



Remote Access Policy

Policy:	No: 6.0
Responsible Officer:	Chief Information Officer, James Johnson
Effective Date:	May 23, 2025
Updated:	May 23, 2025
Issued By:	ITS - Information Technology Services

CONTENTS

1.0 Purpose, Scope and Responsibilities	1
2.0 Remote Access Standards	2
3.0 Virtual Private Network Access	3
4.0 Remote Desktop Access	3
5.0 Third-Party Remote Access	4
6.0 Contact Information	4
7.0 Revision History	4

1.0 Purpose, Scope and Responsibilities

1. The Information Security Policy indicates that one of the ways Saint Mary's College will protect the Confidentiality and Integrity of Saint Mary's College Data is by providing secure access to Saint Mary's College resources contained within the Saint Mary's College's network when connecting through an external network ("Remote Access").

2. The purpose of this Standard is to minimize the potential exposure and damage resulting from unauthorized access to Saint Mary's College technology resources by establishing the requirements for Remote Access. This Standard is based on requirements within NIST Special Publication 800-171 and NIST 800-46, Guide to Enterprise Telework, Remote Access, and Bring Your Own Device Security.
3. This Standard applies to any Authorized User accessing Saint Mary's College technology resources from an external network using Remote Access solutions.
4. The CIO, supported by the Network and Systems Manager, is responsible for the implementation of this standard. Information Technology Services ("ITS") Network Operations serve as the responsible units to ensure proper and appropriate access is granted to those seeking Remote Access to Saint Mary's College technology resources.
5. The vCISO will serve as an advisor to ensure this Standard establishes and maintains the best security practices for Remote Access.
6. All Authorized Users using Remote Access solutions are responsible for:
 - a. Reading and adhering to all Saint Mary's College technology policies and standards.
 - b. Adhering to the applicable requirements outlined in this standard.
 - c. Reporting all known abuse or violations of this Standard to the IT Security via e-mail at it.security@stmarys-ca.edu or phone at 925-631-4266.
 - d. Securing your home office space. Please refer to the [Tips For a Secure Workspace](#) document.
 - e. Never permitting an unauthorized user to utilize their credentials to facilitate Remote Access to Saint Mary's College technology resources.
7. Failure to follow the requirements within this Standard may result in loss or denial of Remote Access privileges.

2.0 Remote Access Standards

1. Remote Access to the Saint Mary's College Network must be used by Authorized Users to connect to non-public facing Saint Mary's College technology resources when working from a non-University location.
2. Authorized Users must authenticate Saint Mary's College technology resources using Saint Mary's College login credentials only for all Remote Access solutions. Authorized Users must never share their credentials to facilitate Remote Access Authentication for unauthorized individuals.
3. Multi-Factor Authentication (MFA) is required for all Remote Access solutions.
4. All Saint Mary's College devices must meet the SMC-owned device standards to be used as an entry point for Remote Access.
5. Remote access is only available within the United States. Access from outside the U.S.
6. Authorized Users must report any suspected, known, or imminent threat of a security incident while remotely accessing Saint Mary's College technology resources to the IT Department immediately at its.help@stmarys-ca.edu or 925-631-4266.
7. Saint Mary's College may block Remote Access in the following instances:

- a. Saint Mary's College Governance violation
 - b. Failure to adequately protect Saint Mary's College data
 - c. Evidence of security compromise in Saint Mary's College login credentials and/or hardware or software used for access
8. Blocked access may be reinstated only after the IT Department has verified that the problem(s) that resulted in access being blocked has been adequately addressed and resolved.
 9. Authorized Users must never permit Saint Mary's College devices to be used for Remote Access to be controlled or viewed remotely unless the user is required to accept the remote connection upon request using the device's input method.

3.0 Virtual Private Network Access

1. Saint Mary's College provides Virtual Private Networks ("VPNs") to permit access to Saint Mary's College's Information Systems and network folders on file servers from locations outside of Saint Mary's College's network.
2. Saint Mary's College's VPNs will employ at minimum AES-128 CBC Advanced Encryption Standard to ensure confidentiality over remote connections.
3. Remote Access to Saint Mary's College's resources via public networks is only permitted using the following approved VPN resources: Palo Alto Global Protect.
4. All VPN solutions must be configured to prevent simultaneous non-remote connections ("Split Tunneling"). All network traffic will be routed through the Saint Mary's network while connected to the VPN.
5. VPN access is provided to Saint Mary's employees and contractors who have filled out the [VPN Access Request Form](#).
6. Devices connecting to the VPN must be running a supported, up-to-date operating system: macOS Sonoma or Sequoia, or Windows 10 Workstation Pro or Windows 11.
7. If a user needs to connect to the SMC VPN using a personal device, they assume full responsibility for the security of that device and any potential unauthorized exposure of SMC data or intellectual property. Personal devices must be running a supported, up-to-date operating system to be approved for VPN access. While use of personal devices is permitted under these conditions, it is not encouraged. Users are strongly advised to use an SMC-managed device to ensure the highest level of security and compliance with SMC's Data Protection Policy.

4.0 Remote Desktop Access

RDP access via VPN may be granted on a case-by-case basis to Saint Mary's employees and contractors who have completed the [VPN Access Request Form](#).

5.0 Third-Party Remote Access

1. Vendors and contractors must have a Saint Mary's College IT Department approval to utilize Saint Mary's College's Remote Access solutions.
2. All third parties granted Remote Access to Saint Mary's College technology resources are responsible for ensuring the external networks used to access the Saint Mary's College networks are secure.
3. Connections provided to third parties will be based on Least Privilege to conduct business relative to the contractual relationship established.
4. Network to network connectivity is not permitted. Example - VNC, network sharing, and other VPN software.

6.0 Contact Information

Submit all inquiries and requests for future enhancements to the policy owner at:
Saint Mary's College of California
1928 St. Marys Rd.
Moraga, CA 94575

7.0 Revision History

This standard shall be subject to periodic review to ensure relevancy.

Date	Description of Change	Reviewer
5/23/2024	Publish	James Johnson