Fashion Institute of Technology
State University of New York

Information Security

Policy IT002
Volume 10, Information Technology
Responsible Administrator: Vice President for Information Technology and CIO
Responsible Office: Information Security Office
Issued: November 2017
Last Updated: January 2023

Policy Statement

FIT is committed to protecting its information and systems assets, as well as the professional and personal information of students and employees. FIT ("college") also has an ethical responsibility to its community members to protect their original research and designs, health and personal data, and other critical institutional information, the loss and damage of which could result in serious financial or reputational loss to the college. As a result, FIT will have several policies that govern the classification, technical protection, information security awareness, and procedural protection of its information assets and systems. This policy documents Information Technology controls governing all forms of college data, as well as technical and procedural steps that must be followed by all members of the FIT community relative to configuration and use of FIT hardware, software, and networks, as well as guidelines for the protection of data.

Reason for the Policy

As an institution of higher education operating in New York State, FIT must comply with federal and state confidentiality and information safeguarding laws, as well as meet data protection requirements imposed by its accrediting agency, the Middle States Commission on Higher Education (MSCHE). FIT also has legal obligations under such regulations as the Family Educational Rights and Privacy Act (FERPA), a federal law that protects the privacy of student education records and applies to all institutions that receive funds under any program administered by the Department of Education, as well as other laws, including various contracts to protect student and employee information.

Who is Responsible for this Policy

- Chief Information Security Officer (CISO)

Who is Affected by this Policy

- All members of the FIT community (students, employees, and third-parties)
- All other individuals and entities granted use of FIT information, including but not limited to: contractors, temporary employees, volunteers, etc.

Definitions

- **Authentication**: A security method used to verify the identity of a User.

- **Authorization:** The lawful and business-appropriate permission and access rights granted to a User of FIT IT Systems.

- **Breach**: means the unauthorized acquisition, access, use, alteration, destruction, or disclosure of Private Information which compromises the security or privacy of such information. For purposes of this definition, any acquisition, access, use or disclosure of Private Information in a manner not permitted under applicable international, federal, state, and local privacy laws and regulations shall be presumed to be a Breach, unless further investigation of the incident by the college shows otherwise.

- **Critical Breach** means a Breach involving significant risk of, or actual, exposure, dissemination, and/or misuse of Private Information as assessed by the Breach Response Team, taking into account factors including, but not limited to, the nature of the data breached (e.g. involving sensitive personally identifiable information), type of breach (e.g. intentional hacking with malicious intent or accidental exposure to unauthorized employees), the volume of breached data, how long the data was exposed, what other controls were in place to limit exposure (e.g. encryption), whether those controls were breached, and the likelihood of misuse of the breached data.

- **Data Custodians**: college personnel having direct operational-level responsibility for the management of one or more types of institutional data.

- **Data Owners**: Vice Presidents or their designees who have planning and policy-level responsibility for data within their functional areas and management responsibility for defined segments of institutional data.

- **Generic Accounts:** accounts that are used as a resource or that perform a service (for example, department@fitnyc.edu).

- **Information System(s):** The system(s) under the direct control of the college used to create, store, receive and transmit information, including but not limited to the hardware, software, networks, servers, information, data, applications, and communications that are part of the system(s).

- **Multi-Factor Authentication:** layered authentication method that required the user to provide two or more verification factors to gain access to a resource or online account.

- **Named Accounts:** accounts that follow a standardized naming convention of a user's first name, last name, unless there are multiple users with the same name (in which case a number shall be appended to the end of the named account in the order in which they are provisioned onto the FIT domain).

- **Private Information**: includes all college data, whether held by the college or a third party on behalf of the college, not identified as Public Information. This includes, but is not limited to, data protected by state and federal regulations, FERPA-protected student records, Personally Identifiable Information (e.g., bank account number, credit card number, debit card number, social security number, state-issued driver license number, and state-issued non-driver identification number) that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual. It also includes health-related information or any other information that is confidential to the college and is not intended for public disclosure. Private Information must be protected to ensure that they are not disclosed as governed or dictated in laws that restrict the disclosure of such data, and must be protected from disclosure under the New York State Freedom of Information Law (FOIL) as appropriate. Generally, FOIL excludes data that if disclosed would constitute an unwarranted invasion of personal privacy, as that term is defined by FOIL. Any breach of Private Information will be considered an Information Breach as described below, and will be governed subject to the college's incident response policies and procedures, plus any applicable disclosure requirements and the college's obligations to data subjects.

- **Public Information**: includes all college data not identified as Private, and the data is intended for public disclosure, or the loss of confidentiality of the data or system would have no adverse impact on our mission, safety, finances, reputation, privacy, and confidentiality. Public Information includes any data that is releasable in accordance with FOIL. This category also includes general access data, such as that available on unauthenticated portions of on FIT's website. Public Information has no requirements for confidentiality; however systems housing the data should take reasonable measures to protect the information from unauthorized changes.

- **Unauthorized Access**: Looking up, reviewing, copying, modifying, deleting, analyzing, or handling information without proper authorization and/or legitimate business need.

- **User:** Any individual, authorized or not, using any FIT IT System from any location.

Principles

- **Policy Governance**
  - **Applicability**
    All access to and use of the college's network, infrastructure, or information is governed by this policy. This policy also addresses the use of any information generated, accessed, modified, transmitted, stored, or otherwise used by the FIT community on the college's information resources and network infrastructure.

  - **Exceptions**
    - In certain limited cases, compliance with specific policy requirements may not be immediately possible or practical. Reasons include, but are not limited to, the following:
      - Required commercial or other software in use is not currently able to support the required features.

      - Legacy systems are in use which do not comply, but near-term future systems will, and are planned for;
      - Costs for reasonable compliance are disproportionate relative to the potential damage.
    - In such cases, exceptions to the policy must be documented and approved by: the CISO, the Chief Information Officer, and the divisional vice president in charge or the requesting department.
    - Exceptions must be re-authorized annually.
    - The request for exception must include:
      - The reason for the exception;
      - The reason that the system in question can't comply with the policy;
      - The risk posed by the non-compliance;
      - Any compensating controls being implemented to reduce the risk; and
      - Duration of the exception and the timeline for the system to become compliant with the policy.
    - Periodically a list of exceptions must be presented to the President's cabinet for review.

- **Awareness and Training**
  - FIT must ensure that users of organizational information systems are made aware of the Information Security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of organizational information systems. FIT must provide appropriate Information Security training to all members of the college community that is appropriate to the role of the recipient.
  - All members of the FIT community must apply the Information Security knowledge and training provided in the execution of their role at FIT.

- **Data Classification**
  - It is essential that all college data be protected. There are however, gradations that require different levels of security for Private and Public Information.
  - Data, including electronic and physical records, will be classified and handled according to SUNY standards, unless a Federal regulation supersedes.
  - All college electronic data will be reviewed on a periodic basis and classified according to its use, sensitivity, and importance to FIT. Data owners are responsible for establishing the appropriate review basis for their data.

- **Audit and Accountability**
  - All systems, applications, and network infrastructure devices must log all transactions and administrative access needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity. For clarity, this policy is aimed at Information System devices such as servers, routers, and firewalls, and is not meant to include devices such as televisions that, although they are attached to FIT's network, do not perform Information Technology functions.
  - Unless otherwise specified, systems must log in accordance with New York State Information Technology Standard NYS-S14-005.
  - Logs must be retained for six months or as required by regulation governing the data being logged, whichever is longer.

- **Physical Protection**
    - Designated secure areas such as data centers, distribution closets, and areas where restricted physical documents are stored must be locked at all times. Entrance to such areas much be logged either in a log book or using the logging capabilities of an electronic lock system. Where practical, video surveillance must also be used to record entry and exit. Videos must be retained for a minimum of 30 days. Per FIT's records retention schedule videos containing incidents warranting retention for administrative or potential legal uses must be retained for three years. Guests must be escorted by authorized personnel.
    - Private Information must be stored securely. All members of the college community must exercise care to keep such information out of public view and locked away.

- **System and Communication Protection**
    - All FIT information systems, whether developed in-house or by a third party, must undergo a security architecture review. Additionally and based on risk, the review may include a code review, penetration test, or other methods to ensure that the system adheres to best security practices.
    - All boundaries where the FIT network meets public networks must be protected by a firewall or similar device, that limits traffic to only the minimum sources, destinations, and protocols required to conduct FIT's mission. Boundaries must also be monitored by an Intrusion Prevention System (IPS) or similar technology.
    - Public-facing applications such as web services must be in a separate logical network area such as a demilitarized zone (DMZ).
    - System administrators must execute administrative functions using identities and passwords separate from the ones they use for daily business. Administrative accounts must not have access to email. Administrators must use reasonable precautions to access the public Internet to download vendor patches, security upgrades, bug fixes, and similar required files.
    - All Private Information must be encrypted in transit.

- **System and Information Integrity**
    - Vendor-provided security updates and patches to FIT systems must be applied in a timely manner, based on risk as determined by the Common Vulnerability Scoring System (CVSS) rating. The Chief Information Officer can require more expedited application of a specific patch based on risk to FIT.

- **Access Control**
    - Data access controls will be established by the college to allow the appropriate authorized access to college data, based on its classification.
    - Where possible and financially feasible, more than one person must have full rights to any college-owned server storing or transmitting Private Information. The college will establish guidelines that apply to user access rights in collaboration with data owners or custodians.
    - Access to FIT data is provided to college employees, consultants, third parties, etc., to conduct college business. Private Information, as defined by this policy, will be made available to people who have a legitimate need as approved through the documented access control process by the data owner.

  - Users must not share usernames and passwords, nor should they be recorded in unencrypted electronic files or documents. If passwords are written down they must be treated and secured as Private Information. All users must secure their username, password, and system access from unauthorized use. (See Acceptable Use for FIT IT Systems policy, Related Policies section below, for more details)
  - While not encouraged, FIT understands there are times when users may download third party applications. Users should be mindful that third party applications be obtained from a verified source such as dedicated app stores that have policies, procedures, and safeguards in place. Information Technology reserves the right to revoke permissions of third party applications if it is determined to be an information security risk.
  - It is the responsibility of supervisors to inform data owners of any changes within their areas (i.e., changes in job responsibilities, transfers, and terminations) requiring a change in access to data by their employees.
  - Periodic user access reviews will be conducted by data owners of Private Information to adjust access as needed for employees whose status has changed (i.e., termination or separation from the college, change in responsibilities, department, or other change where the user no longer is required to access the data to perform their job responsibilities or functions).

- **Configuration Management**
  - There must be a baseline configuration standard for each Information Technology device type in the FIT environment. Standards must be based on a national standard such as NIST or Center for Internet Security, as modified by the FIT Technical and Security teams. Standards must be documented and reviewed at least annually.
  - Nonessential programs, functions, ports, protocols, and services must be disabled or de-installed. Apply deny-by-exception (blacklist) policy to prevent the use of unauthorized software or deny all, permit-by-exception (whitelisting) policy to allow the execution of authorized software.
  - All hardware and software being run on FIT's Information Technology environment must be supported by the vendor (i.e., the vendor is actively monitoring for security flaws and releasing remediative patches as needed). Hardware and software that is running beyond its support life will be documented per the exception process.
  - Change management protocols must be followed to ensure that only authorized changes are made in production. Such changes must be documented.

- **Breach Reporting and Breach Response Team**
  - **Reporting:**
    - College Employees, and Students, or third parties who hold private information on behalf of the college, must immediately report all suspected Breaches of unsecured Private Information.
      - Suspected Breaches of electronic information should be immediately reported to the IT Department, and/or to the CISO, and to the Employee's Vice President.
      - Suspected Breaches of physical information should be immediately reported to the Records Management Officer (RMO), and to the Employee's Vice President.

            - Students may report directly to either the CISO or RMO and may also report to the Dean of Students; the Dean of Students will notify the appropriate officer.
            - Any verbal reports shall be documented by the person who receives the report, and submitted to the CISO or RMO as appropriate, or by the CISO or RMO, if the verbal report is made to directly to the CISO or RMO.

    - **Breach Response Team:**
        - The CISO shall lead the efforts of the Breach Response Team to mitigate Critical Breaches of electronic information. In the event of a Breach involving physical information, the RMO shall lead the Team's response.
        - The Breach Response Team shall also include the following individuals: Vice President for Finance and Administration, the General Counsel, the Vice President for Communications and External Relations, the Vice President for Enrollment Management and Student Success, and the Vice President for Human Resources, or their designees.
        - The Breach Response Team shall develop criteria for categorizing Breaches as Critical Breach based on circumstances of the Breach.
            - The Breach Response Team shall assume responsibility for overseeing the response to any Breach confirmed as a Critical Breach.

    The college will implement steps as quickly as practicable to mitigate, to the extent practicable, any harmful effect from any Breach of unsecured Private Information or other violation of Privacy or Security policies or procedures. Response to Critical Breaches of Private Information, including but not limited to notification of affected parties, and implementation of corrective actions, will follow protocol set forth in FIT's Breach Response Plan and ensure adherence to all federal, state, local, and/or international laws and regulations that may be applicable given a Breach of Private Information. Private Information

- **Maintenance**
    - The college will develop effective controls on the tools, techniques, mechanisms, and personnel used to conduct security patches and updates.
    - FIT may contract for system and network local or remote maintenance or support. Information Technology will provide oversight of the contractor during the time they have access to college resources. Representatives of these contracted companies must follow all FIT policies.

- **Security Assessment**
    - Periodic reviews of security controls in organizational information systems and networks will be conducted to determine if the controls are effective in their application.
    - The college will develop and implement plans of action designated to correct deficiencies and reduce or eliminate vulnerabilities identified in institutional information systems.

- **Identification and Authentication**
    - Authentication will be used for all systems and devices that send or receive Private Information or when it is critical that both parties know with whom they are communicating. Multi-factor authentication (at least 2-step verification) will be used for all named email accounts. The CISO's office may approve, in advance, exception requests (i.e. generic accounts) based on balancing the benefit versus the risk to the college. Authentication may be required for changing Public Information based on the sensitivity of the data. Access to the network and servers and systems must be achieved by individual and unique logins and require authentication. Authentication includes the use of passwords, smart cards, biometrics, or other recognized forms of authentication, and must be risk-based.

- **Media Protection**
    - FIT non-Public Information will be physically controlled and securely stored regardless of the media used (both paper and digital).
    - Access, regardless of the media used, will be limited to authorized users.
    - college data will be discarded in a manner consistent with the information's classification level, type, and FIT's Records Retention and Disposition policy. This includes information contained in any hard copy document, or in any electronic, magnetic or optical storage medium (including, but not limited to a memory stick, CD, hard disk, magnetic tape, disk, etc.).

Responsibilities

- **FIT Community**
  All members of the FIT community share responsibility for protecting information resources to which they have access, or are custodians. Individual users are responsible for ensuring that others do not use their system privileges (see Acceptable Use for FIT IT Systems policy for more information). Appropriate Information Security practices and procedures, as described in this policy and as published in trainings and other materials provided by the Division of Information Technology, should always be followed, including the proper disposal of records (see Records Retention and Disposition policy). Anyone whose failure to follow this policy results in unauthorized access, disclosure, alteration, or destruction of college data and/or systems, may be subject to appropriate disciplinary action[1].

  Further, it is the responsibility of all members of the FIT community to report all suspected Breaches of Private Information to the appropriate party as dictated by this policy (see Breach Reporting section).

- **System Administrators**
  System administrators are authorized to create or alter system accounts and services. Responsibilities include:

[1] If employees are tenured and/or have a Certificate of Continuous Employment (CCE), the disciplinary process will comply with section 28.28.0 of the Collective Bargaining Agreement. For employees not in the collective bargaining unit, the Vice President for Human Resource Management and Labor Relations or their designee(s) will review the violation and may make a recommendation to the President to take such administrative action, including, but not limited to disciplinary action such as dismissal, demotion, reassignment, suspension, reprimand, removal of privileges, or training.

    - Performing administration duties such as configuration, log management, and account provisioning in accordance with this policy.
    - Maintaining their own credentials and practices in accordance with the system administrative requirements of this policy.
    - Enable multi-factor authentication (at least 2-step verification) on all administrative accounts that have privileged authorization over college data.

- **College Administrators**
  All senior-level administrators are responsible for ensuring compliance with this policy. Responsibilities include:
    - Communicating this policy to their division and encouraging completion of relevant training; and
    - Ensuring the implementation of this Information Security policy and related procedures within their division.
    - Chief Information Security Officer (CISO)

  The CISO is responsible for:
    - Directing and coordinating the college-wide Information Technology Security Program;
    - Providing a focal point for oversight of Breaches, in coordination with the Breach Response Team, and the Records Management Officer, if applicable;
    - Establishing security metrics, tracking the progress of the Information Technology Security Program, and providing a college-wide risk profile; and
    - Assisting divisions in fulfilling their Information Security requirements.

Procedures

Appropriate Information Security practices and procedures will be developed in accordance with this policy and communicated to the FIT community accordingly.

Violations

N/A

Related Policies

- Acceptable Use for FIT IT Systems
- Information Security
- FERPA
- Records Retention and Disposition

Related Documents

- Information Security Policy Exception Documentation
- FIT Breach Response Plan
- New York State Freedom of Information Law (FOIL)
- SUNY Information Security Guidelines: Campus Programs and Preserving Confidentiality
- SUNY Information Security Policy

Contacts

- **Chief Information Security Officer (CISO)**
  Information Technology
  (212) 217-3415