Policy Title	**Information Security Program**	**Policy Number**	**209**
Section	**Financial Affairs and Development**	**Approval Date**	**12/2005**
Subsection	**General Financial Policies**	**Effective Date**	**12/2005**
Responsible Office	**Information Technology**	**Review Date**	**2/2012, 5/2013, 5/2014, 7/2015, 6/2019, 12/15/2020**

1.0 Purpose

1.1 The purpose of the Information Security Program Policy to comply with the Gramm-Leach-Bliley Act of 1999 and the New York State Information Security Breach and Notification Act of 2005.

2.0 Policy

2.1 It is the policy of Jamestown Community College (JCC) to:

- ensure the security and confidentiality of customer records and information;
- protect against anticipated threats to the security and/or integrity of such customer records and information;
- guard against unauthorized access to or use of customer records or information that could result in substantial harm or inconvenience to any customer;
- comply with the Gramm-Leach-Bliley Act (GLB) and the rules promulgated thereunder by the Federal Trade Commission;
- comply with the NYS Information Security Breach and Notification Act (NYSISBNA) comply with the Federal Trade Commission's ("FTC") Red Flags Rule, which implements Section 114 of the Fair and Accurate Credit Transactions Act of 2003

3.0 Procedures

3.1 Program Coordination.

3.1.1 The President shall appoint the Information Security Committee to coordinate college compliance with the GLB and NYSISBNA, and the FTC Red Flag Rules.

3.1.2 The program shall include input from other departments as warranted, including college counsel.

3.1.3 The program will be reviewed and evaluated periodically. Selected aspects will be tested and adjustments to the program will be made as needed.

3.2 Risk Assessment and Safeguards. There is inherent risk in handling and storing any information that must be protected. Identifying areas of risk and maintaining appropriate safeguards can reduce risk. Safeguards are designed to reduce the risk inherent in handling customer information. The college will address the following areas to assure that the appropriate administrative, technical, or physical safeguards

are used to access, collect, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle customer information:

- Employee Management and Training
- Information Systems
- Managing System Failures
- Service Providers

3.3 Program Details

3.3.1 Program Coordinator. The President has designated the Information Security Committee as Program Coordinator.

3.3.2 Representatives: This committee is chaired by the Executive Director of Human Resources and Executive Director of Technology and consists of members from the following offices: Academics, Admissions, Business Office, Workforce Readiness, Student Affairs, Marketing, Financial Aid, Faculty Student Association, Foundation, Health Center, Human Resources, Information Technology, Institutional Research, and Registrar.

3.3.3 Offices Possessing/Safeguarding Customer Information: The following have been identified as among the relevant offices to be considered when assessing the risks to customer information: Admissions, Alumni Affairs, Business Office, Campus Life, Workforce Readiness, Counseling Center, Financial Aid, Faculty Student Association, Health Center, Human Resources, JCC Foundation, Registrar, Student Affairs, Information Technology, Institutional Research, Small Business Development Center, and North County Extension Center.

3.4 Employee Management and Training. Employees handle and have access to customer information in order to perform their job duties. This includes permanent and temporary employees and work-study students, whose job duties require them to access customer information or work in a location where there is access to customer information.

3.4.1 Hiring Employees. The college exercises great care in trying to select well-qualified employees. Hiring supervisors and search committees review applications/resumes, carry out interviews and check references before making their final selection. The director of human resources acting as affirmative action officer also reviews the resumes and signs off on the search procedure providing an additional review of the process and the hire.

3.4.2 Work-Study Students (& Temporary Employees). Work-study students are referred by the financial aid office and the counseling office. Individual offices interview the students referred and make the final decision before a student is placed. Confidentiality and safeguarding of information and the college's Acceptable Use Policy is covered in an individual orientation session.

3.4.3 Permanent Employees. All employees who have access to secure information in Banner are trained about Information Security Program and the college's Acceptable Use Policy. Every new employee is required to complete training through SafeColleges. All employees receive a copy of the document "Maintaining the Security, Confidentiality & Integrity of Customer Information" and the College's Acceptable Use Policy.

3.4.4 Ongoing Training. Periodically, employees with access to protected customer information take part in FERPA and Information Safeguard training, as a refresher.

3.4.5 Access to Customer Information. Only employees whose job duties require them to access customer information shall have access. Access will be limited to the fields, screens, and tables that contain information required for an employee to do their job. Student-worker access will also be limited in a similar fashion. The Management Information Systems (MIS) department is authorized to establish administrative student accounts at the request of each department head. The student accounts will allow Windows access to restricted programs and BANNER forms as defined by each department head. The department supervisor will be responsible to ensure appropriate training.

3.4.6 Disciplinary Measures for Breaches. Breaches of information security may result in appropriate disciplinary action depending on the nature and severity of the breach. Each department is expected to follow appropriate chain of command in dealing with accidental breaches of security. Issues identified should be rectified as soon as possible. Where the breach is determined to be serious in nature or intentional and/or malicious these incidents should be reported to the Executive Director of Human Resources and the Executive Director of Technology.

3.4.7 Notification of a Breach. If a breach occurs, the Executive Director of Technology, Director of MIS and/or the Director of Information Technology Services (ITS) should be notified immediately upon discovering of a potential breach. The Director of MIS and/or Director of ITS will investigate the situation and report their findings to the Executive Director of Technology and the Vice President of Administration. The following factors will be assessed in determining if a breach has occurred:

- Indications that the information is in the physical possession and control of someone unauthorized (i.e. lost or stolen computer)
- Indications that the information has been downloaded or copied.
- Indications that the information was used by an unauthorized individual (i.e. fraudulent accounts opened or instances of identity theft.)

If it is determined that a breach has occurred, the Vice President of Administration will:

- Consult with NYS Cyber Security Critical Infrastructure Coordination (NYS-CSCIC) to determine the scope of the breach and restoration measures.
- Disclose the breach to those whose private information was, or is reasonably believed to have been, acquired by a person without valid authorization.
- Inform the college president.
- Report any unusual or serious cyber security incidents to SUNY System Administration Chief Information Security Officer (CISO).
- Contact the college's breach insurance carrier.

Such notification may be done in writing, by electronic notice (provided there was a previous express consent to this method) and a log of electronic notice must be maintained, by telephone with a log to record the call.

Notification will be provided in the most expedient manner, without reasonable delay, but only after necessary measures are taken to determine the scope of the breach and restore integrity to the system. Notification will be delayed if law enforcement determines it will impede a criminal investigation.

Notification will include contact information for the college and a description of the categories of information that were or are reasonably believed to have been acquired including specification of elements

of acquired information. The NYS Attorney General, NYS Consumer Protection Board, and the NYS-CSCIC will be notified. The required form for such notification is included within this procedure.

3.5 Information Systems. Information systems include network and software design, and information processing, storage, transmission, retrieval, and disposal.

3.5.1 Paper Storage System. Access to rooms, offices and file cabinets where paper records are kept is controlled as follows:

- Doors to office areas are locked during non-business hours;
- Areas where customer information is processed are locked when left unattended;
- Visitors are escorted in areas where customer information is processed;
- Visitors are restricted to areas that do not have customer information in plain view;
- File cabinets used to store customer information are located in locked areas, where such areas cannot be locked the file cabinets are locked when left unattended;
- Documents no longer needed are shredded.
- Storage and work areas are protected and secured, only those employees having the need to work in these areas are given keys to those areas.

3.5.2 Computer Information Systems. The Executive Director of Technology, Director of ITS, and Director of MIS, provide the function of electronic information security. The following information security policies and practices that protect against threats to the security and integrity of electronic customer information and guard against the unauthorized use of such information apply:

- A registry of all computers attached to the college network is maintained;
- A registry of employees with access to covered data is maintained;
- Physical security plans for servers and terminals are maintained;
- Social security numbers are not the unique identifier used for customers;
- Employees who cease employment with the college will no longer have access to files and programs that contain protected customer information.

3.5.3 Customer Information Disposal

- Supervisors within each department/office are responsible for the confidential disposal of day-to-day documents. The confidential disposal of college-wide stored records is coordinated by the Vice President of Administration or the Director of Administrative Services.
- Obsolete confidential documents are set aside for shredding in secure areas and marked confidential before being transferred to the shredding center.
- The college erases or destroys all data when disposing of computers, copiers, CDs, magnetic tapes, hard drives or any other electronic storage devices that contain customer information.
- The college disposes of obsolete customer information in accordance with applicable records retention policies.

4.0 Definitions

4.1 Covered data and information – for the purposes of this policy includes student and other customer financial information required to be protected under the GLB and NYSISBNA, and FTC Red Flag Rules. Covered data and information includes both paper and electronic/magnetic records.

4.2 Private Information – is unencrypted personal information plus one (1) or more: social security number, driver's license number or non-driver ID, account number, credit or debit card # plus security code, access code or password which permits access to an individual's financial account.

4.3 Customer financial information – is that information the college has obtained from a student or other customer in the process of offering a financial product or service, or such information provided to the college by another financial institution. Offering a financial product or service includes offering student loans to students, receiving income tax information from a student's parent when offering a financial aid package and other miscellaneous financial services as defined in 12 CFR § 225.28. Examples of customer financial information include addresses, phone numbers, bank and credit card account numbers, income and credit histories and social security numbers, in both paper and electronic format.

5.0 References

5.1 Gramm-Leach-Bliley Act of 1999, NYS Information

- https://www.ftc.gov/tips-advice/business-center/guidance/how-comply-privacy-consumer-financial-information-rule-gramm

5.2 Security Breach and Notification Act 2005

- https://www.congress.gov/congressional-report/111th-congress/senate-report/290/1?s=1&r=42
- https://ag.ny.gov/new-york-state-information-security-breach-and-notification-act

5.3 Federal Trade Commission Red Flags Rule

- https://www.ftc.gov/tips-advice/business-center/privacy-and-security/red-flags-rule