Vulnerability Assessment	6-017 TECHNOLOGY SERVICES JUNE 2021

PURPOSE

1.01 The purpose of this policy is to authorize appropriate members of the Technology Services Infrastructure team and authorized external security auditors to conduct audits, including penetration tests and vulnerability assessments, against the OSU Institute of Technology's computing, networking, telephony, and information resources.

SCOPE

2.01 This policy applies to all university owned or controlled information technology resources whether individually controlled or shared, stand alone, or networked.

2.02 This policy applies to persons, whether students, staff, faculty, or authorized third-party users, within OSUIT departments and any other affiliated agencies, entities, groups or organizations which at any point, such as in business operations or administrative processes, control university-owned or university-leased information assets or technology resources.

2.03 This policy stipulates basic configurations of, and applies equally to, all information assets or systems used to access or protect access to those assets.

2.04 These audits may be conducted for purposes of:

- Investigating possible security incidents
- Assurance of the confidentiality, availability, and integrity of information systems
- Ensuring compliance with OSUIT policies and associated regulations such as PCI-DSS, HIPAA, GLBA, FERPA, GDPR, and others
- Verifying that information is only accessible by the stakeholders with authorized access
- Ensuring the availability of technology resources necessary to support OSUIT's mission, vision, and strategic plan
- Ensuring the prevention of modification of protected university data by unauthorized entities

POLICY

3.01 Members of the Technology Services Infrastructure Team and authorized external auditing entities approved by the Associate Vice President of Technology Services are authorized to access the OSUIT computing, networking, telephony, and information

resources and devices to the extent required to perform the scans permitted by this policy. This access may include:

- Access, user and system level, to any OSUIT computing, networking, telephony, and information resources and devices
- Access to university areas including labs, offices, cubicles, storage areas, etc.
- Access to information resources including electronic, hardcopy, etc.
- Access to interactively monitor and log OSUIT network traffic

3.02 Routine Vulnerability Scanning

The Technology Services Infrastructure Team will perform routine internal authenticated vulnerability scanning monthly. The Technology Services Infrastructure Team will utilize the results of these scans to evaluate the vulnerabilities and resulting risk to OSUIT to aid in mitigation strategies.

3.03 Service Interruption or Degradation

Performance of detective network scanning may adversely affect network and server performance. The scanning is intended to be a detective control that mitigates the greater risks and disruption that unmitigated vulnerabilities pose to the confidentiality, integrity, and availability of the OSUIT network resources.

3.04 PCI Requirements

The Technology Services Infrastructure Team will perform external and internal authenticated network vulnerability scans at least monthly and following any significant change to the OSUIT network. The vulnerabilities found using these scans will be mitigated. Although rogue access points are not allowed by OSUIT policy, OSUIT uses scanning at least monthly to assure that there are no rogue wireless networks available for connection. The Technology Services Infrastructure Team will maintain an up-to-date inventory of authorized wireless access points.

3.05 Vulnerability Risk Identification and Ranking

Routinely, the Technology Services Infrastructure Team will review vulnerabilities published by US-CERT and MITRE. Based on the MITRE CVE scores, each vulnerability will be scheduled for remediation response, scheduling, and documentation.

3.06 Penetration Testing

The Technology Services Infrastructure Team will engage an independent external auditor to run penetration testing annually on the PCI_DSS environment in addition to other rotated areas of focus. Penetration tests include network and application layer tests as well as segmentation testing.

3.07 Non-PCI-DSS Patching Schedule

Application of non-PCI patches are required following the patching schedule below. Any exploitable findings must be mitigated, and the vulnerability scan/penetration test repeated to ensure the control has been effectively applied. CVSS scores between 9.0-10.0 must be patched with 10 days. CVSS scores between 7.0-8.9 must be patches with 30 days. CVSS scores between 4.0-6.9 must be patched within 120 days.

3.08 PCI-DSS Patching Requirements

PCI-DSS requires installation of necessary critical vendor-supplied security patches during the first month after release. All other vendor-supplied patches must follow the non-PCI-DSS patching schedule. All patches considered critical by the Technology Services Infrastructure Team, regardless of CVSS score, must be patched as soon as it is practical.

3.09 Automated Monitoring and Alerting

OSUIT Technology Services uses intrusion detection and prevention systems (IDPS). All internal network traffic is monitored. The IDPS is configured to alert the Technology Services Infrastructure Team.

3.10 Exceptions

All exceptions to this policy will be handled according to existing Technology Services policies.

3.11 Emergencies

In the event of an incident emergency, actions may be taken by the Incident Response Team in accordance with the Incident Response Plan. To ensure the safety and confidentiality of university confidential information, these actions may include making systems inaccessible.

Approved:
Policy and Procedures Committee, 6/16/2021
Effective date: 6/16/2021