Vendor VPN Access Procedure

Policy Title:
Vendor VPN Access Procedure

Responsible Executive(s):
Chief Information Security Officer

Responsible Office(s):
University Information Security Officer

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

I. Policy Statement

This document describes the procedure to activate VPN access for vendors to Loyola networks and systems for maintenance and support. In addition, please note that this policy covers all IoT devices. Vendors requiring remote access to Loyola's intranet for configuration, maintenance, and emergency support are required to use the Loyola VPN service. As outlined in PCI-DSS requirement 8.1.5, access is enabled only when needed and disabled when not in use.

II. Definitions

VPN: a service that helps you stay private online. A VPN establishes a secure, encrypted connection between your computer and the internet, providing a private tunnel for your data and communications while you use public networks.

III. Policy

Enabling Access

When the vendor requires access to a system on the Loyola environment through a scheduled window or to respond for emergency support, the Loyola primary system contact shall contact the Loyola ITS Service desk to have access enabled.

ITS Service desk 773-508-4487 helpdesk@luc.edu

The Loyola primary system contact must provide the following information to the Servicedesk when requesting access:

- Vendor Organization
- VPN account name & associated email address

- Name and contact (phone/email) for staff performing maintenance
- System(s) to be accessed
- Anticipated time window of access required

The ITS Service desk will assign the ticket to the University Information Security Office with the above information for the account to be enabled. Once enabled, the user provided as the vendor staff member will be notified of the account activation. The remote sessions from vendors will be monitored while in use.

Emergency Procedure

The ITS Service desk maintains a list of emergency contacts that can be contacted in case of an emergency situation requiring vendor VPN access.

Disabling Access

When the vendor has completed their maintenance of the necessary systems, they should notify Loyola that access is no longer required and can be disabled.

The vendor should do this by replying to the email with notification of account enabling. The UISO department will disable the account until further use is requested.

If the vendor does not provide notification that all necessary work is completed, and access is no longer required, the Loyola vendor VPN account will be automatically disabled after 24 hours.

In addition, please note that this policy covers all IoT devices.

IV. Related Documents and Forms

Not applicable.

V. Roles and Responsibilities

Chief Information Security Officer	Enforcing the Vendor VPN Access Procedure 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:**	March 28th, 2019
Review Authority:	Jim Pardonek	**Review Date:**	June 14th, 2024

Responsible Office:	UISO	**Contact:**	datasecurity@luc.edu