Software Installation	**6-016** **TECHNOLOGY SERVICES** **June 2021**

OVERVIEW

1.01 Allowing employees to install unapproved software on OSUIT computing devices opens the university up to unnecessary exposure and liability. Conflicting file versions or DLLs which can prevent programs from running, the introduction of malware from infected installation software, unlicensed software which could be discovered during audit, and programs which can be used to hack the organization's network are examples of the problems that can be introduced when employees install software on company equipment.

PURPOSE

2.01 The purpose of this policy is to outline the requirements regarding installation of software on OSU Institute of Technology (OSUIT) computing devices. This control is in place to minimize the risks of the loss of program functionality, the exposure of sensitive information contained within OSUIT computing network, the introduction of malware, and legal exposure due to the use of unlicensed software.

SCOPE

3.01 This policy applies to all OSUIT employees, contractors, vendors, and agents with an OSUIT-owned mobile device, computer, server, smartphone, tablet, and other computing devices operating within OSUIT.

POLICY

4.01 Employees, with the exception of Technology Services staff, may not install software on OSUIT computing devices operated within the OSUIT network.

4.02 Software requests must first be approved by the requester's manager and then be made to the Service Desk in writing or via email.

4.03 Software must be selected from an approved software list, maintained by Technology Services, unless no selection on the list meets the requester's need.

4.04 Technology Services will obtain, track, and charge the requesting department for the licenses, test new software for conflict and compatibility, and perform the installation.

POLICY COMPLIANCE

5.1 Measurement: Technology Services will verify compliance to this policy through various methods, including but not limited to, periodic walk-throughs, video monitoring, business tool reports, and internal or external audits.

5.2 Exceptions: Any exception to the policy must be approved by the AVP of Technology Services in in writing in advance of installation.

Approved:
Policy and Procedures Committee, June 16, 2021
Effective date: June 16, 2021