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.

UPDATED 11/2/2018

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.

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

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 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.