UNIVERSITY OF MIAMI

UNIVERSITY OF MIAMI POLICY AND PROCEDURE MANUAL

TITLE:	Remote Access	REFERENCE:	Revised
CATEGORY:	Information Technology	PAGE:	1
		SUPERSEDES:	New
APPROVER:	Joe Natoli Senior Vice President Business and Finance	VERSION: EFFECTIVE:	2 Nov. 1, 2016

I. PURPOSE:

The purpose of this policy is to define standards for connecting to the University of Miami (University) internal network and cloud hosted applications from any remote host. These requirements are designed to minimize the potential exposure of the University's information resources from damages that may result from unauthorized use. Damages include the loss of confidential or University restricted data, intellectual property, reputational damage and financial liabilities incurred as a result of those losses.

II. SCOPE:

This policy applies to University employees, faculty, students, contractors, guests, consultants, vendors, and any other non-University employee, with remote access to its network and cloud-hosted applications. This policy also applies to the University of Miami Information Technology (Central IT) personnel responsible for remote access solutions.

Remote access implementations covered by this policy, include, but are not limited to, VPN, SSL VPN, SSH, firewall exceptions, and Wi-Fi.

III. POLICY:

Remote access requires additional security controls and monitoring due to the increased risk it presents. Individuals requiring remote access privileges to University networks are responsible for ensuring their remote access connection is given the same consideration as the User's on-site connection. Only Central IT is authorized to provide remote access into the University network. Implementation for external entity remote access must be sponsored by a University employee, documented and approved by Central IT Security Operations.

IV. DEFINITIONS:

Business Associate: A vendor, consultant, contractor or any other non-University employee that performs functions or activities that involve the use or disclosure of PHI on behalf of, or provides services to, the University.

External Entity: A vendor, consultant, contractor or any non-University employee that has access to the University network or cloud hosted information resources.

Multifactor Authentication: A security system that requires more than one method of authentication from independent categories of credentials to verify the user's identity for a login or other transaction.

PII: Personally Identifiable Information

RDP: Remote Desktop Protocol

Remote Access: Any access to the University network or cloud hosted information resources through a non-University controlled network.

Restricted Data: Any data governed under Federal or State regulatory or industry compliance requirements such as HIPAA, FERPA, GLBA, PCI/DSS, Red Flag, and FISMA as well as data deemed critical to business and academic processes which, if compromised, may cause substantial harm and/or financial loss.

Trusted User: Active directory enabled University employees, faculty, students and the external entities who have executed a Third Party Connection or Business Associate Agreement.

VPN: Virtual Private Network.

V. PROCEDURE:

1. User Requirements

- Remote access to the University Network will only be allowed from Trusted Users.
- All individuals and devices connecting remotely are subject to applicable University policies; may not perform illegal activities; and may not use the access for outside business interests.
- All individuals connecting remotely will have the least amount of privilege necessary to perform their job or function.
- Remote access devices must be secured with up-to-date anti-virus software, system updates and a personal firewall.
- A remote connection must session lock after 15 minutes of inactivity and must be closed when not in use.
- A user must ensure their remote connection to the University network is not connected to any other network at the same time, with the exception of the user's personal network.
- Devices connected to a Wi-Fi network for a remote session must be encrypted.

2. Permitted Forms of Remote Access

- Remote access must be controlled with encryption as a VPN or SSL VPN connection. A SSL VPN connection is mandatory for remote access to University of Miami Hospital and University Networks that store restricted data.
- VPN and SSL VPN remote access is centrally managed by Central IT. User support for the approved connection method is provided by the University Information Technology Help Desk.
- Remote access through a SSH tunnel requires business justification and may not be used to access an information resource containing restricted data.

- Direct remote access using Telnet, RDP or other insecure method is not permitted.
- Multi factor authentication is required as an additional security control for remote access to applicable enterprise applications.

3. External Entities

- An external entity requiring remote access must execute a Third Party Connection Agreement.
- A Business Associate Agreement must be executed if requiring access to a University information resource that stores PHI data.
- Each individual in a third party organization requires a dedicated account to access University resources that handle PHI or PII.

4. Exceptions

Any exception to this policy must be approved, in advance, by Central IT Security Operations.

5. Sanctions

Knowing violations of this policy will be addressed by disciplinary policies and procedures applicable to the individual.

6. Other Applicable Policies

- Information Security Policy
- Malicious Software Prevention Policy
- Electronic Data Protection and Encryption Policy
- Mobile Computing Policy