Information for New Users

Remote Access and Personal Device Policy

Purpose

The purpose of this policy is to define standards, procedures, and restrictions for employees who have legitimate business needs for connecting personal devices to Saint Mary's University of Minnesota's (SMUMN's) network and/or need to remotely connect to SMUMN resources using either a personal or a Saint Mary's device. SMUMN's systems (i.e. computer systems, networks, databases, etc.) must be protected from unauthorized use and/or malicious attack that could result in loss of information/data assets, inappropriate access to confidential data, damage to critical applications, disruptions in operations, loss of revenue, and damage to the institution's public image. Therefore, all remote access and mobile privileges to SMUMN enterprise resources must employ only university-approved methods.

Scope

This policy applies to all SMUMN employees, full-time and part-time, who utilize SMUMN cloud hosted systems and/or SMUMN's internal network. **General Information** Remote access is defined as any connection to SMUMN's network and/or other applications from off-campus locations, such as the employee's home, a hotel room, airports, cafés, a satellite office, etc. There are two main types of remote access. Direct access, which is often referred to as a VPN connection, and indirect access, which is a connection to a SMUMN system that is openly available on the internet, such as the institution's Google Workspace, LMS, portal, etc. Due to the confidential data some employees require to fulfill position duties, employees in the following departments/roles are required to use SMUMN devices for all on campus and remote work. Individual positions not listed below may also require a SMUMN device for remote access based on a supervisor's recommendation and consultation with IT.

- Business Office
- Executive Leadership
- Financial Aid
- Human Resources ·
- Information Technology ·
- Institutional Effectiveness ·
- Registrars' Offices

The SMUMN IT HelpDesk will support connectivity to university systems (email, LMS, etc.) for an employee's personal device, but will not troubleshoot personal internet home networks. The employee is responsible for any issues with their personal device and "non-university" applications.

Saint Mary's will not reimburse any employee for any home internet service fees. The use of a Saint Mary's credit card for any IT hardware or software purchases is not allowed.

Policy Statements

1. It is the responsibility of all employees of SMUMN to ensure that their remote access network connection remains as secure as their network connection in their on-campus office.

2. It is imperative that any network connection, including remote access network connection, used to conduct SMUMN business be utilized appropriately, responsibly, and ethically. SMUMN's

© 2024 Saint Mary's University of Minnesota <helpdesk@smumn.edu> | 2024-04-27 10:02
URL: https://techfaq.smumn.edu/index.php?action=faq&cat=4&id=522&artlang=en

Appropriate Use of Technology Policy must be followed. No employee is to use access through university networks for the purpose of illegal transactions, harassment, competitor interests, or obscene behavior, in accordance with other related policies found in the Employee Handbook.

3. Employees must use secure remote access procedures. Use of strong passwords in accordance with SMUMN's Password Policy is required, as is securing the password so it cannot be used by others to access a university device or to access the SMUMN network. Employees must not disclose their passwords to anyone, including family members. Additionally, all computer equipment and devices used from a remote location must be reasonably secured.

4. University data of a confidential nature, especially personally identifiable information, should never be stored locally on any device (computer desktop, USB, etc.) and should be saved to SMUMN's Google Drive or an internal SMUMN drive. Employees may not under any circumstances retain confidential university documents/information in other off-network servers, Dropbox, or iCloud servers.

5. If any device used for remote access (personal or university owned) is damaged, lost, or stolen, the employee must notify their supervisor and SMUMN IT HelpDesk immediately.

6. If any incident or suspected incident of unauthorized access and/or disclosure of university resources, databases, networks, etc. occurs, the employee must notify their supervisor and SMUMN IT HelpDesk immediately.

7. Only SMUMN devices will be allowed to connect to the VPN, as this is a direct connection to the internal network. No personal devices are allowed to connect to the VPN. SMUMN devices have specific software and settings that minimize the risk of a cyber-security threat due to a lost, stolen or compromised device. Duo 2 factor authentication is required for all VPN connections.

8. Access to the Google Workspace, Canvas and other SMUMN cloud hosted software that is available on the outside internet is not considered a direct connection; therefore, access may occur from a personal device as long as the guidelines listed in #9 and #10 are followed.

9. SMUMN software should never be installed on any personal device unless authorized by SMUMN IT staff.

10. Employees must have an updated and working anti-virus program installed on any personal device that is used for remote access to SMUMN systems. Failure to do so may results in denied access to SMUMN's network. This includes operating system patches.

Investigations

Alleged violations of this policy will be investigated by the employee's supervisor, in coordination with the assistant vice president of human resources or their designee. The assistant vice president for information technology or their designee will assist with investigations, as appropriate.

Consequences

Violation of this policy will be handled according to established procedures in the Saint Mary's Employee Handbook, under the Work Rules and Conduct Standards and the Corrective Action sections. The university supports the theory of corrective action and retains discretion to take action that is appropriate to the particular circumstances. Violations of rules or policies may result in corrective measures that, depending upon the circumstances and at the discretion of the university, may include verbal or written warnings, suspension (with or without pay), or immediate discharge. These corrective measures do not constitute an exclusive list of possible action and may be repeated, skipped or taken out of order.

Sanctions for non-compliance may include legal action according to applicable laws and contractual agreements.

© 2024 Saint Mary's University of Minnesota <helpdesk@smumn.edu> | 2024-04-27 10:02
URL: https://techfaq.smumn.edu/index.php?action=faq&cat=4&id=522&artlang=en

Information for New Users

Unique solution ID: #1529
Author: n/a
Last update: 2023-10-17 21:22

© 2024 Saint Mary's University of Minnesota <helpdesk@smumn.edu> | 2024-04-27 10:02
URL: https://techfaq.smumn.edu/index.php?action=faq&cat=4&id=522&artlang=en