WEST VIRGINIA STATE UNIVERSITY BOARD OF GOVERNORS

West Virginia State University

BOG Policy #52

Title: Information Technology (IT) Security Policy

Section 1. General

1.1 Purpose: This policy establishes guidelines and responsibilities for West Virginia State University (WVSU)employees regarding information security and the protection of West Virginia State University information resources. This information is based on the State of West Virginia Information Security Guidelines.

1.2 Scope: This policy applies to all WVSU employees who have access to WVSU information and to systems that store, access, or process the information.

1.3 Effective Date: 12/31/2002

2.0 Policy

2.1 Administration

2.1.1 An ISO (Information Security Officer) role must be assigned. This individual must perform or delegate the necessary functions and responsibilities of the position;

2.1.2 All information resources, regardless of medium, will be used, maintained, disclosed, and disposed of according to law, regulation, or policy;

2.1.3 All employees and others who access computer systems should be provided with sufficient training in policies and procedures, including security requirements, correct use of information resources, and other organizational controls;

2.1.4 A risk analysis program will be implemented and a risk analysis will be conducted periodically;

2.1.5 A cost effective incident response recovery plan will be maintained providing for prompt and effective continuation of critical missions in the event of a security or other incident that impacts West Virginia State information resources;

2.1.5.1 Procedures, guidelines, and mechanisms that are utilized during a security incident, along with the roles and responsibilities of the incident management teams, must be established and reviewed regularly.

2.2 Access Controls

2.2.1 Access controls must be consistent with all state, federal, and local laws and statutes and will be implemented in accordance with this policy;

2.2.2 Procedures must be implemented to protect information resources from accidental, inadvertent, unauthorized, or malicious disclosure, modification, or destruction;
2.2.3 Appropriate controls must be established and maintained to protect the confidentiality of passwords used for authentication;
2.2.4 Individual users must have unique userids and passwords;
2.2.5 All employees must be accountable for their computer and for any actions that can be identified to have originated from it;
2.2.6 When employees are transferred or their employment is terminated, user ids and authorizations should be disabled immediately;
2.2.7 Confidential or sensitive data (i.e., credit card numbers, calling card numbers, log on passwords, etc.) must be encrypted before being transmitted through the Internet;
2.2.8 The network access control devices and mechanisms must be appropriately configured to control all incoming services in a manner consistent with the mission of West Virginia State and sufficient protection of West Virginia State information assets;
2.2.9 Data and supporting software necessary for the continuation of West Virginia State functions will be periodically backed up;
2.2.10 All information assets must be accounted for and will have an assigned owner;
2.2.10.1 Owners, custodians, and users of information resources must be identified;
2.2.10.2 All access to computing resources will be granted on a need-to-use basis;
2.2.11 Each owner or custodian of information will determine its classification based on the circumstances and the nature of the information;
2.2.12 The owner or custodian will determine the protective guidelines that apply for each level of information. They include the following:
Access
Distribution within West Virginia State University
Distribution outside West Virginia State University
Electronic distribution
Disposal/Destruction
2.2.13 All programmable computing devices must be equipped with up-to-date virus protection software, if available;
2.2.13.1 Virus protection procedures will be developed to address system protection.

2.3 Personnel Practices
2.3.1 All IT assets, including hardware, software, and data are owned by West Virginia State unless excepted by contractual agreement, or federal law or regulation;
2.3.2 Information resources are designated for authorized purposes only. West Virginia State reserves the right to monitor and review employee use as required for legal, audit, or legitimate authorized West Virginia State operational or management purposes;

2.3.3 Employees must receive an appropriate background check when their position is determined by the Information Security Officer, or the President of West Virginia State University, or the President's designees, to be a critical position with respect to IT assets;
2.3.4 Procedures must be established to ensure that all WVSU employees have read, understand, and will abide by West Virginia State University policies and procedures regarding IT security;
2.3.5 All vendors and contractors must sign and abide by a contract/confidentiality statement to ensure compliance with state and West Virginia State University information security policies and procedures;
2.3.6 All employees must abide by any rules regarding acceptable and unacceptable uses of IT resources.

2.4 Physical and Environmental Security

2.4.1 Information resource facilities will be physically secured by measures appropriate to their critical importance;
2.4.2 Security vulnerabilities will be determined and controls will be established to detect and respond to threats to facilities and physical resources;
2.4.3 Critical or sensitive data handled outside of secure areas will receive the level of protection necessary to ensure integrity and confidentiality;
2.4.4 Equipment will be secured and protected from physical and environmental damage;
2.4.5 Equipment used outside West Virginia State University premises will be given the appropriate degree of security protection and will be equivalent to that of on-site information resource equipment used in a similar manner.

3.0 ENFORCEMENT

3.1 Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

4.0 DEFINITIONS

Access - to approach or use an information resource.

Access Control - the enforcement of specified authorization rules based on positive identification of users and the systems or data they are permitted to access.

Authentication - the process of verifying the identity of a user.

Chief Information Officer - the person responsible for West Virginia State University's information resources.

Custodian of Information - the person or unit assigned to supply services associated with the data.

Employee - Individuals employed on a temporary or permanent basis by WVSU as well as contractors, contractors' employees, volunteers, and individuals that are determined by West Virginia State University to be subject to this policy.

Encryption - process of encoding electronic data that makes it unintelligible to anyone except the intended recipient.

Firewall - specialized computers and programs residing in a virtual area between an organization's network and outside networks which are designed to check the origin and type of incoming data in order to control access and block suspicious behavior or high-risk activity.

Information Assets - Any of the data, hardware, software, network, documentation, and personnel used to manage and process information.

Information Security - those measures, procedures, and controls that provide an acceptable degree of safety for information resources, protecting them from accidental or intentional disclosure, modification, or destruction.

Information Security Officer (ISO) - the person designated by the WVSU President, or his/her designee, to administer West Virginia State University's information security program. The ISO is West Virginia State University's internal and external point of contact for all information security matters.

Owner of Information - the person(s) ultimately responsible for an application and its data viability.

Password - a string of characters known to a computer system or network and to a user who must enter the password in order to gain access to an information resource.

Risk Analysis - the evaluation of system assets and their vulnerabilities to threats in order to identify what safeguards are needed.

Security Incident - an event that results in unauthorized access, loss, disclosure, modification, or destruction of information resources, whether deliberate or accidental.

Threat - includes any person, condition or circumstance that endangers the security of information, or information systems, in the context of Information Security.

User of Information - a person authorized to access an information resource.