Introduction to the Protection and Use of University Identifiers Protocol

A component of the University’s Information Security Program

This protocol, its accompanying standards and procedures, and a glossary of technical and legal terms, are designed to offer a set of principles for evaluating the relative sensitivity of personal identifiers, rules and practices designed to minimize and mitigate the threats of exposure or loss of business records containing identifying information, and support for the campus Internal Controls initiative.

Faculty and staff at the University at Albany are required to collect and use a wide variety of information, in both paper as well as electronic formats. Grades, research data, application submissions, health records, and financial transactions are just some of the types of business records we utilize in the course of performing our work.

As criminal fraud incidents involving stolen or lost information have proliferated, states and the federal government have imposed increasingly stringent requirements on businesses and government entities to ensure that adequate protections are applied to collections of business records containing sensitive, personal information.

The Family Education Rights and Privacy Act (FERPA) and the Health Insurance Portability and Accountability Act (HIPAA) are two examples of federal legislation that require specific levels of protection and authorize penalties for failure to comply with those requirements.

Two statutes in New York State, the Information Security Breach and Notification law and the Social Security Protection law, impose severe penalties for the mishandling and misuse of social security numbers. Recently, new provisions in the state’s Labor Law and Public Officers Law imposed additional restrictions on the use of social security account numbers by state entities.

Because of the possible sanctions the University could suffer resulting from the loss or exposure of regulated information, and the increasing threats to that information posed by cyber crime and emerging technologies (e.g., cloud services, social networking sites), it is vitally important that University faculty and staff understand what business records they need to protect, and how best to protect them.
Protection and Use of Faculty, Staff, and Student Identifiers Protocol

Pursuant to the University at Albany Information Security Policy, this protocol is established as part of the Identity Management Security Domain*. [An asterisk indicates that the term is defined in the attached glossary.]

SECURITY DOMAIN

Identity Management—A comprehensive and unified approach to managing the identities of persons and processes issued by the University for the purpose of granting and controlling access to campus information resources. This includes exercising due care in the areas of identity assurance, issuance, authentication, authorization, revocation, and recovery of identity elements (NetIDs, tokens, etc.).

OBJECTIVES

1. Broaden awareness about the need to maintain confidentiality and privacy of unique identifiers used at the University.
2. Reduce reliance on and use of SSNs for identification purposes.
3. Establish consistent University-wide and divisional protection and use policies and practices for institutional identifiers.
4. Increase student and employee confidence surrounding handling of their personal identifiers, including SSNs.

BACKGROUND

Given the increasing trend of data breaches and the legal and financial penalties facing those organizations that suffer the exposure of personal, private, and sensitive information, as well as the serious reputational damage that can result from such incidents, it is in the University's best interest to formulate standards and procedures for handling and safeguarding personal identifiers.

The University at Albany is committed to ensuring the privacy and proper handling of confidential information it collects and maintains on faculty, staff and students, including the Social Security Number (SSN) which is required for state and federal government reporting purposes. It is the policy of the University at Albany to protect the privacy of SSNs and to place appropriate limitations on its use throughout the admission, financial aid, billing, registration, and HR processes. These limitations apply equally to University information systems and the information systems of contracted third parties.

Likewise, the University creates, assigns, and uses unique identifiers to accurately distinguish and track faculty, students, and staff through a myriad of business, research, academic, and health care processes. Changes in FERPA rules (Dec 08) require institutions to maintain appropriate levels of privacy protection for these institutional forms of identification due to their close association with educational records. Sensitive information related to employment and health records are linked to them, as well.

This protocol outlines the acceptable use of SSNs and all other institutional identifiers, limiting their use to business purposes only and establishing procedures to assure that University employees are aware of and comply with all applicable laws and regulations.

SCOPE

This is a University-wide protocol affecting all business and academic units and affiliate entities that rely on University institutional identifiers for their operations.
GUIDING PRINCIPLES

1. Use of unique identifiers should progress from the least confidential required to the most confidential. For example, if a NetID or AlbanyID is sufficient to uniquely establish an identity, these identifiers should be used instead of SSNs. Generally speaking, the least confidential identifier is a name; the most confidential identifier is the SSN with the name.

2. The number of unique identifiers required should be determined by the minimum needed to effect the transaction. If the Albany ID is sufficient to positively identify someone, there is no need to add additional identifiers to the record set unless they are essential to the transaction.

3. Excluding systems of record, identifiers should not be retained beyond the period defined by document retention requirements, or if otherwise unspecified, the time needed to complete the transaction requiring their use.

ROLES AND RESPONSIBILITIES

1. Regulatory Compliance. All staff are expected to know, understand, and comply with the regulations governing the collection, distribution, storage, and disposal or destruction of information they work with in the course of performing their duties.

2. Supervisory Personnel. In addition to the above general compliance requirement, supervisory personnel have the following responsibilities:
   a. Ensure that their staff understand and adhere to the statutory or University regulations that govern the use of the unit's or department's information.
   b. Ensure compliance and adherence on the part of employees to the protocol's Standards and Procedures document (See Related Documents for link).
   c. Periodically review and update data access permissions and privileges to ensure that staff have appropriate access levels to records. Terminations, transfers, and changes in employee work assignments require a review and adjustment of employee access privileges.
   d. Report incidents of abuse of privileges, or unauthorized access to information, to the appropriate authorities upon discovery of such abuse or unauthorized access.

COMPLIANCE

Compliance with this protocol and its related standards and procedures will be in accordance with the Compliance section of the University's Information Security Policy as well as any and all applicable laws.

REVIEW

This protocol and all related published documents will be reviewed no less than once every three years.

RELATED DOCUMENTS

Protection and Use of Identifiers: Standards and Procedures
- [https://wiki.albany.edu/download/attachments/33496625/Protection_of_Identifiers_Standards_Procedures.pdf?version=1&modificationDate=1296847520730>

Internal Control Vulnerability Assessment (See Factor 10)
- [http://www.albany.edu/internalcontrol/links.shtml>

SUNY Information Security Guidelines, Part 1: Campus Programs & Preserving Confidentiality, #6608
NYS Labor Law

www.albany.edu
NYS Public Officers Law
NYS Social Security Number Protection Law
Federal Educational Rights and Privacy Act
Federal Trade Commission Identify Theft Red Flag Rules
Health Insurance Portability and Accountability Act
Gramm Leach Bliley Act
Freedom of Information Law
NYS Information Security Breach & Notification Law
NYS Business Law and Technology Law
NYS Information Security Policy P03-003
SUNY Policies of the Board of Trustees

February, 2011
Protection and Use of Faculty, Staff, and Student Identifiers Glossary

Confidentiality
Confidentiality is concerned with controlling the dissemination or publication of information that, if widely publicized, or obtained by unauthorized individuals, could result in harm to the subjects of the information. In some cases, certain types or classes of data are statutorily regulated and require data owners to implement certain controls to prevent the unauthorized disclosure of this information (see Regulated Data below).

Encryption
Encryption refers to the process whereby plain text is converted into humanly un-decipherable text by the application of an encryption algorithm. Encryption requires the use of a key that is applied to the plain text by the algorithm to generate the encrypted text. The same key is required to de-crypt the text in symmetric encryption. In asymmetric encryption schemes, a private-public key pair is used for the encryption-decryption process. Generally speaking, only the individuals who possess the key can read the encrypted text. Therefore, care must be taken to keep the keys secret to prevent unauthorized access.

Identifiers
For the purpose of this protocol, the term identifier applies to any data element that uniquely distinguishes any member of the University at Albany community. Different identifiers may be used for different business processes, and not all identifiers require the same level of confidentiality. The use and protection of some identifiers (e.g., Social Security numbers) are subject to statutory requirements (FERPA, NYS Information Security Breach and Notification Law, HIPAA).

“Need-to-know”
Because of the potential harm resulting from unauthorized disclosure, access to sensitive or regulated data should be governed and limited by the individual's need to utilize that information for legitimate business purposes. As employees' roles or duties change, so will their need to access different data collections and data elements (fields) within those collections.

Regulated Data
Regulated data refers to any data elements or data collections subject to regulatory controls. Examples of regulated data include education records (FERPA), personal health information (HIPAA), Social Security numbers (NYS ISBN Law, NYS Labor Law, NYS Public Officers Law), and financial records (FTC Red Flag Rules, Gramm Leach Blilley). Penalties for failing to comply with regulatory requirements can result in severe financial and operational sanctions (e.g., loss of federal education aid).

Security Domain
The University at Albany's Information Security policy identifies ten domains which serve as a basis for protocol development and controls management. Examples of other domains include: Asset Classification, Access Control, and Incident Detection and Management.