Procedure - System Acquisition, Deployment, Integration, and Maintenance

Purpose

The purpose of this procedure is to ensure that information security requirements are established across the lifecycle of licensed third-party information systems, which includes testing, implementation and updates of information systems.

Provisioning of Hardware and Software

IT must be consulted whenever deploying any new systems for adequate provisioning of system hardware and software. IT will obtain and install the equipment, as appropriate, and then allow access to the appropriate groups for use of the equipment. Provisioning of software requires purchasing of any applicable licenses for use.

Management of Network Storage

To allow adequate storage capability to support all users, IT will develop, implement, and review standards and processes for managing online and offline storage capacity. These standards will include types or classes of storage, data backup, protection by classification, and any quotas necessary based on the business reasons for storage. Management of storage will incorporate any requirements given in information retention policies.

System Acceptance

To ensure new systems or applications do not disrupt the network, existing applications, or other systems, IT will define a system acceptance process. This process will document acceptance criteria for new systems prior to acceptance. All systems will be tested prior to acceptance, including a vulnerability assessment or scan prior to being permitted to connect to the ESD network. This process will ensure that security controls are in place and that the new system complies with the design and function required.

Vulnerability Management

ESD IT will run ensure the following:

1. System or network devices are using current patch levels, not running unnecessary services, and do not have default passwords.
2. Internal vulnerability scans against any systems containing (or accessing systems that contain) confidential data at least on a quarterly basis.
3. Internet-facing systems and/or all public internet protocol address space are scanned by a trusted third party to run external vulnerability scans on at least a quarterly basis.

Timeline for Implementation of Procedure

Given the required changes to ESD processes to fully implement this procedure, new technology systems will be subject to this procedure immediately while existing processes or systems will be reviewed as required by the procedure’s periodic review. If an operating practice is needed from

IT as part of the procedure, IT will develop and have implemented that process before running proposed technology system through it. Procedure to be fully implemented by September 1, 2024.