OSU INSTITUTE OF TECHNOLOGY
POLICY & PROCEDURES

Cyber Resilience	**6-003** **TECHNOLOGY SERVICES** **June 2021**

PURPOSE

1.01 This policy sets forth the intent, establishes the direction, and sets the expectations of behaviors regarding the cybersecurity/cyber resilience program at OSUIT. This policy is a living document and will be updated as changes occur in the cybersecurity threat landscape. OSUIT takes the security of our stakeholders and data very seriously. After having enumerated and evaluated OSUIT's assets, vulnerabilities, threats, and risk appetite, OSUIT understands that we must take specific and measurable cyber resilience actions. Failure to design a defense-in-depth strategy exposes all OSUIT stakeholders to unacceptable risks. This Cyber Resilience Policy and associated Technology Services policies, procedures, and processes are the means to minimize and mitigate these risks to the greatest extent possible relative to OSUIT's risk appetite.

1.02 OSUIT Technology Services has chosen applicable elements of several leading frameworks including NIST Cyber Security Framework (CSF), NIST Risk Management Framework (RMF), ITIL4, and COBIT 5 to provide the OSUIT community with a common language for understanding, managing, and expressing cyber resilience to both internal and external stakeholders. The CSF is focused on making sure that any cybersecurity measures taken are appropriate for the level of risk involved. The Risk Management Framework (RMF) provides a process that integrates security, privacy, and cyber supply chain risk management activities into the system development life cycle. The goal of ITIL is to improve efficiency and achieve predictable service delivery by standardization of the selection, planning, delivery, maintenance, and overall lifecycle of IT services. COBIT's guiding principles are meeting stakeholder needs, covering the enterprise end-to-end, applying a single integrated framework, enabling a holistic approach, and separating governance from management. Technology Services will operate using the continuous improvement cycle. The CSF promotes the alignment of policy, university business, and university technology based on existing best-practice standards, guidelines, and controls. The goal is to protect the confidentiality, integrity, and availability (CIA) of OSUIT's information resources. Toward this goal, appropriate controls from NIST SP800-171, ISO/IEC 27001 Annex A, and the Center for Internet Security Center for Internet Security (CIS) Security Controls for Effective Cyber Defense (SCS) will be used to mitigate cyber threats.

SCOPE

2.01 Policies governing our cyber resilience program apply to everyone with access to OSUIT information technology and/or data. Cyber resilience affects all stakeholders of OSUIT and is everyone's responsibility.

2.02 The CSF supporting this policy provides overarching guidance to OSUIT on how to identify, protect, detect, respond, and recover from any existing cyber resilience vulnerability or threat in the OSUIT data environment.

POLICY

3.01 OSUIT will identify all technology assets and vulnerabilities through asset inventories and vulnerability testing.

3.02 In accordance with Internet Standards Organization ISO/IEC 27001 Annex A – Reference control objectives and controls, regular, in-house and independent, authenticated vulnerability scans and penetration testing will be performed on OSUIT's applications and networks.

3.03 Processes will be in place to ensure regular vulnerability patch management in accordance with Technology Services departmental Patch Management Policy.

3.04 The Infrastructure Administrator shall perform a daily check of the Common Vulnerabilities and Exposures (CVE) website provided by MITRE and the U.S. National Vulnerability Database (NVD).

3.05 Annual authenticated external vulnerability and penetration testing scans must be performed.

3.06 Monthly external vulnerability and penetration testing scans must be performed.

3.07 Monthly authenticated internal vulnerability and penetration scans must be performed.

3.08 Protection will include deny-all-by-default posture firewalls inbound and outbound, malware detection software, remote access management, network segmentation, secure asset disposal, and other applicable controls. Exceptions to the deny all inbound and outbound default must be approved using the OSUIT and OSU system change management processes.

3.09 Login access to all university devices is authenticated by active directory either by individual user, departmental global security groups, or by other role-based global security groups based on committee, position, or department.

3.10 Multifactor authentication will be required for connection to servers processing regulated data.

3.11 Detection will include intrusion detection systems, event monitoring, and logging.

3.12 Our incident response plan will inform our response to a cyberattack.

3.13 The Backup and Restoration of University Owned Data policy will provide cyber resilience by allowing restoration of any compromised systems.

3.14 A Remote Access Policy shall be in place.

3.15 Cybersecurity policies, procedures, standards, and processes at the Technology Services departmental level shall be reviewed annually by Technology Services staff and approved by the Associate Vice President of Technology Services.

3.16 University level technology policies shall be approved as per OSUIT Policy and Procedure 1-023 by the OSUIT Policy and Procedures Committee.

3.17 A patching process shall be in place to track published patches and vulnerabilities. Patches must be approved and logged in OSUIT's Configuration Management Data Base (CMDB) and any applicable OSU System change management process prior to application with explicit consideration of the security impact the patches might have on university systems.

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