POLICY STATEMENT

This policy aims to establish controls and processes for the identification and management of technical vulnerabilities and their associated risks to University of Oklahoma Norman campus information assets owned by OU IT in order to avoid potential negative business impact.

PURPOSE OF POLICY

The University of Oklahoma must assess IT systems and software to determine potential security impacts due to flaws, weaknesses, or intentional malice to protect the confidentiality, integrity, and availability of OU systems and data.

WEB ADDRESS FOR THIS POLICY

This Policy:

SCOPE

ENTITIES/INDIVIDUALS AFFECTED BY THIS POLICY
Any person or entity within or affiliated with the University of Oklahoma Norman campus Information Technology department managing an IT System that processes, stores, transmits, and/or collects University data is responsible for complying with this policy.

RESOURCES AFFECTED BY THIS POLICY
This policy applies to all Information and/or Technology Resources that are owned by, or in custody of the University of Oklahoma Norman campus IT department.
POLICY

VULNERABILITY ASSESSMENT

Scanning Frequency
- Periodic or continuous vulnerability assessment scanning of all supporting assets in the University of Oklahoma Norman campus network that are owned by OU IT will be performed at least monthly.
- If scanning cannot be performed against a supporting asset in a non-destructive manner it may be temporarily exempted from vulnerability scanning. This does not exempt the supporting asset from other vulnerability assessment. All temporary exemptions must be approved via the information security risk acceptance process as approved by the OU Executive Director for IT Security.

Scanning Accuracy
- All supporting assets on a University of Oklahoma Norman campus network owned by OU IT must be scanned via an authenticated scan for increased accuracy.
- If credentialed scanning is not possible, a temporary exception must be approved via the information security risk acceptance process as approved by the OU Executive Director for IT Security.

Scanning Validation
- External and internal penetration testing will be performed on a scheduled basis. The purpose of a penetration test is to verify that the security controls protecting OU IT owned assets are working properly.
- Testing will minimally consist of network and application-layer penetration tests.
- The OU IT Security team will provide the results of penetration tests in detailed reports to the system administrator responsible for the OU IT owned asset.

Scanning Remediation
- Any vulnerabilities discovered during a security assessment will be corrected by the system administrator responsible for the asset and a retest will be performed to validate that the identified vulnerability has been appropriately remediated or mitigated. High risk vulnerabilities must be remediated or mitigated within 30 days of being reported to the system administrator. Medium risk vulnerabilities must be remediated or mitigated within 90 days and low risk vulnerabilities must be remediated or mitigated within 120 days. If an issue cannot be fixed within this timeframe, approval for an extension must be signed by the OU Executive Director for IT Security along with a detailed timeline outlining a plan of action.

EXCEPTIONS
The vulnerability management program is managed by OU IT Security. To assist with vulnerability management of any assets that cannot comply with this policy, an exemption from vulnerability scanning may be requested. Requests must document the business need for the exemption and be submitted to the OU Executive Director for IT Security for approval. Any approved requests for exception extensions will require a documented remediation action plan as agreed upon by the OU Executive Director for IT Security and the asset owner.
RESPONSIBILITIES

The following roles are responsible for assessment, application of vulnerability remediation steps, and program compliance:

- **The IT Security team** will work with the asset owner to perform a technical assessment of vulnerabilities in the supporting IT asset, product or service being addressed.
- **Asset owners** will be responsible for ensuring that the associated asset is available for security auditing and verifying that it is functioning properly after identified vulnerabilities have been mitigated.
- **System administrators** will be responsible for implementing remediating actions defined as a result of detected vulnerabilities on the OU IT owned asset.
- **The Executive Director for IT Security** will be responsible for ensuring organizational compliance with this policy.

COMPLIANCE

Failure to comply with this policy will result in the interruption of network service of an offending asset. Legal actions and fines may result from violations of applicable regulations and standards, including but not limited to, HIPAA, FERPA, and PCI.