University of New Haven

POLICIES AND PROCEDURES

Policy Title: Office of Information Technology Eligibility for Network System Access

Policy No.: 7002 **Rev.:** N/A
Effective Date: October 1, 2019
Last Revision: N/A

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

Introduction 1

Policy Sections 2
7002.1 Eligibility and Deactivation for Accounts 2
7002.2 Network 3
7002.3 Policy Compliance 4
7002.4 Process 4

- **Introduction:**

Scope

This policy applies to all University of New Haven employees, students, emeritus, retirees, alumnus, affiliates, contractors and guests with an expressed need to connect to the University of New Haven network and other secure technology resources. This policy applies to affiliates and contractors accessing the network to do work on behalf of University of New Haven, including reading or sending email and viewing intranet web resources.

Policy Statement

University of New Haven network access accounts (Username) are provided with the assumption that use of them will be consistent with, and will not interfere with, the main purposes of the University. All account owners must agree to abide by, in writing, the Acceptable Usage Policy.

7002.1 Eligibility and Deactivation for Accounts

1.1 Students: All active students, including Special Day, transfer, exchange students and USCGA Cadets, will receive an account on "payment of deposit" with intent to attend the University. Students "studying away," SATA and "on leave" will continue to have active accounts.

Deactivation: Students who are "inactivated" by the Registrar or withdraw permanently from the University will have their account deactivated thirty (30) days after the end of their last semester.

1.2 **Faculty:** All faculty, including visiting, continuing part-time, head coaches and adjunct faculty, are given accounts up to thirty days prior to the start of the semester following the completion of Human Resource required paperwork. Adjunct faculty will remain active between semesters.

Deactivation: Faculty, including adjunct, who leave the University will retain network, Banner self-service, Intranet, Moodle and email access for twelve (12) months following their job record "termination date." Dean of Faculty Office will notify AVP Enterprise and Technical Systems of terminating adjuncts by June 30th each year.

1.3 Staff: All staff (full-time, part-time, on-call, temporary, seasonal) are given account access up to thirty (30) days prior to the start of employment or following the completion of their employment paperwork, whichever is later.

Deactivation: Accounts of staff who voluntarily leave the University are deactivated thirty (30) days after their "termination effective date." Deceased and involuntary terminations will have all access removed immediately following notification from Human Resources.

1.4 Alumni: Network accounts of graduating students are transitioned into Alumni accounts within two weeks of graduation. Therefore they no longer have student access to the University Network. If they are working for the University they transition to a staff or affiliate role. Their email accounts will be transitioned to 'alumni email' accounts sometime during the year following graduation. Graduates email account addresses do not change. Alumni are encouraged to use the alumni portal iModules for access to their email account. They continue to have access to Banner self-service but not printing or Moodle.

1.5 Retired Staff & Emeriti Faculty: Emeritus faculty and retired staff retain their accounts with basic network account, gmail access, Banner self-service and access to online journals and databases. Emeritus faculty and retired staff **do not** have access to printing or Blackboard

Deactivation: Deceased Emeriti and retired staff accounts will be removed immediately upon notification.

1.6 University Affiliate: University Affiliates (e.g., contractors, contract temporary staff, interns) may have a legitimate need for secure network access and authentication to basic system resources such as e-mail and Intranet. An example of a "contract temporary staff" is someone under contract with Kelly Services or Manpower where they are employees of the Contractor, not University of New Haven. In accordance with the *Contractor Screening Policy*, the Contract Manager shall submit the approved contract to the Information Security Office. The Contract Manager is responsible for establishing the identity of the individual for whom the access is being requested. The Contract Manager is responsible for ensuring the account is used in ways that are consistent with the main purposes of the University and do not interfere with the work of other members of the University community.

Affiliates **do not** automatically receive Banner self-service, print, Banner INB or Moodle access. University Affiliate accounts will be activated in four business days following the request and expire in six months unless their Contract Manager makes other arrangements in advance. University Affiliate account access must be requested through the WebHelp Desk system. Access to systems in addition to the basic access (e.g., Banner self-service, print, Intranet, Moodle) should be requested in the WHD ticket. The Affiliate must sign the Administrative Systems Confidentiality Agreement. The University Information Security Office in collaboration with the appropriate Data Steward(s) may approve special requests, based on the benefit to the University of providing an account.

1.7 Campus Guests: Guests are provided unsecure network access. Guests who stay in University residence halls during the summer may also access the Internet through an unsecured wireless connection in the residence hall rooms. Non-University sponsored summer programs and visitors to the University may use the Internet via unsecured wireless access throughout campus. The Guest wireless is accessible after required registration using a valid email account. The University assumes no liability for the guest use of these open-unsecured access points.

1.8 Guests from eduroam Participating Institutions: University of New Haven provides secure **eduroam** access service to students, faculty, researchers and staff from other **eduroam** participating institutions.

7002.2 Network

The University's wired and wireless networks are for the use of University of New Haven students, faculty, and staff. However, with Information Security Office permission and Contract Manager sponsorship, affiliates who are working for the University may be granted secure access to the Internet via the University network. The University does provide restricted guest access to

the University network upon registration.

7002.3 Policy Compliance

7.1 Compliance Measurement
The Information Security Office will verify compliance to this policy through various methods, including but not limited to periodic walk-thrus, application tools reports, internal and external audits, and feedback.

7.2 Exceptions
There may be situations not covered here in which someone has a legitimate need for an account at University of New Haven. The Information Security Office may approve special requests based on the benefit to the University of providing an account. Exceptions should be requested in a WHD ticket

7.3 Non-Compliance
Use of an account in ways that are not consistent with the main purposes of the University, or that interfere with the work of other members of the University community, may be revoked, following the usual disciplinary processes of the University for students, faculty, and staff. For all others, the Associate Vice President for Technology & CIO may revoke accounts for those who are neither employed nor enrolled in the University.

7.4 Related Policies

- Third Party Access Policy
- Confidentiality Agreement

7002.4 Process

University Affiliate/Contractor Secure Access:
Requests for University affiliate access to the secure network and Internet should be forwarded to the Information Security Office via WebHelpDesk ticket to include Contractor's full name, along with the Contract Manager requesting the account, Contractors' ID Number, the start and expiration dates for the account, and the Contract Manager on campus who will be responsible for supervising the account.

Reason for the Policy

The purpose of this policy is to define eligibility standards for network system access and authorization for access to basic system resources which include University of New Haven's email, shared file server space, secure and unsecure networks. All employees and students are provided Banner self-service (SSB) access, intranet, print access, and other systems as necessary. These eligibility standards are designed to minimize the potential exposure to University of New

Haven from damages which may result from unauthorized use of University of New Haven resources. Damages may include the loss of sensitive or University confidential data, loss of intellectual property, damage to the University's reputation, harm to critical University of New Haven internal systems, etc. Access to the administrative systems (e.g., Banner Internet Native (INB), Blackboard, WebFocus) should be requested through the Help Desk system.

Definitions

"Secure Network" uses encryption to secure the wireless network from intruders. There are two main types of encryption available for this purpose: Wi-Fi Protected Access (WPA) or Wi-Fi Protected Access 2 (WPA2). Your computer, router, and other equipment must use the same encryption.

"Unsecure Network" A wireless network is "unsecured" if you can access the internet using the network without entering a password or network key. For example, a "hotspot" is a wireless network that is open and available for the public to use.

"University Affiliate" or "Contractor" is someone officially attached or connected to the University who is not a student or employee (e.g., contractors, vendors, interns, temporary staffing, volunteers.)

"University Contract Manager" is an employee of the University who provides funding, management and connection to an Affiliate doing work on behalf of University of New Haven. The Contract Manager bears responsibility for the Affiliate should they misuse their access.
"Guests" are participants in University conferences, non-University sponsored summer programs, and visitors to the University (i.e., parents, alumni, and speakers).

"Basic account and system access" allows access to the University network, email, Banner self-service (SSB), and other systems.
"Administrative systems access" allows access to the University administrative network, and University business related systems. This level of access requires signature acceptance of the Confidentiality Agreement. Administrative systems include Banner, Blackboard and WebFocus.

"eduroam" (**edu**cation **roam**ing) is the secure, world-wide roaming access service developed for the international research and education community. Eduroam allows students, researchers and staff from participating institutions to obtain Internet connectivity across campus and when visiting other participating institutions. See https://www.eduroam.us/ for more information.