Security Awareness Training

Objective
This guideline is in support of the WISP to ensure that all Suffolk University employees and Suffolk University members with access to University Information, are provided Information Security Awareness on the importance of securing the University Information and University Information Resources to establish a security culture that ensures all information used by it members is secure. This guideline and associated procedures establish the minimum requirements for the Security Awareness and Training controls.

Scope
Applies to all University staff, faculty, and students that handle University data as defined in the WISP Data Classification.

Definitions
“Security Awareness Training” is a formal process for educating employees about University information security policies, data security, data privacy, and the proper handling of data. See WISP and Data Classification.

Supplemental Guidance
Educating users and administrators at all levels on the safe and responsible use and handling of information is necessary. In direct support of the WISP, it is the obligation of Suffolk University faculty and staff to protect Suffolk University Information and University Information Resources, which includes all University data. To facilitate appropriate information security practices the Information Security Office requires security training that addresses general security awareness and the classification 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 until employee orientation to complete the training program, or they will be deemed non-compliant. Faculty and Staff with access to PII, as well as data stewards, and functional leads are recommended to 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 University PII data.

Staff or faculty employees who have not completed the security awareness training may have limited access to University Information Resources and University Information.

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

Training Compliance
The Information Security Office will review and measure 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.

Exceptions
Staff members that do not have access to computers or access to PII data. Any other exception must follow the terms of the WISP.

Non-Compliance
Staff and Faculty members that do not comply with WISP and required training may have network and or system access rights suspended, depending on the nature of the data they access.

Security Incident
Suffolk University employees that incur a security risk exposure, such as falling victim to a phishing attempt, may be required to retake Security Awareness training.

rev1.0
08/18/2020 ITS Information Security Officer