University Security Camera System
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 SUNY 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 the University Security Camera 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 the University Security Camera 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.

Definition of Personal, Private, and Sensitive Information (PPSI)

New York State Cyber Security Policy P03-002: Information Security Policy
Rev. Date: March 10, 2017

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 State Entity (SE), 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[1]. 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;
    - driver's license number or non-driver identification card number;
    - 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, and 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 or relates to subjects and areas of concern as determined by SE executive management.

[1] General Business Law §§399-ddd; 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).

I acknowledge that I have received training on how to access and use the University Enterprise Camera system. I have read and understand the policies and procedures governing its access and usage. I agree to use the system only as intended.

Print Name _____ Date: _____

Signature _____