Policy: **Security of IT Systems and Data** Policy Number: **J-9**
Responsible for Policy: Information Technology Most recent approval date: Fall 2017

Policy Statement
Finger Lakes Community College will provide resources, policies and procedures necessary to the maintenance of the security of information stored and utilized on its computer systems and networks in accordance with federal, state and local laws and consistent with SUNY security guidelines. Measures taken to protect IT Systems and Data will be based on recognized best-practices and will include data access control managed by independent Data Stewards, an active user re-certification effort, and enforced standards for user passwords.

Reason for Policy
To establish formal compliance with the SUNY Information Security Guidelines and relevant federal regulations.

Applicability of the Policy
FLCC Information Technology resources and all users of those resources.

Definitions
Information Technology Division
The Division of Information Technology (IT) consists of those staff members under the supervision of the Chief Information Officer.

Users
The term user for the purpose of this policy refers to all students, faculty, staff, retirees and visitors and volunteers who are authorized by Finger Lakes Community College to access and utilize its IT resources.

Data Stewards
For those college computer systems on which sensitive information is stored, one or more data stewards will be identified by the respective division head or in the absence of designation by the division head, the Chief Information Officer. Typically, the data stewards are the heads of offices responsible for creating and maintaining the data on the respective computer system.

IT Security Incident
Any event involving Finger Lakes Community College computer systems and/or communications networks that is suspected or determined to a) violate applicable state or federal law or regulation; b) be harmful to the security or privacy of Finger Lakes Community College computer systems, communications networks, Finger Lakes Community College information, or the general public; c) be otherwise harmful to Finger Lakes Community College computer systems and/or communications networks; or d) cause unexpected disruption to Finger Lakes Community College computer systems and/or communications networks.

Critical Incident
Some incidents will rise to the "critical" level, due to their impact on the campus. Any IT security incident that impacts regulated data (e.g., student information, personal health information, SSN's) sensitive Finger Lakes Community College data (as defined below), or which otherwise meets the standards as a reportable cyber incident under SUNY's required Cyber Incident Reporting Guidelines will be regarded as "Critical."

Related Documents
- SUNY Cyber Incident Reporting Policy
- Family Educational Rights & Privacy Act (FERPA)
- Health Insurance Portability and Accountability Act of 1996 (HIPAA)
- Graham-Leach-Bliley Act
- Sarbanes Oxley Act

- Freedom of Information Act
- Colleague Administrative Information System Policy
- Network Usage Policy

Review date/action taken:

- March 2011: original approval
- Fall 2012: no policy revisions
- Fall 2014: non-substantive revisions
- April 2016: no policy revisions
- Fall 2017: no revisions

Procedures: **Security of IT Systems and Data** Procedure Number: **J-9**
Responsible for Procedure: Information Technology Most recent effective date: Fall 2017

Procedures

IT Division Responsibilities

The Information Technology division is responsible for the maintenance of the security of the data residing on its systems and transmitted across its networks. This effort will involve the maintenance of appropriate physical and environmental security of systems, data storage and network resources. It also includes provisions for the security of information through the appropriate use of authenticated logins, passwords, and layered protection from viruses and external intrusion. This effort additionally involves the creation, publication and implementation of an integrated system of policies governing the use of the institution's IT resources.

The division's staff, as determined by the Chief Information Officer (CIO), will have access to facilities, systems, software and data to ensure the viable and secure operation of the College's IT systems, networks and other resources. The CIO may also approve cooperative system and network support arrangements with external organizations or other internal college divisions, and will be responsible for defining appropriate levels of data, software and system access in those cases.

The IT division in addition is responsible for taking a lead role in the handling of IT-related security incidents as identified below in the "Procedure for IT Security Incidents."

Data Steward Responsibility

Access to sensitive information is a necessity for many College business operations, and Federal regulations allow for the provision of access to this information for those users who have a legitimate "need to know." The data stewards serve the function of determining access to sensitive information on a need to know basis. The data stewards are responsible for defining the level and extent of access for individual users for the sensitive data under their stewardship.

The data stewards also work in conjunction with IT staff and users to develop effective means of utilizing the information under their purview while preserving the security of the data. Whenever possible, the data stewards and IT staff will provide methods for utilizing aggregate information devoid of individual identifiers. Where sensitive information is to be accessed and distributed, the data steward and IT staff are responsible to ensure that access is provided to only those users with a definable need to know.

User Responsibility

All authorized users are responsible for knowing and adhering to the policies and procedures identified in this and all IT policies, which are relevant to the IT resources they utilize (e.g. Employee Desktop Policy, E-mail Use Policy, Network Use Policy, etc.). All users are responsible for exercising good judgment in the use of Finger Lakes Community College's computer systems and communications networks. They are responsible for maintaining the security of their individual accounts through proper password protection, and the privacy and security of any sensitive data they have access to. In handling sensitive information, users are required to follow the prescribed procedures defined by IT and the relevant data steward for their permitted forms of data access, and are not allowed to circumvent intended data security practices. In working with sensitive individual information Users are responsible for removing individual identifiers whenever the resulting information will satisfy the particular business need.

Password Parameters and Access Rights Procedure

IT will enforce passwords with a minimum length of 8 characters, complexity enabled, expiration of no more than 180 days, previous password history limited, and lockout duration of 30 minutes following successive failed attempts.

Access rights for new requests will be processed through the relevant data stewards or shared drive owners in all cases. Recertification of access rights for all users will be conducted annually. The Human Resources Office will notify the

Information Technology department area immediately when employee leaves, retires, or is otherwise ended as an employee in the HR system and/or changes jobs/roles or department at FLCC.

For cases where employment has ended, IT will disable the appropriate accounts. For other changes, the IT area will verify any new access to be granted as well as which prior access should be revoked through the respective data stewards.

Classification of Information

A number of federal, state, and local laws (e.g. FERPA, HIPAA, Graham-Leach-Bliley, Sarbanes Oxley, FOIL, ESRA, etc.) have required that personal information (such as academic records, finance, health etc.) be treated in a secure and confidential manner. Finger Lakes Community College defines sensitive information per the State University of New York's definition declaration of sensitive information under the category of "Confidentiality." A link to SUNY's definition of sensitive information can be found below. Examples of sensitive information include but not are limited to the following:

- Social security numbers (as well as national identification numbers for foreign nationals)
- Financial/banking account numbers, credit or debit card numbers
- Government issued identification card numbers
- Financial records & tax documents (for students, or their family who submit them for financial aid purposes).
- Education records: including transcripts, grade information, payment/tuition records, records pertaining to academic Student judicial/disciplinary information
- Patient health records
- Maiden name (or parent's surname prior to marriage)
- Biometric records (such as fingerprints)
- Passwords (including a person's own password)
- Personally Identifiable Information (PII) - Information that alone or in conjunction with other information identifies an individual

Information which resides on the institution's IT systems, and which is not covered by the above classification may be regarded as sensitive at the discretion of the division head overseeing the office responsible for its creation.

SUNY's definition declaration of sensitive information (section I. Confidentiality, sub items I.A., I.B., and I.C. only): https://www.suny.edu/sunypp/docs/587.pdf

Non-sensitive information consists of the following: public directory (name, title, work phone, e-mail address); information covered explicitly by the Freedom of Information Act, and aggregate information on individuals that precludes personal identification.

Procedure for IT Security Incidents

IT Security Incident Response

IT security incident response procedures are intended to protect the Finger Lakes Community College computer systems and communications networks, including information resources, from future unauthorized access, use or damage, and to mitigate the impact of the IT security incident. These procedures will also be followed in connection with academic, disciplinary or administrative inquiries.

IT Security Incident Response Team

The IT department, in consultation with the college administration, will be responsible for coordinating the handling of all IT Security Incidents, and any related duties, such as alerting the campus to reportable attacks or intrusions (as defined by the SUNY Cyber Incident Reporting Policy). The response to IT security incidents will involve both technical and management personnel that are properly positioned to represent key IT and business interests. Oversight of the response to IT security incidents will be the responsibility of the Chief Information Officer.

Internal Reporting and Detection of IT Security Incidents

Any member of the Finger Lakes Community College campus community may request investigation of a suspected IT security incident from the IT department. The IT department itself might detect IT security incidents. IT will take appropriate steps to track, investigate, and resolve reported or detected IT security incidents and report the outcome to the appropriate parties. Critical IT security incidents must be immediately reported to the IT department Help Desk. Departments and individuals are encouraged to report all IT security incidents to help improve the tracking of trends and threats.

Assessment and Escalation

Finger Lakes Community College has the authority to access, inspect, and disclose the contents of any College equipment, files or email on its systems. Access to files on College owned equipment will only be approved by specific personnel when there is a valid reason to access those files. If it is necessary to access User files, authority must be obtained from the Chief Information Officer and the Vice President to whom the User reports (or the President if the subject of investigation is a Vice President). Finger Lakes Community College legal counsel will be consulted if deemed necessary.

IT Authority and Actions

For critical IT security incidents, IT management will have authority to involve legal entities, to disconnect or shut down part or all of the campus IT infrastructure, and to direct other campus IT personnel to take specific actions. For non-critical IT security incidents, IT may disconnect individual systems, as needed, but will work with User areas to balance disruptions against the security risks.

Reporting, Documentation, and Communication

IT will maintain records of all reported or detected IT security incidents and will follow SUNY Cyber Incident Reporting Policy guidelines in communicating important security information to the campus community and SUNY System Administration.

Forms/Online Procedures

- None

Appendix

- None

Review date/action taken:

- March 2011: original effective date
- Fall 2012: no revisions
- Fall 2014: no revisions
- April 2016: revisions to procedures (approved by College President)
- Fall 2017: no revisions