OF INFORMATION

Two University-Related Organizations (UROs)—the University of Illinois Foundation (UIF) and the University of Illinois Alumni Alliance (UIAA)—maintain information on friends, alumni, 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 that alumni, staff, and others can access. 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 Alliance 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 Alliance 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: ADD iLEARN Advancement to this list

- 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.

** Confidential information must be stored in a secure environment and should not be redistributed electronically except to persons authorized to receive such content. **
• 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.

• Vocus – Used for Illinois Connection, an advocacy network for the University of Illinois.

The Foundation is the custodian of data contained in TED for use by Advancement staff throughout the University, the Foundation, and the Alumni Alliance. 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 Alliance. 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

**Confidential information must be stored in a secure environment and should not be redistributed electronically except to persons authorized to receive such content.**
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 Alliance – 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) 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.

UIF Training offers a variety of training courses and tutorials through the iLEARN online system. The Alumni Alliance 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 Alliance 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 Alliance 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
** Confidential information must be stored in a secure environment and should not be redistributed electronically except to persons authorized to receive such content. **
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 this 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.

**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.

** Confidential information must be stored in a secure environment and should not be redistributed electronically except to persons authorized to receive such content. **
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 Alliance 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 Alliance 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 Alliance 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 Alliance, 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 Alliance 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 Alliance.

RELEASE

Confidential information is collected and maintained for the purpose of furthering the membership or fundraising operations of the Foundation or the Alumni Alliance, 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 Alliance 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 Alliance 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 Alliance 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 Alliance 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

** Confidential information must be stored in a secure environment and should not be redistributed electronically except to persons authorized to receive such content. **
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 Alliance President and may result in immediate revocation of systems access or termination of employment.

** Confidential information must be stored in a secure environment and should not be redistributed electronically except to persons authorized to receive such content. **
** Confidential information must be stored in a secure environment and should not be redistributed electronically except to persons authorized to receive such content. **
ADVANCEMENT INFORMATION
CONFIDENTIALITY AGREEMENT

UPDATED 04/30/18
The Alumni Alliance, 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 Alliance, 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 Alliance 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.
- Vocus – Used for Illinois Connection, and advocacy network for the University of Illinois.

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

** Confidential information must be stored in a secure environment and should not be redistributed electronically except to persons authorized to receive such content. **
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 Alliance, 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 Alliance 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 Alliance 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 Alliance, 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 Alliance.

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

** Confidential information must be stored in a secure environment and should not be redistributed electronically except to persons authorized to receive such content. **
APPENDIX D: VENDOR CONFIDENTIALITY/NON-DISCLOSURE AGREEMENT

UPDATED 8/27/2018

TERMINATION CLAUSE

The VENDOR agrees that at the termination of this contract, all University of Illinois Foundation data will be either returned to the Foundation and/or destroyed as indicated by the Foundation at the time of contract termination.

REGULATORY MATTERS

Contractor and/or its agents or employees agree to comply with all laws, statutes, regulations, rulings, or enactments of any governmental authority. Contractor shall obtain (at its own expense) from third parties, including state and local governments, all licenses and permissions necessary for the performance of the work.

DATA SHARING

Except as otherwise specifically provided for in this Agreement, the VENDOR agrees that Foundation data will not be shared, sold, repurposed, anonymized, or licensed with any third-party, with the exception of approved subcontractors, without the express approval of the Foundation through a written agreement with the Foundation. VENDOR agrees that VENDOR shall ensure that all approved subcontractors and any third-parties approved by the Foundation in connection with Foundation data relating to this Agreement will be similarly bound to terms restricting their use of such Foundation data like those terms present in this agreement.

USE OF DATA

The VENDOR agrees that data provided to them during the provision of service shall be used only and exclusively to support the service and service execution and not for any other purpose. This shall include not examining data for targeted marketing either within the confines of the service or external to the service (e.g., keyword indexing). The VENDOR may use aggregate statistics on service usage in order to enhance or optimize the functionality of the service. The phrase ‘Foundation data’ includes data uploaded by users of the service and communications between the user, the Foundation, and the VENDOR.

Uses of Foundation data provided under this Agreement other than for the use as specifically detailed in this Agreement is strictly prohibited, unless such other use is subsequently specifically agreed to in writing by the parties.

INTELLECTUAL PROPERTY

The VENDOR acknowledges that all content uploaded to the vendor service, or made accessible to the VENDOR’s systems or personnel remains the intellectual property of the Foundation as defined by existing regulation and Foundation policy.

** Confidential information must be stored in a secure environment and should not be redistributed electronically except to persons authorized to receive such content. **
NOTIFICATION ON SECURITY INCIDENTS

The VENDOR agrees to notify the Foundation when any VENDOR system that may access, process, or store Foundation data is subject to unintended access. Unintended access includes compromise by a computer worm, search engine web crawler, password compromise or access by an individual or automated program due to a failure to secure a system or adhere to established security procedures. The VENDOR further agrees to notify the Foundation within twenty-four (24) hours of the discovery of the unintended access by providing notice via email to security@uif.uillinois.edu.

ACCESS TO DATA

The VENDOR certifies that only employees of the company or approved contractors will be granted access to Foundation data.

ENCRYPTED DATA TRANSMISSION

The Vendor agrees that any transfer of data between the Foundation and the VENDOR or within the VENDOR’s computing environment will take place using encrypted protocols such as SSL, or SFTP.

ENCRYPTION FOR DATA BACKUPS

The VENDOR certifies that all data backups of the Foundation’s data will be stored and maintained in an encrypted format using at least a 128 bit key.

Signature_________________________ Date ____________

Name______________________________

Title______________________________

Vendor____________________________

** Confidential information must be stored in a secure environment and should not be redistributed electronically except to persons authorized to receive such content. **
APPENDIX E: CONFIDENTIALITY AGREEMENT FOR CLUB/GROUP

UPDATED 8/27/2018

Data being provided by the University of Illinois Alumni Alliance 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 Alliance 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:

_____________________________________________  ___________

_____________________________________________

_____________________________________________

** Confidential information must be stored in a secure environment and should not be redistributed electronically except to persons authorized to receive such content. **
## APPENDIX F: ADVANCEMENT DATA ACCESS PLAN

### INFORMATION SECURITY CLASSIFICATION

*Add Advancement Administrator*

<table>
<thead>
<tr>
<th>Proposed Role</th>
<th>Description</th>
<th>Examples</th>
<th>Information Access Categories</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Security Class: Public</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Advancement Constituent</td>
<td>Access to limited contact and degree information regarding individuals in UIAA Directory and Alumni Network. Individuals can opt for non-disclosure.</td>
<td>All UI faculty, staff, and alumni who use UIAA Gateway (Alumni Directory) and/or Network.</td>
<td>Education (Directory), Contact (Limited).</td>
<td>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.</td>
</tr>
<tr>
<td><strong>Security Class: Confidential I</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Business Manager</td>
<td>Access to information necessary to manage pledges, gifts, gift funds, and gift acknowledgement programs.</td>
<td>Business Operations.</td>
<td>Fund/Ledger, Revenue (Limited).</td>
<td>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.</td>
</tr>
</tbody>
</table>

**Confidential information must be stored in a secure environment and should not be redistributed electronically except to persons authorized to receive such content.**
<table>
<thead>
<tr>
<th>Proposed Role</th>
<th>Description</th>
<th>Examples</th>
<th>Information Access Categories</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Class: Confidential II</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Advancement Support</td>
<td>Access to information necessary to perform administrative duties that pertain to Advancement.</td>
<td>Human Resources, Support Staff for Advancement/Development, Student Worker for Advancement/Development.</td>
<td>Public level of access, plus Basic Constituent information—Personal Info, Advancement Employment (Directory) Information, Relationships, Contact information (Full), Documentation, Volunteer</td>
<td>Assistants, other office support professionals, and student employees may request higher access levels if needed to accomplish tasks for other designated persons.</td>
</tr>
<tr>
<td>Security Class: Confidential III</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Advancement Constituent Relationship Management (CRM)</td>
<td>Access to information needed to manage constituent contacts through events, communications, and marketing.</td>
<td>Events, Marketing/Communications.</td>
<td>Internal level of access, plus Full Constituent Information, Revenue, Gift/Funding Agreements, Fund/Designation, Marketing and Communications.</td>
<td>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.</td>
</tr>
</tbody>
</table>

** Confidential information must be stored in a secure environment and should not be redistributed electronically except to persons authorized to receive such content. **
<table>
<thead>
<tr>
<th>Proposed Role</th>
<th>Description</th>
<th>Examples</th>
<th>Information Access Categories</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Security Class: Confidential IV</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Advancement Officer</td>
<td>Access to all appropriate information needed to solicit private support for the University, with ability to view and add solicitations, call reports, etc.</td>
<td>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.</td>
<td>Confidential II level access, plus Prospect, Wealth and Ratings, Prospect Plans, Interactions, Opportunities.</td>
<td>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.</td>
</tr>
<tr>
<td><strong>Security Class: Confidential V</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>UIAA/UIF Specialized</td>
<td>Access to all appropriate information w/ ability to maintain and to modify systems as required.</td>
<td>Specialized functions within UIAA/UIF, including Information Technology, Research, Cash Receipts, Gift Processing, Stewardship Services, and Trust Services.</td>
<td>Confidential III, plus access to various screens and tables.</td>
<td>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.</td>
</tr>
</tbody>
</table>

** Confidential information must be stored in a secure environment and should not be redistributed electronically except to persons authorized to receive such content. **
** Confidential information must be stored in a secure environment and should not be redistributed electronically except to persons authorized to receive such content. **

<table>
<thead>
<tr>
<th>Proposed Role</th>
<th>Description</th>
<th>Examples</th>
<th>Information Access Categories</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>UIAA/UIF Specialized</td>
<td>Access to all appropriate credit card information, bank information, Social Security numbers, and the like as required to conduct business operations.</td>
<td>A small number of staff (&lt; 25) within UIAA/UIF. Limited largely to Gift Administration, Trust Services, and Records</td>
<td>Confidential III, plus controlled access to specific personal constituent information, largely from donors.</td>
<td>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.</td>
</tr>
</tbody>
</table>
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.

** Confidential information must be stored in a secure environment and should not be redistributed electronically except to persons authorized to receive such content. **
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 information must be stored in a secure environment and should not be redistributed electronically except to persons authorized to receive such content. **
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.

** Confidential information must be stored in a secure environment and should not be redistributed electronically except to persons authorized to receive such content. **
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.

** Confidential information must be stored in a secure environment and should not be redistributed electronically except to persons authorized to receive such content. **
**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.

** Confidential information must be stored in a secure environment and should not be redistributed electronically except to persons authorized to receive such content. **
### Data and Systems Inventory

<table>
<thead>
<tr>
<th>Security Class</th>
<th>Information Category</th>
<th>Description</th>
<th>Host System</th>
<th>Category of Misuse</th>
</tr>
</thead>
<tbody>
<tr>
<td>P</td>
<td>Education</td>
<td>Data regarding attendance at the University of Illinois, University Laboratory High School and, in some cases, other higher education institutions.</td>
<td>UIAA Directory, UI Alumni Network, TED</td>
<td>Minor</td>
</tr>
<tr>
<td>P-CI</td>
<td>Contact Information</td>
<td>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</td>
<td>UIAA Directory, UI Alumni Network, TED</td>
<td>Severe</td>
</tr>
</tbody>
</table>

** Confidential information must be stored in a secure environment and should not be redistributed electronically except to persons authorized to receive such content. **
<table>
<thead>
<tr>
<th>Security Class</th>
<th>Information Category</th>
<th>Description</th>
<th>Host System</th>
<th>Category of Misuse</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>UIAA Directory and Alumni Network. Full contact information is available at the CI level.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>I-CV</td>
<td>Training</td>
<td>Information regarding training classes offered by various advancement offices, including offerings, attendance and effectiveness. Examples include attendance rosters, instructor evaluations, and summary reports.</td>
<td><a href="https://ilearn.uif.uillinois.edu/#/dashboard">https://ilearn.uif.uillinois.edu/#/dashboard</a></td>
<td>Serious</td>
</tr>
<tr>
<td>CI-CIII</td>
<td>Constituent</td>
<td>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.</td>
<td>TED</td>
<td>Serious</td>
</tr>
<tr>
<td>CIII</td>
<td>Events</td>
<td>Event invitations and attendance lists.</td>
<td>TED, CVent</td>
<td>Serious</td>
</tr>
<tr>
<td>CIII</td>
<td>Marketing and Communications</td>
<td>Documents and data pertaining to mass contacts by mail, telephone, and email from advancement offices to constituents for purposes of solicitation or communication.</td>
<td>TED</td>
<td>Serious</td>
</tr>
</tbody>
</table>

** Confidential information must be stored in a secure environment and should not be redistributed electronically except to persons authorized to receive such content. **
<table>
<thead>
<tr>
<th>Security Class</th>
<th>Information Category</th>
<th>Description</th>
<th>Host System</th>
<th>Category of Misuse</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Examples include newsletters, events invitations, solicit codes, mail preference codes, marketing efforts, and segments.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CIII</td>
<td>Revenue</td>
<td>Documents and data relating to revenue transactions, including pledges, deferred gifts, outright gifts, securities, gifts-in-kind, grants, and contracts.</td>
<td>TED</td>
<td>Severe</td>
</tr>
<tr>
<td>CIII</td>
<td>Planned Gifts</td>
<td>Documents and data pertaining to planned gifts, including original amounts, adjustments, vehicles, maturity dates, and other information.</td>
<td>TED</td>
<td>Severe</td>
</tr>
<tr>
<td>CIII</td>
<td>Memberships</td>
<td>Commitments and payments to the UI Alumni Alliance for membership programs.</td>
<td>TED</td>
<td>Severe</td>
</tr>
<tr>
<td>CI-CIII</td>
<td>Fund/Designation</td>
<td>Documents and data pertaining to fund balances and transactions.</td>
<td>TED, UIF Online (Fund, Accounting tabs)</td>
<td>Severe</td>
</tr>
<tr>
<td>CIV</td>
<td>Prospect</td>
<td>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.</td>
<td>TED</td>
<td>Severe</td>
</tr>
</tbody>
</table>

** Confidential information must be stored in a secure environment and should not be redistributed electronically except to persons authorized to receive such content. **
** Confidential information must be stored in a secure environment and should not be redistributed electronically except to persons authorized to receive such content. **

<table>
<thead>
<tr>
<th>Security Class</th>
<th>Information Category</th>
<th>Description</th>
<th>Host System</th>
<th>Category of Misuse</th>
</tr>
</thead>
<tbody>
<tr>
<td>CIV</td>
<td>Wealth and Ratings</td>
<td>Wealth and giving capacity information obtained primarily from public sources.</td>
<td>TED</td>
<td>Severe</td>
</tr>
<tr>
<td>CIV</td>
<td>Plans</td>
<td>Collections of steps and solicitations planned by advancement officers for particular prospects.</td>
<td>TED</td>
<td>Severe</td>
</tr>
<tr>
<td>CIV</td>
<td>Interactions</td>
<td>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.</td>
<td>TED</td>
<td>Severe</td>
</tr>
<tr>
<td>CIV</td>
<td>Opportunities</td>
<td>Planned and made personal solicitations from an advancement officer to a prospect, including status and amount.</td>
<td>TED</td>
<td>Severe</td>
</tr>
<tr>
<td>H</td>
<td>Personal Identification Numbers</td>
<td>Credit Cards, SSNs, etc., stored within UIAA/UIF systems or files.</td>
<td>Local UIAA/UIF systems only.</td>
<td>Severe</td>
</tr>
<tr>
<td>All Security Groups</td>
<td>Records</td>
<td>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, acknowledgement letters, summary activity reports, gift related correspondence and payment data.</td>
<td>TED, Hyland OnBase</td>
<td>Various, depending on the document type</td>
</tr>
<tr>
<td>Security Class</td>
<td>Information Category</td>
<td>Description</td>
<td>Host System</td>
<td>Category of Misuse</td>
</tr>
<tr>
<td>----------------</td>
<td>----------------------</td>
<td>-------------</td>
<td>-------------</td>
<td>-------------------</td>
</tr>
<tr>
<td></td>
<td>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.</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

** Confidential information must be stored in a secure environment and should not be redistributed electronically except to persons authorized to receive such content. **