Westfield State University
Policy concerning

APPROVED: October 2014

REVIEWED: August 2024

INFORMATION SECURITY

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. Area Security Officials 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.

Westfield State University

Policy concerning

APPROVED: October 2014 REVIEWED: August 2024

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, and 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

Westfield State University's Information Security Officer will establish security program that will be based upon the best practices recommended in the SANS Critical Security Controls for Effective Cyber Defense - Version 5. The components defined by these System Administration Networking and Security Institutes (SANS) Critical Security Controls are a subset of the National Institute of Standards and Technology (NIST) SP 800-53, prioritizing the controls that will provide a measurable security program, appropriately adopted to meet the specific needs of Westfield State University. This program will also incorporate applicable regulations and laws, such as, but not limited to, the Gramm-Leach-Billey Act (GLBA), the Health Insurance Portability and Accountability Act (HIPPA), Family Educational Rights and Privacy Act (FERPA), and the Commonwealth of Massachusetts Information Technology Department (ITD) and Office of Consumer Affairs and Business Regulations. Additional organizations, such as EDUCAUSE and the International Organization for Standardization and the International Electrotechnical Commission (ISO/IEC 27005:2011) will be utilized as resources for additional security practices.

PROCEDURES

The SANS Critical Controls for Effective Cyber Defense – Version 5 and other noted sources in the above policy statement will be utilized to guide, develop, and enhance any additional Information Technology policies, procedures and guidelines as needed to address the security needs of Westfield State University.

REVIEW

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

Frameworks

Name	Reference
NIST	AC-1 Access Control Policy and Procedures AC-2 Account Management AC-3 Access Enforcement AC-8 System Use Notification AC-14 Permitted Actions Without Identification or Authentication AC-16 Security Attributes AC-19 Access Control for Mobile Devices AC-21 Information Sharing AC-22 Publicly Accessible Content MP-3 Media Marking RA-2 Security Categorization AU-9 Protection of Audit Information CM-5 Access Restrictions for Change IA-1 Identification and Authentication Policy and Procedures IA-2 Identification and Authentication (Organizational Users) IA-4 Identifier Management IA-5 Authenticator Management PE-2 Physical Access Authorizations PE-3 Physical Access Control PS-1 Personnel Security Policy and Procedures PS-4 Personnel Termination PS-5 Personnel Transfer

Regulations and Requirements

Name	Reference
PCI DSS 4.0	Requirement 9 Requirement 12

Supporting Standards and Procedures