Vulnerability Assessment Policy

Policy Title:
Vulnerability Assessment Policy

Responsible Executive(s):
Chief Information Security Officer

Responsible Office(s):
University Information Security Office

Contact(s):
If you have questions about this policy, please contact the University Information Security Office.

I. Policy Statement

This policy covers all of Loyola University Chicago's computing, networking, telephone, and information resources. In addition, please note that this policy covers all IoT devices. The purpose of this policy is to grant authorization to appropriate members of the Information Security Team to conduct audits, consisting of vulnerability assessments and penetration tests, against the University's computing, networking, telephone, and information resources.

Audits may be conducted to:

- Investigate possible security incidents
- Ensure conformance to the University's ITS policies and corresponding regulations (FERPA, PCI/DSS, HIPAA, GLBA, GDPR, etc.)
- Confirm the security of information systems
- Ensure that information is only accessible by the individuals who should be able to access it
- Ensure that system resources are available to support the mission of the University
- Ensure that information is protected from modification by unauthorized individuals

II. Definitions

CVE: The Common Vulnerabilities and Exposures (CVE) system provides a reference-method for publicly known information-security vulnerabilities and exposures.

SME: Subject Matter Expert

PCI-DSS: The Payment Card Industry Data Security Standard (PCI DSS) is a proprietary information security standard for organizations that handle branded credit

cards from the major card schemes including Visa, MasterCard, American Express, Discover, and JCB.

III. Policy

For the purpose of performing an audit, consent to access identified systems will be provided to members of the Information Security Team through the ITS Vulnerability Assessment Authorization Form. With completion of the form the University hereby provides its consent to allow members of the Information Security Team to access its computing, networking, telephone, and information resource devices to the extent necessary to perform the scans authorized in this policy.

This access may include:

- User level and/or system level access to any University computing, networking, telephone, or information resource
- Access to information (electronic, hardcopy, etc.) that may be produced, transmitted, or stored on the University's equipment or premises
- Access to work areas (labs, offices, cubicles, storage areas, etc.), through the assistance of Campus Safety
- Access to interactively monitor and log traffic on the University's networks in accordance with ITS policies and regulatory requirements

The Information Security Team will communicate the details of the vulnerability assessment with the Department Head before scheduling and deploying any assessments.

Periodic Vulnerability Scanning

The Information Security Team will run periodic, internal vulnerability scans at least quarterly. Results of these scans will be addressed in accordance with the risk posed to the University. The Information Security Team will use the Common Vulnerability Scoring System (CVSS) to aid in setting patching guidelines.

Service Degradation and/or Interruption

Network and server performance and/or availability may be affected by network scanning. The University releases the Information Security Team of any and all liability for damages that may arise from network and server availability restrictions caused by approved network scanning.

PCI Environment Requirements

The Information Security Team will run internal and external network vulnerability scans at least quarterly and after any significant change in the network. Results of these scans will be addressed in accordance with the PCI-DSS. Although the University utilizes access controls to prevent the deployment of rogue access points in the PCI-DSS environment, the Network Services Team will use wireless scanners in the University's cardholder environment on at least a quarterly basis to ensure that rogue wireless networks are not present. To aid in the identification of non-authorized access points, the Network

Services Team will maintain an inventory of authorized wireless access points including a documented business justification for each instance.

Vulnerability Risk Identification and Ranking

On a bi-weekly basis the Information Security Team along with an assigned SME from each of the functional areas of ITS will review all published vulnerabilities to determine if applicable to any operating systems or applications that are in use at the university and will rank each applicable vulnerability according to the published US-CERT and MITRE CVE scores along with the university's risk priority descriptions. Based on risk each vulnerability will be assigned to the appropriate team for response and remediation scheduling and tracking.

Penetration Testing

The information Security Team will run internal and external penetration testing annually on the PCI-DSS environment as well as on a selected rotation of non-PCI applications. Penetration tests include network-layer penetration tests, application-layer penetration tests and segmentation tests. Additionally, a second segmentation test will be performed six months from the initial penetration testing.

Application of System/Application Patches

Non-PCI patches must be applied following the patching schedule below. Any exploitable findings must be corrected, and the vulnerability scan or penetration test repeated to verify corrections.

Patching Schedule	CVSS Score
Within 30 days	7.0-10.0
Within 120 days	4.0-6.9

PCI –DSS Patching Requirements

Requirement 6.2 mandates installation of applicable critical vendor-supplied security patches within one month of release and installation of all other applicable vendor-supplied security patches within an appropriate time frame per the above patching schedule.

In addition to the above patching guidelines, vulnerabilities and exploitable findings deemed critical by the Information Security Team, regardless of CVSS score, must be patched as soon as possible.

Automated Monitoring and Alerting

Loyola employs the use of intrusion-prevention systems (IPS). All traffic at the perimeter of the cardholder data environment as well as at critical points in the cardholder data environment are monitored. All IPS monitoring points are configured to alert personnel of suspected compromises. IPS configurations and devices are configured, maintained, and updated per vendor instructions to ensure optimal protection.

Emergencies:

In emergency cases, actions may be taken by the Incident Response Team in accordance with the procedures in the ITS Incident Response Handbook. These actions may include rendering systems inaccessible.

IV. Related Documents and Forms

Please see below for the hyperlink to the ITS Vulnerability Assessment Authorization Form:

- https://www.luc.edu/its/uiso/services/vulnerabilityreviews/vuln_scan.shtml

V. Roles and Responsibilities

Chief Information Security Officer	Enforcing the Vulnerability Assessment Policy at the University by setting the necessary requirements

VI. Related Policies

Please see below for additional related policies:

- ITS Incident Response Plan
- ITS Incident Response Plan - Appendix
- ITS Security Policy

Approval Authority:	ITESC	**Approval Date:**	June 15th, 2017
Review Authority:	Jim Pardonek	**Review Date:**	June 14st, 2024
Responsible Office:	UISO	**Contact:**	datasecurity@luc.edu