SOUTHWESTERN ILLINOIS COLLEGE
DISTRICT 522

BOARD POLICY

TITLE:	**Information Technology Security**
CODE:	**6011**
DATE ADOPTED:	**Oct 1991**
DATE REVIEWED:	**01/08; 10/10; 01/23; 07/23; 08/23**
DATE AMENDED:	**02/08; 11/10; 03/23; 09/23**

1. Purpose

Southwestern Illinois College (SWIC) is responsible for managing and securing the information it stores, processes, and transmits, in support of its business functions in accordance with state and federal laws and regulations. All data and systems are to be secured in an appropriate manner and used for only authorized purposes. The information contained or collected are not intended to be used for personal gain or for non-academic business. The use of these resources is monitored to identify unauthorized use. Data may only be disclosed to the extent and in the manner authorized. Unauthorized access, disclosure, modification, use, or destruction of data is prohibited. This policy with corresponding administrative procedures establishes the actions to be taken to identify, manage, and respond to suspected or confirmed breaches (e.g., Personally Identifiable Information (PII)). This policy ensures that responses to breaches will be consistent, comprehensive, complete, and delivered in an effective and timely manner in order to minimize the risk to the college and stakeholders.

2. Accountability

Under the direction of the President, the Chief Information Officer and the Information Security Manager shall implement and ensure compliance with this policy.

3. Applicability

This policy applies to all SWIC employees, organizational units and organizations conducting business for and on behalf of the college through contractual relationships when interacting or using SWIC information technology (IT) resources (e.g., network services, applications, databases, etc.) This policy does not supersede any other applicable College Board policy, laws or higher level agency directive. College officials shall apply this policy to employees, contracted agencies, contracted individuals, vendors, and other non-college employees (e.g., POI's, interns, etc.) All organizations and agencies collecting or maintaining information, using or operating information systems on behalf of the college, or are integrated into college on premise applications and databases, are also subject to the stipulations of this policy (e.g., cloud and managed services). The content of and compliance with this policy shall be incorporated into applicable contract language or memoranda of agreement under separate cover (e.g., grants and outside consultants, vendor contracts, etc.)

4. Definitions

Administrative Safeguards – administrative actions, policies and procedures to manage the

selection, development, implementation, and maintenance of security measures to protect the

College’s information assets and to manage the conduct of the college community in relation to

the protection of those information assets.

Breach – The compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or loss of control of college managed or contracted services of information systems and data. Any similar term referring to situations in which unauthorized persons, or authorized persons with unauthorized privileges, gain access or potential access to either physical or electronic data.

Data Collector - any person (e.g., Records Officer, Data Steward, etc.), organizational unit of the college or contractor (e.g., agency, vendor, or individual) that, for any purpose, handles, collects, disseminates, or otherwise deals with non-public personal information.

Security – the expectation that only authorized individuals, processes, and systems will have access to SWIC’s data.

Integrity – the expectation that SWIC’s data will be protected from improper, unauthorized, destructive, or accidental changes.

Physical Safeguards – physical measures and procedures to protect the college’s data assets from natural and environmental hazards and unauthorized intrusion.

Risk – The level of impact on college operations (including mission, functions, image, or reputation), college assets, or individuals resulting from the operation of an information system, given the potential impact of a threat and the likelihood of that threat occurring.

Risk Assessment – The process of identifying risks to college operations (including mission, functions, image, or reputation), college assets, or individuals resulting from the operation of an information system. Part of risk management and synonymous with risk analysis, risk assessment incorporates threat and vulnerability analyses and considers mitigations provided by established or planned security controls.

Technical Safeguards – the technology, policy and procedures for its use that protect the College’s data and controls access to it.
SWIC Community – faculty, staff, POI non-employees, students, contractors, and vendorsof SWIC.

User – Any person, whether authorized or not, who makes any use of or interfaces with any SWIC IT resource, system or service from any location.

"Personal Identification Information (PII)" means either of the following:
An individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted or redacted or are encrypted or redacted but the keys to unencrypt or unredact or otherwise read the name or data elements have been acquired without authorization through the breach of security:

- Social Security number.
- Driver's license number or State identification card number.
- Account number or credit or debit card number, or an account number or credit
- card number in combination with any required security code, access code, or
- password that would permit access to an individual's financial account.
- Medical information.
- Health insurance information.
- Unique biometric data generated from measurements or technical analysis of
- human body characteristics used by the owner or licensee to authenticate an
- individual, such as a fingerprint, retina or iris image, or other unique physical
- representation or digital representation of biometric data.

User name or email address, in combination with a password or security question and answer that would permit access to an online account, when either the user name or email address or password or security question and answer are not encrypted or redacted or are encrypted or redacted but the keys to unencrypt or un-redact or otherwise read the data elements have been obtained through the breach of security.

"Personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

Note: Source: (815 ILCS § 530/) Personal Information Protection Act; effective. 1-1-17

Policy Statement

The SWIC Community is responsible for the security of the information that the public has entrusted to it, including PII that can be used to distinguish or trace an individual's identity such as a name or social security number. SWIC must, therefore, mitigate the risks associated with the inadvertent loss or unapproved disclosure of PII.

The granting and revoking of access to data and systems is to be made on a valid need-to-know basis. Authorization for access is to be based on the least-privilege (minimum necessary) principle. Decisions regarding the granting and revoking of access to data and systems are the responsibility of the authorized administrator.

Any unauthorized use, disclosure, or loss of such information can result in the loss of the public's trust and confidence in the college's ability to properly protect it. Some information or data types may require additional protection due to its sensitivity and the risks of misuse associated with a potential unauthorized disclosure (e.g., PII, HIPPA, FERPA, etc.) Data breaches may have far-reaching implications for individuals whose information is compromised, including identity theft resulting in financial loss and/or personal hardship experienced by the individual. A data breach may also require significant staff, time, assets, and financial resources to mitigate the negative consequences, which may prevent the college from allocating those resources elsewhere.

6011AP Security Policy Administrative Procedure ensures that responses to PII data breaches are consistent, comprehensive, complete, and delivered in an effective and timely manner in order to minimize the risk to the college and individuals.

Gramm-Leach Bliley Act (GLBA) requires financial institutions to provide particular notices and to comply with limitations on disclosure of nonpublic personal information (NPI). The College's policy is to only disclose necessary information to affiliated third parties that will either provide direct instruction, financial, or support services to our students, donors, and employees.