

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

PERSONAL ACCOUNT ACCESS AND COMPLIANCE AGREEMENT

Required of all individuals seeking access to University at Albany Personal Accounts

I certify that I have received and read the attached information regarding policies that govern access to and use of non-public Personal, Private, and Sensitive Information (PPSI) about employees, applicants, students or donors.

I understand that I am being granted limited access to information and data that may contain non-public PPSI, and that my access to this information is based on my agreement to comply with the following terms and conditions:

- My right to access material residing in a University at Albany personal account is strictly limited to the terms and conditions specified in this document
- I will comply with the state and federal laws and University policies that govern access to and use of information about employees, applicants, students or donors (e.g., FERPA, HIPAA).
- Access is restricted to the information and data that was identified in my "Request for Access" form (attached) submitted to and approved by the Office of University Counsel.
- I am prohibited from copying or otherwise disseminating information or data that may be held in the account unless explicit permission to do so was granted to me in the "Request for Access" form.
- I am prohibited from viewing, using, copying or otherwise disseminating additional information or data that may be held in the account other than the information specifically identified in the "Request or Access" form.
- I will limit access to the dates and times stipulated.
- I will maintain the privacy and confidentiality of the information and data that I access.
- I will not share information or data unless explicitly authorized to do so, and in no instance will I share PPSI with third parties without written authorization.
- I will keep account credentials (e.g. passwords) confidential, and will not disclose or share them with anyone.

I understand that violations of this agreement may result in appropriate administrative action, including, but not limited to, disciplinary action, and may also subject me to prosecution by state or federal authorities.

I certify that I have read this "Access and Compliance Form," and the attached information pertaining to access to and use of information contained in employee, applicant, student or donor records, that I understand both, and that I agree to comply with the above terms and conditions.

Signature

Name (Please print)

Date

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; financial services account number or code; savings account number or code; checking account number or code; debit card number or code; automated teller machine number or code; electronic serial number.
- Other *information* which could be used to assume a person's identity or gain 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).
- *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 or relates to subjects and areas of concern as determined by the University's executive management.