Wireless Access Point and Router Policy

Policy Title:
Wireless Access Point and Router 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 devices that provide wireless access to the Loyola network. Devices that provide wireless access to a network are commonly referred to as wireless access points or wireless routers. These devices may create a security risk by providing unauthorized access to Loyola resources, including the disclosure of Loyola protected data.

II. Definitions

PCI-DSS: is a set of security standards designed to ensure that all companies that accept, process, store or transmit credit card information maintain a secure environment.

III. Policy

Faculty, Staff, Students, and Guests are prohibited from attaching any device operating as a wireless access point or router in any University building.

Any wireless connectivity into the PCI-DSS environment is strictly prohibited. Wireless networks are not allowed to connect to the credit card processing (High Security Network) environment under any circumstances.

PCI-DSS Rogue Access Point Detection

Each quarter a helpdesk ticket will be created and assigned to ITS Network Services to request a rogue wireless scan at all sites where credit cards are processed. The scan will be performed using a wireless scanner. Scan information will be reviewed and compared to a list of known Loyola access points as well as known nearby non-Loyola access points (e.g. Starbucks). All non-Loyola access points will be checked against the Loyola network MAC address table to verify that the MAC address is not present on Loyola networks. The outside access point will be added to the Loyola wireless management system (NCS) and is

marked as 'malicious. NCS will alert Network Services should it appear on the Loyola network. Results are to be saved to a spreadsheet and the ticket closed.

When Information Technology Services (ITS) becomes aware of any problem that involves a device operating as a wireless access point that is attached to the campus network in violation of this policy, the network connection to the device will be severed. If additional attempts to reconnect a prohibited device to the campus network are made, the matter will refer to the appropriate University disciplinary staff.

IV. Related Documents and Forms

Not applicable.

V. Roles and Responsibilities

Chief Information Security Officer	Enforcing the Wireless Access Point and Router Policy at the University by setting the necessary requirements

VI. Related Policies

Please see below for additional related policies:

- Security Policy
- Acceptable Usage Policy

Approval Authority:	ITESC	**Approval Date:**	October 1st , 2022
Review Authority:	Jim Pardonek	**Review Date:**	June 14st, 2024
Responsible Office:	UISO	**Contact:**	datasecurity@luc.edu