University of New Haven

Policies and Procedures

Policy Title: Office of Information Technology Security Statement

Policy No.: 7000 Rev.: 0
Effective Date: October 8, 2019
Last Revision: October 8, 2019

Responsible Office: Office of Information Technology
Responsible Official: Associate Vice President for Technology & CIO

Contents

Scope 1
Policy Statement 1
Reason for the Policy 2
Definitions 2
Policy Sections 3

Scope

The goals of this policy are to define the University of New Haven's statement addressing Information Security.

Policy Statement

The University of New Haven has developed information security policies to protect the availability, integrity, and confidentiality of University's information technology (IT) resources. While these policies apply to all faculty, staff, and students of the University, they are primarily applicable to Data Stewards, those that manage access to data and IT resources, and those who use University IT resources. The University expects all faculty, staff, and students to adhere to the policies herein. No set of policies can address all scenarios of IT security; therefore, these policies address the most common aspects of security. We cannot eliminate malicious behavior or irresponsibility, but we can guide users and administrators toward responsible decisions and actions.

The Office of Information Technology (OIT) manages the University's information security activities and works in cooperation with University staff whose responsibilities address information technology and information security of supported systems and applications.

In order to protect resources from threats and ensure compliance with applicable laws and industry standards, the University will manage and regulate networks and other IT resources. The University's IT resources, whether owned or contracted, will be configured to meet the requirements set forth in these policies. Agreements that involve a third party accessing or managing the University's IT resources shall comply with all of the requirements specified in these policies.

IT resources must be protected from activities that could compromise the confidentiality, integrity, or availability of the resources. Owners shall perform regular and timely computer maintenance, which includes, but is not limited to, installation of software patches, and updates to malware and virus protection. The automatic implementation of patches and updates at regular intervals will be utilized for all capable devices. Owners of IT resources should be aware of the business and availability requirements for their systems, and owners shall create appropriate documentation and processes to meet the requirements outlined in these policies.

For purposes of protecting the University's network and information technology resources, the OIT may temporarily remove or block any system, device, or person from the University network that is reasonably suspected of violating University information security policies. These non-punitive measures will be taken only to maintain business continuity and information security, and users of the University's information technology resources will be contacted for resolution

Reason for the Policy

The University must ensure that IT resources are protected from malicious activity that could compromise the University network and digital assets and identity.

Definitions

Confidentiality
The protection of IT assets and networks from unauthorized users

Integrity
Ensuring that the modification if IT assets are handled in a specific and authorized manner

Availability
Ensuring continuous access to IT assets and networks by authorized users.

Policy Sections

The details of each policy can be found in the following documents;

Acceptable Usage – Policy No. 7001
Password – Policy No. 7005
Email Usage and Retention – Policy No. 7010
Third Party Access – Policy No. 7015
Wireless Security Access – Policy No. 7020
Record Retention – Policy No. 7025
Asset Protection – Policy No. 7030
Firewall Policy – Policy No. 7040
Computer System Support – Policy No. 7050
Copyrights and License Agreements – Policy No. 7060
Social Networking Guidelines – Policy No. 7080
Hardware and Software – Policy No. 7200
Software Installation for Classrooms and Labs – Policy No. 7800
Cellular Policy – Policy No. 7900