

M E M O R A N D U M

To: Employees and Appointees, University at Albany and its Affiliated Entities
From: Office of the Chief Information Officer
Re: Protection of University at Albany Business Records

Faculty and staff at the University at Albany are required to collect and use a wide variety of information. Grades, research data, application submissions, health records, and financial transactions are just some of the types of academic and business records we use 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.

Because of the possible sanctions the University could suffer resulting from the loss or exposure of regulated information, and the increasing threats targeting that information, it is vitally important that University employees accept the role of informed guardians of campus business records.

By signing the attached **Employee Access and Compliance Agreement**, you agree to comply with the applicable laws and University policies and procedures governing the handling and use of those records. Your efforts in protecting information vital to the campus's mission of teaching, learning, and research are greatly appreciated.

July 2010

University at Albany
Office of Human Resources Management
Office of the Chief Information Officer

EMPLOYEE ACCESS AND COMPLIANCE AGREEMENT

I understand that I am being granted access to information and data that may contain records subject to federal or state regulations (“regulated data”) regarding privacy and confidentiality, and that I may handle other information considered Personal, Private, and Sensitive. My continued access to this information is based on my agreement to comply with the following terms and conditions:

- **I will comply with all state and federal laws and University policies that govern access to and use of information about employees, applicants, students or donors.**

- **My right to access this is strictly limited to the specific information and data that is relevant and necessary for me to perform my job-related duties.**

- **I am prohibited from accessing, using, copying or otherwise disseminating regulated data that is not relevant and necessary for me to perform my job-related duties.**

- **I will not share regulated data unless explicitly authorized to do so, and in no instance will I share regulated data with third parties without appropriate authorization.**

- **I will sign-out of electronic records systems when I am not actively using them.**

- **I will keep my account credentials (e.g., NetID, password) confidential, and will not disclose or share them with anyone.** (Please note: Any request for your UAlbany password(s) in any format, by phone, email, or in person, should be considered fraudulent.)

I understand that violations of this agreement may result in the revocation of my access privileges to University information systems, may result in appropriate administrative action, including, but not limited to, disciplinary action, and may also subject me to prosecution by federal or state authorities.

I certify that I have read this Access and Compliance Agreement and the attached NYS policy excerpt pertaining to Personal, Private, and Sensitive Information (PPSI), that I understand both, and that I agree to comply with the above terms and conditions.

_____ Signature	_____ Name (Please print)	_____ Date
_____ Title	_____ Department	

New York State Cyber Security Policy P03-002: Information Security Policy Rev. Date: August 1, 2007

Personal, Private, and Sensitive Information (PPSI): Any information where unauthorized access, disclosure, modification, destruction or disruption of access to or use of such information could severely impact the University, its critical functions, its employees, its customers, third parties, or citizens of New York. This term shall be deemed to include, but is not limited to, the information encompassed in existing statutory definitions, e.g., General Business Law §§399-dd; 399-h(1)(c),(d),(e); 899-aa(1)(a)(b); Public Officers Law, §§86(5); 92(7), (9); State Technology Law §§202(5); 208(1)(a).

PPSI includes, but is not limited to:

- Information concerning a person which, because of name, number, personal mark or other identifier, can be used to identify that person, in combination with:
 - Social Security Number or any number derived from the Social Security Number;
 - driver's license number or non-driver identification card number; or
 - mother's maiden name; or
 - financial account identifier(s) or other information which would permit access to a person's financial resources or credit.
- Information used to authenticate the identity of a person or process (e.g., PIN, password, passphrase, biometric data). This does not include distribution of one-time-use PINs, passwords, or passphrases.
- Information that identifies specific structural, operational, or technical information, such as maps, mechanical or architectural drawings, floor plans, operational plans or procedures, or other detailed information relating to electric, natural gas, steam, water supplies, nuclear or telecommunications systems or infrastructure, including associated facilities, including, but not limited to:
 - training and security procedures at sensitive facilities and locations as determined by the Office of Homeland Security (OHS);
 - descriptions of technical processes and technical architecture;
 - plans for disaster recovery and business continuity; and
 - reports, logs, surveys, or audits that contain sensitive information.
- Security related information (e.g., vulnerability reports, risk assessments, security logs).
- Other information that is protected from disclosure by law.