SUNY Cobleskill
Confidentiality and Security Compliance Agreement

I understand that I may be 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 regardless of my SUNY Cobleskill employment, internship or volunteer status:

- I will comply with all state and federal laws and college policies that govern access to and use of information about employees, interns, volunteers, applicants, students, donors and vendors.
- 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., UserID, password) confidential, and will not disclose or share them with anyone. A request for someone else to use your Cobleskill password(s) is considered fraudulent activity.
- If issued keys or other means of entry, I will not copy or share them with anyone and I will report lost or stolen keys immediately to my supervisor.

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 College, 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, 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 the College's executive management.

Family Educational Rights and Privacy Act (FERPA)

The Family Educational Rights and Privacy Act (FERPA) is a federal law enacted in 1974 that protects the confidentiality of a student's records. As an employee of SUNY Cobleskill, you must become familiar with the basic provisions of FERPA to comply with this federal law. All employees, including full-time, part-time, hourly, and student employees, have the same responsibilities under FERPA. Student educational records must only be accessed if there is a legitimate educational reason to do so.

All student information gained from student records (whether the files are paper or computer generated) or from conversations heard in the course of your work are strictly confidential. As such, you may not share this information with anyone. In addition, no files or copies of records are ever allowed to leave the office or department. Files or copies of records are not to be left unattended in public areas for others to view.

You must avoid acquiring student information that you do not need to do your job, nor should you exchange information about students that you may have learned while performing your job unless there is legitimate educational reason to do so. Disclosure of information (for example, telling another person of a student's class schedule) is considered a violation.

I understand that violations of this agreement may result in the revocation of my access privileges to college information systems, appropriate administrative action, including but not limited to disciplinary action and termination, and may also subject me to prosecution by federal or state authorities.
I certify that I have read all of the above information pertaining to Personal, Private, and Sensitive Information (PPSI) and I agree to comply with the above terms and conditions.

Print Name	Signature	Date