ALBANY STATE UNIVERSITY

SUBJECT: Confidentiality and Security Access Policy

SCOPE: All Employees and Associates

PURPOSE: To Establish the Responsibility of Employees and Associates to Protect the Confidentiality of Confidential Information to Which They Have Access

---

Policy Statement: All Albany State University employees and associates must hold confidential information used or obtained in the course of their duties in confidence. All employees and associates with access to confidential information, including, student records, employment information and/or information systems must read and sign the *Albany State University Confidentiality and Security Access Agreement*, which will be kept on file and updated annually.

Definitions:

Confidential Information: all records, files, reports, protocols, policies, manuals, databases, processes, procedures, computer systems, materials and other information pertaining to the operations of Albany State University, as well as all individually identifiable health information pertaining to employees of Albany State University. Confidential information includes, but is not limited to, past, present or future information about an employee or student, employee records, student educational records, processes, marketing plans or techniques, product or service plans, strategies, forecasts, vendor lists, discoveries, ideas and financial information. Confidential information may be obtained by hearing it, seeing it, viewing a record/file or accessing a University computer system, and it may be in any form including, but not limited to, paper, a computer screen, electronic media, a recording device, etc.

Need-to-know: that which is necessary for one to adequately performs one's specific job responsibilities at or for Albany State University.

Associates: includes, but is not limited to, all employees, volunteers, affiliated students, vendors, contractors and any external agencies that have access to confidential information about Albany State University or its employees.

Proprietary Information

It is the policy of Albany State University to respect the proprietary rights of the companies that develop and support the computer software we use. All Albany State employees and associates who use a personal computer system are required to comply with license agreements associated with the computer software products used. Personal computer systems may not be used for any purpose that violates the law. It is against Albany State University policy to make illegal copies, download or transmit information or software in violation of copyright laws. No software may be installed on any computer system without prior authorization from Division of Information

Technology and Administrative Services. (DITAS)

Monitoring Access to Confidential Data

DITAS is responsible for data security and shall audit the access to enterprise-wide systems and data. This includes, but is not limited to, access to Network, Email, Internet, Human Resources, Accounts Payable, and Payroll.

Protecting Confidential Information

Employees and associates of Albany State University have a responsibility to protect confidential information and therefore may not use or disclose confidential information except in accordance with applicable Albany State University policies and procedures. Employees and associates shall not disclose information in any form (whether verbal, written, electronic, by fax, etc.) without authorization.

Verbal Communication

While on duty at Albany State University, confidential information shall not be discussed where others may hear the conversation, such as in hallways, on elevators, in the cafeteria, etc. Dictation of confidential information should occur in locations where others cannot overhear. While off duty, employees and associates shall not discuss any confidential information.

Written Communication

Confidential papers, reports and computer printouts should be kept in a secure place. Confidential documents should not be left unattended or where they may be viewed by others who do not have a need to know. Confidential documents should be retrieved as soon as possible from copiers, mailboxes, conference room tables and other publicly accessible locations. When no longer needed, confidential documents should be deposited in the document destruction bins. Confidential documents shall not be sent or taken outside of Albany State University except in accordance with applicable University policies and procedures.

Electronic Communication

All confidential information residing within computers, networks, servers, software applications, electronic mail, diskettes and any other storage media is the sole property of Albany State University. Confidential information should not be sent or taken outside the organization or disclosed to anyone who does not have a need-to-know, except in accordance with applicable University policies and procedures. Computer monitors should be positioned so that others cannot easily view the information. A computer user must log out of any computer session opened under his or her user name and password prior to leaving any computer or terminal unattended. Users should always be aware of anyone around them who does not have a need to know so that confidential information is not exposed.

Faxed Information

All employees and associates shall take precautions to protect confidential information when using fax machines to transmit or receive documents. All fax machines shall be located in secure areas away from public access. When sending a fax, be absolutely sure that the correct number is dialed and that a cover sheet is always used. The cover sheet should contain the sender's name, the sender's contact number, the receiver's name, the receiver's fax number, the number of pages and a standard confidentiality statement. When receiving a fax, immediately remove the fax transmission from the fax machine and deliver it to the intended recipient. Destroy or place in a document destruction bin any confidential information received in error and immediately inform the sender.

Compliance

It is the duty of each employee and associate to promptly report any suspected violation of these standards to the employee's supervisor or to the Department of Human Resources.

Consequences of Confidentiality Violations

The consequences of violating the confidentiality of student information or educational records, employee information, business information, financial information and other confidential information relating to Albany State University will result in discipline up to and including immediate termination. Violation of confidentiality policies may also lead to civil and criminal liability.

Levels of Confidentiality Violations

Level 1. Carelessness - An employee or associate unintentionally or carelessly accesses, reviews or reveals confidential information to him/herself or others without a legitimate need-to-know. Examples include, but are not limited to: an employee or associate discussing confidential information in a public area; an employee or associate leaving a copy of confidential information unsecured; an employee or associate leaving a computer on which confidential information is displayed unattended or unsecured.

Level 2. Curiosity or Concern (no personal gain) - An employee or associate intentionally accesses, reviews or discusses confidential information for purposes other than the care of the patient or authorized purposes, but for reasons unrelated to personal gain. Examples include, but are not limited to: an employee or associate looking up a birth date or an address of a friend or relative; an employee or associate accessing and reviewing a patient’s record out of concern or curiosity.

Level 3. Personal Gain or Malice - An employee or associate accesses, reviews or discusses confidential information for personal gain or malicious intent. Examples include, but are not limited to: an employee or associate reviewing, accessing or communicating confidential information for use in a personal relationship; an employee or associate compiling a mailing list for personal use or

to be sold; an employee or associate using confidential information to hurt or harm others.

Procedure for Sanctions

Sanctions for members of the workforce can include documented performance counseling up to dismissal depending on the level of violation and management's consideration of all relevant factors. Listed below are possible sanctions based upon the level of violation.

1). Level 1. Violations – Documented performance counseling and warning by the first immediate supervisor.

2). Level 2. Violations - First line supervisor and next immediate supervisor contact the Department of Human Resources to initiate a Written Warning in accordance.

3). Level 3. Violations – Most senior staff member directly responsible for operations contacts the Department of Human Resources to initiate a Written Warning or formal disciplinary action up to and including dismissal in accordance with Albany State University and University System of Georgia Policies and Procedures.