Protection and Use of Faculty, Staff, and Student Identifiers
Standards and Procedures

A. RECORDS CONTAINING IDENTIFIERS*

1. Authorization: Only individuals with a "need-to-know"* should be authorized to access student and employee records. New hires are required to sign the University’s Employee Access and Compliance agreement (EACA) prior to receiving access to institutional identifiers <http://www.albany.edu/its/ITS_forms.htm#Information_Security>. Student employees with access to student and employee records must sign the EACA or an equivalent non-disclosure agreement as a condition of employment.

2. Authentication: The sharing of uniquely assigned authentication credentials (NetIDs, passwords) or authenticating on behalf of another individual for the purpose of granting access to student or employee records is strictly prohibited.

3. Accountability: Business and academic units should maintain accurate records of those employees who have been granted authorized access to institutional identifiers. Reviews of access permissions should be conducted, at minimum, on an annual basis and appropriate changes made as warranted by an employee’s change in status or work responsibilities.

4. Record Distribution and Storage: Records containing identifiers are not to be distributed to or viewed by unauthorized individuals. Such documents are to be stored in secured locations. Individual workstations, multi-function devices (printers, copiers, scanners), and portable media (USB drives, laptops, iPads, smart phones) are not considered secure unless the stored records are encrypted and password protected. In high traffic areas, such documents are not to be left on desks or other visible areas (e.g., computer monitors) in “open view” where they can be subject to casual or incidental viewing.

5. Record Disposal: Repositories of identifiers stored in either paper or electronic formats are to be destroyed (e.g., shredding papers, wiping electronic files) prior to disposal.

6. Historical and Imaged Records: SSNs are included in archived databases and in imaged documents. Such historical records cannot be altered. All records and files containing SSNs data are to be considered sensitive information and must be handled and stored accordingly.

7. Removal of Records: Removal of University records containing SSNs or institutional identifiers from the campus is prohibited unless authorized by division or department heads for specific business purposes.

8. Acceptable Release to Third Parties: The University at Albany may release SSNs or other identifiers to third parties as allowed by law, when authorization is granted by the individuals (student or staff), when the Office of the University Counsel has approved the release (e.g. subpoenas) or when the authorized third party is acting as the University at Albany’s agent in the context of a valid contract or agreement, and when appropriate security is guaranteed by the contract or agreement (e.g., financial institutions providing student loans or other financial services). All such distributions to third parties of institutional data must be performed by University systems of record or by University employees authorized to release this data. Individual employees are not permitted to release this information directly to third parties without proper authorization.
B. SOCIAL SECURITY NUMBERS

1. New York State Laws

a. Employee Records

NYS Labor Law: Section 203-d, effective January, 2009. Unless otherwise required by law, all New York State employers, including the State in its capacity as an employer, are prohibited from:

- Publicly posting or displaying an employee’s SSN;
- Visibly printing an SSN on any identification badge or card, including a timecard;
- Placing an SSN in files with unrestricted access;
- Using an SSN as an identification number for purposes of any occupational licensing; or
- Communicating an employee’s “personal identifying information” to the general public. “Personal identifying information” means any of the following elements alone or in combination with other elements: an employee’s home address or telephone number, personal electronic mail address, Internet identification name or password, parent’s surname prior to marriage, drivers’ license number, or SSN.

b. Non-Employee Records

NYS Public Officers Law, Article 6-A, Personal Privacy Protection Law (PPPL). Effective January, 2010, a new section (96-a) extends the prohibitions of Section 399-dd of the General Business Law to the context of the State and its political subdivisions. Under Section 96-a, the State shall not:

- Intentionally communicate to the general public or otherwise make available to the general public in any manner an individual’s social security account number.
- Print an individual’s social security account number on any card or tag required for the individual to access products, services or benefits provided by the state and its political subdivisions.
- Include an individual’s social security account number, except for the last four digits, on any materials that are mailed to the individual, or in any electronic mail that is copied to third parties, unless:
  - State or federal law requires the social security account number to be on the document to be mailed; or
  - The State chooses to include the social security account number in applications and forms sent by mail, including documents sent as part of an application or enrollment process, or to establish, amend or terminate an account, contract or policy, or to confirm the accuracy of the social security account number, (but social security account numbers permitted to be mailed under this exception may not be printed, in whole or in part, on a postcard or other mailer not requiring an envelope, or visible on the envelope or without the envelope having been opened).
- Encode or embed a social security account number in or on a card or document, including, but not limited to, using a bar code, chip, magnetic strip, or other technology, in place of removing the social security account number.

The State shall not require an individual to:
• Transmit the individual’s social security account number over the Internet unless the connection is secure or the social security account number is encrypted; or
• Use the Individual’s social security account number to access an Internet website, unless a password or unique personal identification number (PIN) or other authentication device is also required to access the Internet website. Such passwords and PINs should be unique to the individual and based on information which is private and not generally available to others.

2. FERPA Directory Information: The University at Albany considers SSNs to be non-directory information under the Family Educational Rights and Privacy Act of 1974 (FERPA).

3. Partial SSNs: The use of partial SSNs as identifiers should be avoided, particularly in the case of public displays or releases (e.g., via e-mail to multiple students or staff, student rosters, bulletin boards, public grade postings).

4. Collection, Storage, and Transmission: SSNs may be collected as part of the application or hiring process, and are required for registration or employment at the University at Albany. SSNs are also required for government reporting, financial aid, and various business processes.

Care must be taken in the collection, storage, and transmission of SSNs to maintain the confidentiality of this information. Transmission of SSNs over public networks requires encryption in accordance with NYS Cyber Security Standards [S10-006: Cryptographic Controls <http://www.dhses.ny.gov/ocs/resources/>].

   a. Individual employees are prohibited from creating and storing on local workstations, portable devices, or remote (“cloud”) storage facilities collections of SSNs and names in spreadsheets, personal databases (e.g., MS Access), or other electronic formats.

   b. Where storage and removal of SSNs on portable devices is approved for specific business purposes, the files must be encrypted.

Unless otherwise required, the collection and storage of SSNs is prohibited.

5. Minimize Instances of SSNs: The risk of unauthorized disclosure of the SSN increases with each additional electronic or paper copy of the SSN. Divisional leadership is responsible for ensuring that the number and extent of physical and electronic repositories of SSNs are kept to the minimum necessary.

6. Administrative Research with SSN Data: Electronic data maintained for institutional research, enrollment planning, and university planning are considered to be administrative research data for the purposes of this protocol. Administrative research databases or datasets may continue to store or otherwise maintain SSNs so long as divisional leadership is responsible for:

   a. minimizing the use of SSN,

   b. maintaining an up-to-date inventory of SSN databases and datasets,

   c. documenting security controls and risk remediation.

7. Academic Research with SSN Data: Research databases that include SSNs or other forms of regulated data* must be disclosed by the investigator to the Office of Regulatory Research Compliance (ORRC) and the Information Security Officer (ISO). Researchers are responsible for:

   a. minimizing the use of SSN or other forms of personal identification,
b. maintaining an up-to-date inventory of SSN databases and datasets, and other repositories of identifiers,

c. documenting security controls and risk remediation and communicating these to the ORRC and ISO.

February, 2012