The University of Tennessee  
Alumni and Development Information System (ANDI)  
Release and Use of Information Policy Statement

**PURPOSE of ANDI**

ANDI is a computerized data storage and retrieval system that provides the foundation for all communications with the University of Tennessee’s alumni and friends. The system holds over 470,000 records of UT alumni, friends, businesses and other organizations, storing addresses, phone numbers, employment information and other biographic and demographic data. ANDI also serves as the official record of gifts and pledges to the University. ANDI comprises a sophisticated contact management system used to coordinate contact with and solicitation of the University’s major donor prospects and to maintain a record of contacts with those prospects.

ANDI is an implementation of vendor-supplied software, SunGard Higher Education’s Advance suite. User access to ANDI may be granted via a client/server user interface or via a web user interface referred to as AWA (Advance Web Access) or ANDI Web. The policies contained in this document refer equally to both user interfaces as well as to the software, data base structure, and data contained therein; and they apply equally whether the information is accessed directly via the online system or from hardcopy or electronic media reports or downloads generated from the data contained in the ANDI system.

The information contained in ANDI is the property of the University of Tennessee and is to be used in accordance with the policies set forth in this document. Primary responsibility for the management of the computer system and the information it contains rests with the Advancement Services division of the University of Tennessee Office of Development & Alumni Affairs. The ANDI system and users of that system must protect the confidential nature of this information and the privacy of the individuals and organizations involved.

Because ANDI operates on computing equipment and networks maintained by The University of Tennessee’s Office of Information Technology (OIT), all users of ANDI agree to subscribe to all applicable University of Tennessee polices, including but not limited to policy IT0110, the Acceptable Use of Information Technology Resources. (A copy of this policy is contained in Appendix A of this document.) The policies contained in this document in no way override those contained in any University of Tennessee policy and should be viewed as complementary to them.

Any use of ANDI information for purposes other than those outlined in this document or use by individuals or entities not duly authorized is prohibited. Failure by a recipient of information from ANDI to abide by these policies will result in access to services being discontinued and will be subject to disciplinary action as prescribed in University of Tennessee Policies. Disciplinary action may include, but is not limited to: formal reprimand, suspension, termination of employment, and civil and/or criminal penalties as prescribed in the Tennessee Crimes Act (found in the Tennessee Code Annotated, Sections 39-14-601, etseq. – see Appendix C).

The Commission on Educational Fund Raising of the Council for Advancement and Support of Education (CASE) has endorsed and published a document, *Principles and Recommendations Regarding Ethics and Confidentiality in Development Research*. (This document is included as Appendix D.) Additionally, CASE has adopted a *Donor Bill of Rights* (attached as Appendix E). As a member institution of CASE, the University of Tennessee and its advancement professionals should be aware of the letter and spirit of both CASE documents and adhere to the principles contained therein.

- 1 -
GENERAL POLICIES

1. Information contained in ANDI is for the exclusive use of the University of Tennessee and is not for release for commercial or political purposes or to individuals or organizations not affiliated with the University of Tennessee. The information must be used only for the purpose for which it was requested.

2. ANDI and all the data contained in it or extracted from it are classified as Restricted-Confidential (level 3), per UT Policy IT0115, The Information and Computer System Classification, section 5.b.ii (see Appendix B).

3. It is the policy of the Alumni and Development Offices to maintain strict confidentiality of information about alumni, contributors and prospects contained in ANDI. Privacy issues dictate the requirement for confidentiality. We must pay particular attention to item 6 in the Donor Bill of Rights (Appendix E).

4. This information is dynamic, subject to frequent change as alumni and donors move, marry, divorce, die, etc. Because of this volatility, only one official set of data is maintained for use by all University offices. The University of Tennessee makes no claim regarding the accuracy of the information.

5. The original recipient of information from ANDI is responsible for ensuring that all future users of that information are familiar with this policy document. Of particular importance are privacy and confidentiality principles and policies.

6. It is the policy of ANDI to provide information routinely to the following groups:
   - The University of Tennessee Board of Trustees
   - The President of the University of Tennessee and his/her staff
   - The University of Tennessee Alumni Offices
   - The University of Tennessee Development Offices
   - The University of Tennessee National Alumni Association
   - The University of Tennessee National Alumni Association Alumni Chapter Presidents
   - The University of Tennessee Development Council and various campus advisory groups
   - Collegiate development officers of The University of Tennessee, provided they are responsible to the chief campus alumni or development officer.

7. Information is provided to the above groups with the understanding that the information is to be used for University or National Alumni Association sponsored programs or activities. The University of Tennessee does not accept any liability for its use outside the University.

8. The Assistant Vice President for Advancement Services has the final authority to resolve questions regarding what constitutes authorized use of information and who shall be granted access to that information.
9. New requests for information from ANDI should be made to the Department of Advancement Services, Director of Advancement Systems.

10. Authorized users of ANDI information may contract the services of outside vendors such as fundraising consultants or other such enterprises to process and/or distribute information obtained from ANDI. The vendor must agree to use the information only for the purpose intended by the University client and in compliance with all University IT security policies. Sale or transfer of information by the vendor is prohibited.

11. Any copy of information obtained from ANDI (including, but not limited to, hard copy reports, downloaded files, and compact discs) must be destroyed when the project for which it was requested is complete.

12. To maintain the integrity and confidentiality of information contained in ANDI, all users must obtain a user id and password. This user id and password are unique to the individual and must not be shared with anyone else. (See item #1 under the Access Authorization section of this document for instructions on obtaining access to ANDI.)

MANAGEMENT

1. The Director of Advancement Systems makes routine policy interpretations and access decisions.

2. The final authority for all policy and access decisions rests with the Assistant Vice President for Advancement Services.

3. The Director and Assistant Director of Advancement Systems make day-to-day operation decisions.

4. The Director and Assistant Director of Advancement Systems monitor the growth and use of ANDI databases. They also coordinates all activities related to the UT OIT databases with the technical support staff in OIT.

ACCESS AUTHORIZATION

1. Access to ANDI is requested through the Director of Advancement Systems. Access is granted based on a need-to-know basis. Requests for policy or access changes should be submitted to the Director of Advancement Systems. Initial ANDI system access and changes to access require the completion of form Application for Access to ANDI, which may be obtained by sending an e-mail to ANDIHlp@tennessee.edu or by calling 865 – 974 – 4153.
2. Once a user id and password are granted, the ANDI Help Desk or training personnel will contact the user via telephone to inform them of their password. Passwords will not be sent via e-mail. This initial password must then be changed immediately. A user should use a strong password of enough complexity to deter hacking of that password. Passwords must be at least 8 characters and must contain at least three of the following: uppercase alphabetic characters, lowercase alphabetic characters, numbers, and special characters. ANDI passwords should be changed at least every 60 days; and a user should not use any of their previous 8 passwords.

3. It is essential that users understand the nature of the data and how it is to be used and updated. It is also critical that they understand the confidential nature of the data and their role in securing that confidentiality. Therefore, training is required before access is granted to the system. It is the policy of the Department of Advancement Systems to enforce this requirement by providing training of both an initial and an on-going nature to all users of ANDI.

4. Users agree to abide by all UT policies governing the access to and use of information contained in the ANDI system each time they logon to ANDI (via a splash screen with two choices – AGREE or CANCEL). They must AGREE to this statement at each login, or access will not be permitted.

5. Inquiry access to the online portions of ANDI is routinely granted to Alumni and Development officers and their support staff at the University of Tennessee system; University of Tennessee, Knoxville; University of Tennessee, Chattanooga; University of Tennessee, Martin; University of Tennessee, Memphis; Institute of Agriculture; University of Tennessee Space Institute; and the University of Tennessee Medical Center.

6. Update access to basic demographic/biographic and monetary information is limited to staff in the Gift Processing Offices at the University of Tennessee (Systems and Knoxville campus); University of Tennessee, Martin; University of Tennessee, Memphis; University of Tennessee, Chattanooga; and the University of Tennessee Medical Center. Update access to basic demographic/biographic information only is granted to designated support staff in the Alumni offices at the University of Tennessee (System and Knoxville campus); University of Tennessee, Chattanooga; University of Tennessee, Martin; and the University of Tennessee Medical Center.

7. ANDI contains functionality that allows authorized users to create and download files of certain information. These files are for the sole use of the authorized user who created the download file. Requests for files to be downloaded from ANDI for the use of any outside entity should be made through the Director of Advancement Systems. Data transferred via any means to another file or computer system must be properly secured at all times. Such files must be destroyed upon completion of the task for which the data was requested. Recipients of such files assume full responsibility for securing such data and ensuring that the data are used in a manner consistent with this policy. The University of Tennessee assumes no liability for its accuracy or use.
APPENDIX A

University of Tennessee Policy
IT0110

The Policy for Acceptable Use of Information Technology Resources can be viewed by selecting the link below:

Acceptable Use of Information Technology Resources
APPENDIX B

University of Tennessee Policy
IT0115

Policy for Information and Computer System Classification can be viewed by selecting link below:

Information and Computer System Classification
APPENDIX C

Tennessee Computer Crimes Act
Tennessee Computer Crimes Act

39-14-601. Part definitions. As used in this part, unless the context otherwise requires;

(1) "Access" means to approach, instruct, communicate, or connect with, store data in, retrieve or intercept data from, or otherwise make use of any resources of a computer, computer system, or computer network, or information exchanged from any communication between computers or authorized computer users and electronic, electromagnetic, electrochemical, acoustic, mechanical, or other means;

(2) "Authorization" means any and all forms of consent, including both implicit and explicit consent;

(3) "Computer" means a device or collection of devices, including its support devices, peripheral equipment, or facilities, and the communication systems connected to it which can perform functions including, but not limited to, substantial computation, arithmetic or logical operations, information storage or retrieval operations, capable of being used with external files, one (1) or more operations which contain computer programs, electronic instructions, allows for the input of data, and output data (such operations or communications can occur with or without intervention by a human operator during the processing of a job);

(4) "Computer contaminants" means any set of computer instructions that are designed to modify or in any way alter, damage, destroy, or disrupt the proper operation of a computer system, or computer network without the intent or authorization of the owner of the information. They include, but are not limited to, a group of computer instructions commonly called viruses or worms, which are self-replicating or self-propagating and are designed to contaminate other computer programs or computer data, consume computer resources, modify, destroy, record or transmit data, or in some other fashion usurp the normal operation of the computer, computer system, or computer network. Such contaminants may include viruses or worms, which terms shall have the following meanings;

(A) "Virus" means a migrating program which, at least, attaches itself to the operating system of any computer it enters and can infect any other computer that has access to an "infected" computer; and

(B) "Worm" means a computer program or virus that spreads and multiplies, eventually causing a computer to "crash" or cease functioning, but does not attach itself to the operating system of the computer it "infects";

(5) "Computer network" means a set of two (2) or more computer systems that transmit data over communication circuits connecting them, and input/output devices including, but not limited to, display terminals and printers, which may also be connected to telecommunication facilities;

(6) "Computer program" means an ordered set of data that are coded instructions or
(7) "Computer software" means a set of computer programs, procedures, and associated documentation concerned with the operation of a computer, computer system, or computer network whether imprinted or embodied in the computer in any manner or separate from it, including the supporting materials for the software and accompanying documentation;

(8) "Computer system" means a set of connected devices including a computer and other devices including, but not limited to, one (1) or more of the following: data input, output, or storage devices, data communication circuits, and operating system computer programs that make the system capable of performing data processing tasks;

(9) "Data" means a representation of information, knowledge, facts, concepts, or instructions which is being prepared or has been prepared in a formalized manner, and is intended to be stored or processed, or is being stored or processed, or has been stored or processed in a computer, computer system, or computer network;

(10) "Electronic mail service provider" means any person who;
(A) Is an intermediary in sending or receiving electronic mail; and
(B) Provides to end-users of electronic mail services the ability to send or receive electronic mail;

(11) "Financial instrument" includes, but is not limited to, any check, cashier's check, draft, warrant, money order, certificate of deposit, negotiable instrument, letter of credit, bill of exchange, credit card, debit card, marketable security, or any computer system representation thereof;

(12) "Input" means data, facts, concepts, or instructions in a form appropriate for delivery to, or interpretation or processing by, a computer;

(13) "Intellectual property" includes data, which may be in any form including, but not limited to, computer printouts, magnetic storage media, punched cards, or may be stored internally in the memory of a computer;

(14) "Local exchange company" includes telecommunications service providers as defined in § 65-4-101; competing telecommunications service providers as such term is defined in § 65-4-101; telephone cooperatives; cellular or other wireless telecommunications providers; and interactive computer service providers as defined in 47 U.S.C. § 230(f);

(15) "Output" means data, facts, concepts or instructions produced or retrieved by computers from computers or computer memory storage devices;

(16) "Owner" means an owner or lessee of a computer or a computer network, or an owner, lessee or licensee of computer data, computer programs, or computer software;
(17) "Property" shall include:
(A) Real property;
(B) Computers and computer networks; and
(C) Financial instruments, computer data, computer programs, computer software, and all other personal property regardless of whether they are:
   (i) Tangible or intangible;
   (ii) In a format readable by humans or by a computer;
   (iii) In transit between computers or within a computer network or between any devices which comprise a computer; or
   (iv) Located on any paper or in any device in which it is stored by a computer or by a human;

(18) "Services" includes, but is not limited to, the use of a computer, a computer system, a computer network, computer software, computer program, or data to perform tasks;

(19) "System hacker" means any person who knowingly accesses and without authorization alters, damages, deletes, destroys, or otherwise uses any data, computer, computer system, or computer network; and

(20) "To process" means to use a computer to put data through a systematic sequence of operations for the purpose of producing a specified result.


39-14-602. Violations - Penalties. (a) Whoever knowingly, directly or indirectly, accesses, causes to be accessed, or attempts to access any telephone system, telecommunications facility, computer software, computer program, data, computer, computer system, computer network, or any part thereof, for the purpose of:
(1) Obtaining money, property, or services for oneself or another by means of false or fraudulent pretenses, representations, or promises violates this subsection (a) and is subject to the penalties of § 39-14-105;
(2) Causing computer output to purposely be false for, but not limited to, the purpose of obtaining money, property, or services for oneself or another by means of false or fraudulent pretenses, representations, or promises violates this subsection (a) and is subject to the penalties of § 39-14-105;
(3) Effecting the creation or alteration of a financial instrument or of an electronic transfer of funds with the intent to disrupt, alter, misappropriate, or commit fraud violates this subsection (a) and is subject to the penalties of § 39-14-105;
(b) Whoever intentionally and without authorization, directly or indirectly:
(1) Accesses any computer, computer system, or computer network commits a Class C misdemeanor;
(2) Alters, damages, destroys, or attempts to damage or destroy, or causes the disruption to the proper operation of any computer, or who performs an act which is responsible for the disruption of any computer, computer system, computer network, computer software, program, or data which resides or exists internal or external to a computer, computer system, or computer network is punishable as in § 39-14-105;
(3) Introduces or is responsible for the malicious input of any computer contaminant into any computer, computer system, or computer network commits a Class B misdemeanor;
(4) Accesses, causes to be accessed, or attempts to access any computer software,
computer network, or any part thereof, for the purpose of maliciously gaining access to computer material or to tamper maliciously with computer security devices including, but not limited to, system hackers, commits a Class A misdemeanor; or (5) Makes or causes to be made an unauthorized copy, in any form, including, but not limited to, any printed or electronic form of computer data, computer programs, or computer software residing in, communicated by, or produced by a computer or computer network commits an offense punishable as provided in § 39-14-105. (c) Whoever receives, conceals, uses, or aids another in receiving, concealing, or using any proceeds resulting from a violation of either subsection (a) or subdivision (b)(2), knowing the proceeds to be the result of such violation, or whoever receives, conceals, uses, or aids another in receiving, concealing, or using any books, records, documents, property, financial instrument, computer software, program, or other material, property, or objects, knowing that the item has been used in violating either subsection (a) or subdivision (b)(2) is subject to the penalties of § 39-14-105. (d) Any person who violates this section in connection with an act of terrorism commits a Class A felony.  

39-14-603. Unsolicited bulk electronic mail. (a) It is an offense for a person without authority to falsify or forge electronic mail transmission information or other routing information in any manner in connection with the transmission of unsolicited bulk electronic mail through or into the computer network of an electronic mail service provider or its subscribers. (b) Transmission of electronic mail from an organization to its members shall not be deemed to be the transmission of unsolicited bulk electronic mail as prohibited by this section. (c) Nothing in this section shall be construed to interfere with or prohibit terms or conditions in a contract or license related to computers, computer data, computer networks, computer operations, computer programs, computer services, or computer software or to create any liability by reason of terms or conditions adopted by or technical measures implemented by a Tennessee-based electronic mail service provider to prevent the transmission of unsolicited electronic mail in violation of this section. (d) As used in this section, "without authority" means a person who uses a computer, a computer network, or the computer services of an electronic mail service provider to transmit unsolicited bulk mail in contravention of the authority granted by or in violation of the policies set by the electronic mail service provider. (e) The transmission of electronic signals by a local exchange company to the extent that the local exchange company merely carries that transmission over its network shall not be deemed to be the transmission of unsolicited bulk electronic mail as prohibited by this part. (f) A violation of this section shall be punished according to the damage to the property of another caused by the violation and shall be graded as provided in § 39-14-105.  

39-14-604. Civil action - Damages, attorney fees, and costs. (a) Any person whose property or person is injured by reason of a violation of any provision of this part may file a civil action and recover for any damages sustained and the costs of the civil action. Without limiting the generality of the term, "damages" shall include loss of profits. (b) If the injury arises from the transmission of unsolicited bulk electronic mail, the injured person, other than an electronic mail service provider, may also recover attorney's fees
and costs, and may elect, in lieu of actual damages, to recover the lesser of ten dollars ($10.00) for each and every unsolicited bulk electronic mail message transmitted in violation of this part, or one thousand dollars ($1,000) per day. The injured person shall not have a cause of action against the electronic mail service provider that merely transmits the unsolicited bulk electronic mail over its computer network. (c) If the injury arises from the transmission of unsolicited bulk electronic mail, an injured electronic mail service provider may also recover attorney's fees and costs and may elect, in lieu of actual damages, to recover the greater of ten dollars ($10.00) for each and every unsolicited bulk electronic mail message transmitted in violation of this part, or one thousand dollars ($1,000) per day.

(d) At the request of any party to an action brought pursuant to this section, the court may, in its discretion, conduct all legal proceedings in such a way as to protect the secrecy and security of the computer, computer network, computer data, computer program, and computer software involved in order to prevent possible recurrence of the same or a similar act by another person and to protect any trade secrets of any party. The provisions of this section shall not be construed to limit any person's right to pursue any additional civil remedy otherwise allowed by law. [Acts 2003, ch. 317, § 5.]

39-14-605. Venue. For the purposes of venue under the provisions of this part, any violation of this part shall be considered to have been committed: (1) In any county in which any act was performed in furtherance of any transaction violating this part; (2) In any county in which any violator had control or possession of any proceeds of the violation or of any books, records, documents, property, financial instrument, computer software, computer program, or other material, objects, or items which were used in furtherance of the violation; and (3) In any county from which, to which, or through which, any access to a computer, computer system, or computer network was made, whether by wire, electromagnetic waves, microwaves, or any other means of communication. [Acts 1989, ch. 591, § 1; T.C.A. § 39-14-603; Acts 2003, ch. 317, § 6.]

39-14-606. Transmission of electronic signals by a local exchange company. The transmission of electronic signals by a local exchange company to the extent that the local exchange company merely carries that transmission over its network shall not be deemed to be the transmission of unsolicited bulk electronic mail as prohibited by this part. [Acts 2003, ch. 317, § 8.]
APPENDIX D

Case Statement of Ethics
CASE STATEMENT OF ETHICS

Institution advancement professionals, by virtue of their responsibilities within the academic community, represent their colleges, universities, and schools to the larger society. They have, therefore, a special duty to exemplify the best qualities of their institutions and to observe the highest standards of personal and professional conduct.

In so doing, they promote the merits of their institutions, and of education generally, without disparaging other colleges and schools.

Their words and actions embody respect for truth, fairness, free inquiry, and the opinions of others.

They respect all individuals without regard to race, color, sex, sexual orientation, marital status, creed, ethnic or national identity, handicap, or age.

They uphold the professional reputation of other advancement officers and give credit for ideas, words, or images originated by others.

They safeguard privacy rights and confidential information.

They do not grant or accept favors for personal gain, nor do they solicit or accept favors for their institutions where a higher public interest would be violated.

They avoid actual or apparent conflicts of interest and, if in doubt, seek guidance from appropriate authorities.

They follow the letter and spirit of laws and regulations affecting institutional advancement.

They observe these standards and others that apply to their professions and actively encourage colleagues to join them in supporting the highest standards of conduct.

The CASE Board of Trustees adopted this Statement of Ethics to guide and reinforce our professional conduct in all areas of institutional advancement. The statement is also intended to stimulate awareness and discussion of ethical issues that may arise in our professional activities. The Board adopted the final text in Toronto on July 11, 1982, after a year of deliberation by national and district leaders and by countless volunteers throughout the membership.
APPENDIX E

A Donor Bill of Rights
Philanthropy is based on voluntary action for the common good. It is a tradition of giving and sharing that is primary to the quality of life. To assure that philanthropy merits the respect and trust of the general public, and that donors and prospective donors can have full confidence in the not-for-profit organizations and causes they are asked to support, we declare that all donors have these rights:

1. To be informed of the organization's mission, of the way the organization intends to use donated resources, and of its capacity to use donations effectively for their intended purposes.
2. To be informed of the identity of those serving on the organization's governing board, and to expect the board to exercise prudent judgment in its stewardship responsibilities.
3. To have access to the organization's most recent financial statements.
4. To be assured their gifts will be used for the purposes for which they were given.
5. To receive appropriate acknowledgment and recognition.
6. To be assured that information about their donations is handled with respect and with confidentiality to the extent provided by law.
7. To expect that all relationship with individuals representing organizations of interest to the donor will be professional in nature.
8. To be informed whether those seeking donations are volunteers, employees of the organization or hired solicitors.
9. To have the opportunity for their names to be deleted from mailing lists that an organization may intend to share.
10. To feel free to ask questions when making a donation and to receive prompt truthful and forthright answers.

The text of this statement in its entirety was developed by the American Association of Fund-Raising Counsel (AAFRC), Association for Healthcare Philanthropy (AHP), Council for Advancement and Support of Education (CASE), and the Association of Fundraising Professionals (AFP), and adopted in November 1993.