Shepherd University
Board of Governors
Policy 35

TITLE: INFORMATION TECHNOLOGY SECURITY

SECTION 1. GENERAL

1.1 SCOPE: This policy applies to all Shepherd University faculty, staff, students, affiliates, and contractors who have access to University information and to systems that store, access, or process the information.

1.2 AUTHORITY: West Virginia Code §18B-1-6

1.3 EFFECTIVE DATE: February 11, 2010

SECTION 2. DEFINITIONS

2.1 Words not defined in this section have their usual and common meanings.

2.2 Authentication credentials: A set of unique tokens issued to a person and used to verify that person's identity to an information system. An example would be a username and password. Another example would be a username and a scanned fingerprint.

2.3 Information Security Administrator: A person designated to oversee information security practices and procedures.

2.4 Affiliate: As used in this policy, affiliates of Shepherd University are people who use Shepherd computing resources but who are not contractors, students, or paid employees. Examples include interns, volunteers, or Shepherd University Foundation employees.

2.5 Password: A character string, usually eight or more characters, known only to an individual and used to prove that person's identity to a computer system during the authentication process.

2.6 Authorization: The process of determining the access an individual is permitted to have to an information resource.

2.7 Personally Identifiable Information (PII): Information that can be used to uniquely identify an individual, such as a Social Security Number, or a name in conjunction with the date of birth. In most cases this does not include information that is considered directory information according to the Federal Educational Rights and Privacy Act of 1974.

2.8 Information resources: All data, equipment, and software used to process or store information.

2.9 Standard cryptographic techniques: Technology commonly used in the computing industry to encrypt data sent from one information system to another in order to prevent unauthorized access to the data by a third party. The technology may change from time to time as weaker techniques become more easily broken (rendering the technique ineffective) and stronger techniques become more prevalent.

2.10 Access controls: The enforcement of a set of authorization rules governing a person's ability to locate, read, alter, create, or delete information stored in a computer system.

2.11 Username: A character string associated with a unique individual, and used during the authentication process to assert the individual's identity. The username is generally commonly known and generated from the individual's name.

SECTION 3. INFORMATION SECURITY PRINCIPLES

3.1 Background: Shepherd University's information resources are vital academic and administrative assets that require appropriate safeguards. Paper-based systems, computer systems, networks, and data are vulnerable to a variety of threats that have the potential to compromise the integrity, availability, and confidentiality of the information. Effective information security programs must be used to eliminate or reduce the risks posed by potential threats to the university's information resources. Measures must be taken to protect these resources against unauthorized access, disclosure, modification or destruction. Much of the guidelines in information security best practices are incorporated into the State of West Virginia Office of Technology Information Security Policy (WVOT-PO1001, issued January 18, 2007). This Shepherd University policy makes references to the Governor's Office of Technology policy, and all references to it herein shall include any amendments or successor policies thereof. All university employees are expected to comply with WVOT-PO1001.

3.2 Applicable State And Federal Law; Applicable Industry Regulation: All Shepherd University personnel covered by this policy shall comply with applicable laws and regulations. Those include but are not limited to United States Code Title 18, § 1030 (the Computer Fraud and Abuse Act of 1986), Title 20, § 1232g (the Federal Educational Rights and Privacy Act of 1974, FERPA), the Higher Education Opportunity Act of 2008, the West Virginia data breach notification act (SB 340 of 2008, codified as WVC § 46A-2A-101 through 105), the Health Insurance Portability and Accountability Act of 1996 (HIPAA), and the Payment Card Industry (PCI) data security standard, for those systems containing credit card information.

3.3 Appropriate Measures: The University shall implement all necessary access controls, personnel practices, and administration to comply with information security best practices and applicable laws.

SECTION 4. ACCESS CONTROLS

4.1 Authorization: Access to information resources (paper-based or electronic) is available only for authorized, job-related purposes. Access to personally identifiable information (PII) shall be allocated only when determined to be necessary for the work duties of the personnel.

4.2 Authentication: All personnel accessing information resources shall be authenticated before access is granted. In the case of electronic records, the individual shall have a unique set of authentication credentials (for example, a username and password). It is the policy of the University that personnel shall not share authentication credentials. Appropriate access controls shall be set in place to protect the confidentiality of any authentication credentials used to access information systems. Such controls may take the form of a minimum cryptographic strength for passwords, a set time for the expiry of passwords, or the imposition of stronger controls in certain extremely sensitive environments.

4.3 Physical Security: Physical records containing PII shall be locked up when unattended or not in use (e.g. in a records vault). Computer systems containing PII shall be similarly inaccessible. For example, computers that store the information must be in a secured and locked facility.

4.4 Data Security: Electronic records containing PII should be stored on centralized data servers whenever feasible. This can include databases or file servers. Computers used to access electronic records containing PII shall be locked against unauthorized use when unattended (for example, employing a screen saver with a password lock). The storage of PII on mobile computing devices, such as laptops or "smart" phones, is strongly discouraged. If such data must be stored on these devices, the use of data encryption to encode PII is strongly encouraged, to ensure its integrity in the event of theft of the physical device.

4.5 Data Transmission: All PII transmitted into or out of the Shepherd University information systems shall, to the largest extent feasible, employ standard cryptographic techniques to prevent unauthorized access to the PII. The Information Security Administrator is responsible for determining what standard cryptographic techniques are acceptable.

SECTION 5. PERSONNEL PRACTICES

5.1 Training: All personnel who access applicable information resources shall receive adequate training in appropriate information security practices. The Information Security Administrator may update training standards as needed for regulatory compliance. Initial training should cover the basic concepts under section 3 (authentication, authorization, physical and data security, and data transmission). Refresher training shall be offered periodically and required at the discretion of the Information Security Administrator.

5.2 Acceptable Usage Agreement: All personnel who access applicable information resources must accept the Shepherd University acceptable usage agreement. This agreement states that the employee has read, understands, and will comply with the information security policy and related guidelines and procedures, and that information resources will be used in accordance with established policies and guidelines. This also applies to vendors and contractors, per Section 1.0 of WVOT-PO1001. The acceptable usage agreement may be altered as required to maintain compliance with applicable laws and future revisions to WVOT-PO1001.

5.3 Accountability: All personnel using applicable information resources shall be considered responsible for activities performed using the unique authentication credentials (for example, username and password) assigned to them.

SECTION 6. ADMINISTRATION

6.1 Ownership: All information resources, including computer equipment purchased by Shepherd University, software installed on computer equipment, and data resident on computing systems and networks, are owned by Shepherd University, with the exception of assets governed by a contractual agreement (for example, licenses to operate vendor-owned software) or the intellectual property of Shepherd faculty, students, and staff (where applicable).

6.2 Responsibility: The President may appoint designees to implement this policy or serve as the Information Security Administrator for purposes of Section 5.1.1 of WVOT-PO1001. Such designees shall be responsible for creating, disseminating, and enforcing guidelines necessary for implementation of this policy.

6.3 Discipline: Employees who violate this Information Security Policy may be subject to disciplinary action. Appropriate actions may include information security awareness training, removal of access, reassignment, or dismissal. All disciplinary actions will be consistent with established policies concerning employment.