XAVIER UNIVERSITY
Remote Access

Effective: May 26, 2022
Last Updated:
Last Reviewed: May 25, 2022
Responsible University Office: Information Technologies
Responsible Executive: Associate Vice President and Chief Information Officer

Scope: Students, full time and adjunct faculty, staff, retirees, non-employee associates, and guests

A. REASON FOR POLICY

The purpose of this policy is to define standards for connecting to the Xavier University network for any remote host. These standards are designed to minimize the potential security exposure to the University from damages which may result from unauthorized use of University resources. Damages include the loss of sensitive or personal data, intellectual property, damage to public image, and damage to critical internal systems.

B. POLICY

Users may only use approved and configured Virtual Private Network (VPN) client software when a VPN is required to access Xavier IT Resources (https://vpn.xavier.edu)

Users who are granted access are responsible for ensuring that their remote access connection is given the same consideration regarding security, privacy, and other information as on-site connections to the same information resources.

Users must ensure that machines are not left unlocked and unattended while connected or logged into the Xavier University network.

Login information provided for access shall not be shared with others.

VPN users will need to reauthenticate to the Xavier University network after 8 hours.

Users should immediately disconnect their device from the VPN when their work has been completed.

All personal devices that are connected to Xavier internal networks must have appropriate security protections enabled. This includes, but is not limited to, the use of anti-virus software with the latest virus updates installed, all appropriate operating system security patches applied and a personal firewall where available as outlined in the Acceptable Use policy.

All users while connected through VPN, must follow all university policies at all times, including the Acceptable Use Policy.

Remote access users are not allowed to download or store university data which is considered Internal Use, Confidential, Export, Controlled, or contains Personally Identifiable Information on their remote computing devices. This includes the transfer of this data to personal cloud services such as Dropbox or Google Drive. This data must be stored on University authorized data storage including OneDrive, SharePoint, or shared network drives.

If the device used for remote access is lost or stolen, the device should be erased if possible. Contact the help desk to report the incident and to get assistance. Any remote device that is connected to Xavier's network is subject to monitoring, which may include but is not limited to date, time, duration of access, identification of endpoint and all traffic which traverses Xavier networks.

C. DEFINITIONS (if applicable)

Internal use: Internal use information is defined as University information that is to be used within Xavier. Access to this data may be limited to specific departments and cannot be distributed outside of Xavier. Internal use information is less sensitive than Confidential information, but if exposed could have an adverse impact to the University. Internal use information includes but is not limited to strategic plans or other non-public information as dictated by the Data Custodian. All information not otherwise classified will be assumed to be internal use. Users may not disclose internal use information to anyone who is not an authorized user without prior consent of the Data Custodian.

Confidential: Confidential information is defined as personal or University information that may be considered potentially damaging if released and is only accessible to authorized users. Confidential information includes, but is not limited to, medical/health information, legally privileged information, contractual information, payment card information, personally identifiable information, protected health information and protected student information. Users may only share confidential information with people that require the information to perform their job. Sensitive HIPAA and FERPA information are considered confidential and should only be shared on an as needed basis and in compliance with any applicable laws.

Export Controlled: As a means to promote national security, the U.S. Government controls export of sensitive data, equipment, software and technology. This data is labeled Export Controlled. Users of Export Controlled data must follow all the safeguards for Restricted data plus additional safeguards as directed by The Data Trustees, Stewards, and Custodians of systems and applications that have Export Controlled data. The Custodians are responsible to identify appropriate additional safeguards.

Data Custodians: A Data Custodian is the individual authorized by the appropriate Data Steward to be responsible for management of data which includes maintaining and controlling data quality as well as granting inquiry, entry and updating data privileges within their respective area of responsibility. Data Custodians must be and serve as the departmental data liaison for their specific area.

Data Custodians are responsible for the accuracy and completeness of data and responsible for the maintenance and control of data validation and rules tables. These tables, and processes related to their use, define how business is conducted at Xavier University. The Data Custodians are responsible for access control data within his/her charge. They make data available to others for the use and support of the office or department's functions.

D. PROCEDURES

Exceptions to this policy will be handled on a case by case basis. To attain an exception, contact the Help Desk at one of the following:

Phone: (513) 745-HELP (4357)

Link: https://services.xavier.edu/TDClient/Home/

E. EXHIBITS (if applicable)

F. HISTORY

Other applicable policies and/or resources:

Information Technology Policies

- Acceptable Use Policy
- Data Classification Policy
- IT Acquisition Policy
- Remote Access Policy