University of New Haven

POLICIES AND PROCEDURES

Policy Title: Office of Information Technology Security Awareness Training

Policy No.: Rev.: 7004. 0
Effective Date: September 4, 2019
Last Revision: September 4, 2019

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

Contents

Scope

This policy applies to all University of New Haven employees, faculty and staff and identified University affiliates.

Policy Statement

Educating users and administrators at all levels on the safe and responsible use and handling of information is necessary. It is the obligation of University of New Haven faculty and staff to protect University-owned and personal computers containing University electronic information and records. University records exist for the purpose of the business of the University. To facilitate appropriate information security practices the Information Security Office requires specific training based on the classification level of data you have access to.

Full-time staff and faculty are required to attend security awareness training upon employment with the University. The staff or faculty member has 60 days to complete the training program, or they will be deemed non-compliant with this policy. Staff with access to PII, as well as data stewards, and functional leads must take security awareness training on a yearly basis. All temporary employees who have access to PII information must undergo security awareness training before they can access the University records.

Staff or faculty employees who have not completed the security awareness training will be limited to Banner Self Service on the Banner administrative system.

The security awareness training program is subject to yearly review and enhancement based on changes to the information security environment.

Reason for the Policy

The purpose of this policy is to ensure that all University of New Haven employees and University affiliates with access to University data, are taught Information Security Awareness in order to gain an understanding of the importance of securing the University's data. The University seeks to establish a culture that ensures that institutional data is secure. This policy and associated procedures establish the minimum requirements for the Security Awareness and Training controls.

Definitions

"**Security Awareness Training**" is a formal process for educating employees about the internet and computer **security**. A good **security awareness** program should educate employees about institutional policies and procedures for working with information technology (IT).

"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.)

"**Personally Identifiable Information (PII)**" is any data that could potentially identify a specific individual. Any **information** that can be used to distinguish one person from another and can be used for de-anonymizing anonymous data can be considered **PII**.

"**education records**" under FERPA, which - with limited exceptions - means all records in any format or medium that are directly related to a student and are maintained by the University;

"The Family Educational Rights and Privacy Act (FERPA)" is a Federal law that protects the privacy of student education records.

"**Health Insurance Portability and Accountability Act (HIPAA)"** demands that all **HIPAA** covered businesses prevent unauthorized access to "Protected Health Information" or PHI. PHI includes patients' names, addresses, and all information pertaining to the patients' health and payment records.

"**Gramm-Leach-Bliley ACT (GLBA)**" Requires financial institutions – companies that offer consumers financial products or services like loans, financial or investment advice, or insurance – to explain their information-sharing practices to their customers and to safeguard sensitive data.

"**Data Owner**" - is a person responsible for the management and fitness of **data** elements (also known as critical **data** elements) - both the content and metadata.

"Functional Lead" Technical lead point person for a department. Responsibilities include coordination of upgrades, delegating access, and system issues. Acts as a liaison to IT.

Policy Sections

7.1 Compliance Measurement
The Information Security Office in conjunction with the IT Service Desk will verify compliance to this policy through various methods, including but not limited to application tools reports, internal and external audits, and feedback to the Information Security Office.

7.2 Exceptions
Staff members that do not have access to computers or access to PII data. Any other exceptions to this policy must be approved by the Office of Information Technology in advance or the CIO.

7.3 Non-Compliance
Staff and Faculty members that do not comply with this policy will have network access rights suspended until they comply with the policy.

7.4 Related Policies & Documents
Data Governance Policy
Data Classification Policy

7.5 Security Incident
University Affiliates and employees that incur security risk exposure (live or simulated) may be required to retake Security Awareness training.