Westfield State University
Policy concerning

APPROVED: April 2015 REVIEWED: August 2024

INFORMATION SECURITY PASSPHRASES

PURPOSE

The purpose of this policy is to establish a standardized, system-wide approach to managing the protection of information and Information Technology Resources to support core business needs and the provision of continuity and privacy at Westfield State University ("University") and establish sanctions for violations of this policy. This policy is intended to protect the users of the University's Information Technology Resources by ensuring a reliable and secure technology environment that supports the educational mission of the University. These resources are provided as a privilege to all Westfield State University employees, students, and authorized guests. The University seeks to ensure the integrity of Information Technology Resources made available to the user community, as such, to ensure these resources are secure from unauthorized access for those that utilize them. This policy is not intended to inhibit the culture of intellectual inquiry, discourse, academic freedom or pedagogy. In general, the same ethical conduct that applies to the use of all University resources and facilities applies to the use of the University's Information Technology Resources.

SCOPE

This policy applies to all students, faculty, staff, volunteers, vendors, consultants, contractors, or others (herein afterwards referred to as "constituents") who use or have authorized access to University Information Technology Resources. This policy is supplemented by the policies of those networks to which the University is interconnected, including, but not limited to, the University of Massachusetts Information Technology Systems group, the Commonwealth of Massachusetts' Information Technology Division, UMass Online, etc. It covers all University information whether in hardcopy or electronic form and any systems which access, process, or have custody of business data. This policy also applies to any and all information, in any form and in any medium, network, internet, intranet, computing environments, as well as the creation, communication, distribution, storage and disposal of information.

For the purposes of this policy, "Information Technology Resources" means all computer, applications and communication facilities, services, data and equipment that are owned, managed, maintained, leased or otherwise provided by the University and the Office of Information and Instructional Technology (OIT) Area Security Officials (ASO) shall be the supervisor of each department or program with the authority to grant access to Information Technology Resources.

The use of the University's Information Technology Resources constitutes an

understanding of, and agreement to abide by this policy. Additionally, all constituents must protect, and if necessary, intervene to assure that others protect the confidentiality, integrity, and security of all Information Technology Resources.

USER OWNERSHIP AND RESPONSIBILITIES

It is the responsibility of any person using the University's Information Technology Resources to read, understand, and follow this policy. In addition, all users are expected to exercise reasonable judgment in interpreting this policy and in making decisions about the use of Information Technology Resources. Any person with questions regarding the application or meaning of this policy should seek clarification from his or her supervisor or from the Information Security Officer. The University owns and maintains the information stored in its Information Technology Resources and limits access to its Information Technology Resources to authorized users. Users of Information Technology Resources have a responsibility to properly use and protect these resources, respect the rights of other users, and behave in a manner consistent with any local, state, federal laws, and regulations, as well as all University policies, procedures, and guidelines. Information Technology Resources, including Internet bandwidth, are shared among the community and users must utilize these resources with this understanding.

Users must respect all intellectual property rights, including any licensing agreements applicable to information and resources made available by the University to its community.

Information Technology Resources are provided to support the mission of teaching and learning and to conduct official University business. Therefore, the University bears no responsibility for the loss of any personal data or files stored or located on any system.

POLICY

All constituents are responsible for taking the appropriate steps to select and secure their passwords in compliance with the Information Security Policy, the OIT Access Control Guidelines and the OIT Password Creation, Protection and Administration Guidelines. Passwords are an important aspect of information security. A poorly chosen password may result in unauthorized access and/or exploitation of Information Technology Resources.

Westfield State University

Policy concerning

APPROVED: April 2015 REVIEWED: August 2024

PROCEDURE

All passwords must conform to the OIT Password Creation, Protection and Administration Guidelines and the OIT Access Control Guidelines, including but not limited to:

- Establishing a standardized passphrase creation guideline
- Utilizing different passphrase for various access needs
- Establishing an automated, time-based passphrase change requirement
- Educate all constituents on how to protect their passphrases.
- Establishing a guideline for changing forgotten or lost passphrases
- Establishing procedures for the authorization and termination of access to Information Technology Resources

REVIEW

This policy will be reviewed annually by the Chief Information Security Officer.

Frameworks

Name	Reference
NIST	AC-4 Information Flow Enforcement AC-11 Session Lock AC-18 Wireless Access AC-19 Access Control for Mobile Devices AU-8 Time Stamps CM-1 Configuration Management Policy and Procedures CM-2 Baseline Configuration CM-6 Configuration Settings CM-7 Least Functionality CM-9 Configuration Management Plan SA-10 Developer Configuration Management SC-10 Network Disconnect SC-15 Collaborative Computing Devices

Regulations and Requirements

Name	Reference
PCI DSS 4.0	Requirement 8

Supporting Standards and Procedures