Remote Access Policy

Date Approved:	10/27/2010
Effective Date:	1/1/2011
Date(s) Reviewed:	
Date (s) Revised:	

PURPOSE:

Information Security exists to further the mission of the University. The University is comprised of large and diverse populations with evolving needs related to information technology resources and data. University management is committed to safeguarding those resources while protecting and promoting academic freedom. Although intrinsic tension exists between the free exchange of ideas and information security, and can manifest itself in some circumstances, the following framework has been identified to promote the best balance possible between information security and academic freedom.

The Remote Access Policy outlines the requirements for connecting to the internal network from a remote location in order to ensure the confidentiality, integrity, and availability of data and electronic resources throughout the University of Miami.

SCOPE:

This policy applies to all University employees, faculty, students, contractors, guests, consultants, temporary employees, and any other users, including all personnel affiliated with third parties who have access to University resources.

DEFINITIONS:

Modem: An electronic device that converts information from an analog to a digital signal (and vice-versa); thus allowing computer systems to communicate through a standard phone line. Increasingly the term modem is used to denote any device for connecting computers to external transmission lines, whether telephone, cable or some other technology.

Two-Factor Authentication: A system that requires two pieces of information for confirming a user's identity before the user is granted access to data and other network resources.

Remote Access: Communicating with University of Miami network resources from a remote location.

Protected Data: Any data governed under Federal or State regulatory or 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.

HIPAA: The Health Insurance Portability and Accountability Act of 1996 with the purpose of ensuring the privacy of a patient's medical records.

FERPA: The Family Educational Right and Privacy act of 1974 with the purpose of protecting the privacy of student education records.

FISMA: The Federal Information Security Management act of 2002 recognizes the importance of information security to the economic and national security interests of the United States and as a result sets forth information security requirements that federal agencies and any other parties collaborating with such agencies must follow in an effort to effectively safeguard IT systems and the data they contain.

GLBA: The Gramm-Leach-Bliley Act, also known as the Financial Services Modernization Act of 1999, contains privacy provisions requiring the protection of a consumer's financial information.

PCI/DSS: Payment and Credit Card Industry Data Security Standards is guidance developed by the major credit card companies to help organizations that process card payments prevent credit card fraud, hacking and various other security issues. A company processing card payments must be PCI compliant or risk losing the ability to process credit card payments.

Red Flag: A mandate developed by the Federal Trade Commission (FTC) requiring institutions to develop identity theft prevention programs.

POLICY:

Remote access to Protected Data on the University network should be granted on a case-by-case basis only to employees with job or academic functions that make this type of access essential. Remote access requires additional security controls and monitoring due to the increased risk it presents. Users who access information resources remotely are responsible for the physical protection of the resources they use and for the information they access during remote access sessions. Scripted or automated entry of User IDs and passwords is not permitted. These additional guidelines should also be followed:

- Modems are not to be installed on University computer resources such as workstations / desktops, with the exception of University laptops.
- Modems shall be physically disconnected from any telephone line when not in use.
- Users shall maintain dial-up numbers in a strictly confidential manner.
- IT staff shall ensure that adequate controls are in place for managing and monitoring remote access services (i.e., VPN, wireless, and dial-in).
- Two-factor authentication should be implemented for all remote access users of the University network who maintain administrative authority or have access to University Protected Data. Such users include but are not limited to Network Administrators, Firewall Administrators, IT Security personnel.
- Remote workstations should include security software to detect and protect against malicious code such as worms, viruses and application exploits.
- Remote connections must time-out after 15 minutes of inactivity.
- Remote users must close any remote access connections when not in use.

- Remote users shall not employ any mechanisms that would force a connection to stay open automatically. In addition, remote users shall not connect to a University network from multiple places at the same time.

EXCEPTIONS:

Any requests for exceptions to this policy must be submitted in writing and will be reviewed on a case by case basis. Exceptions shall be permitted only after written approval from the responsible Vice President or Information Technology designee of the respective campus. The list of exceptions shall be reviewed annually and cancelled as required.

IMPLEMENTATION:

Remote Users:

- Responsible for following remote access rules outlined within the policy.

System Administrators/Data Custodians:

- Responsible for reviewing and approving requests for remote access to data and resources.

Chief Information Security Office:

- Responsible for regular review of the Remote Access Policy. The review will occur annually or when significant changes occur.

Responsible Vice President or CIO:

- Responsible for reviewing and approving or denying exception requests.
- Responsible for reviewing exceptions yearly.
- Responsible for monitoring the enforcement of the policy.

SANCTIONS:

Accounts and network access may be administratively suspended with or without notice by the University when, in the University's judgment, continued use of the University's resources may interfere with the work of others, places the University or others at risk, or violates University policy.

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

All known and/or suspected violations must be reported to the applicable Systems Administrator, who will report, as appropriate, to the applicable department.. All such allegations of misuse will be investigated by the appropriate University administrative office with the assistance of the Department of Information Technology and the Department of Human Resources.

Penalties may include:

- Suspension or termination of access to computer and/or network resources;
- Suspension or termination of employment, to the extent authorized by other university published policies and procedures;
- Suspension or termination of contract computer and/or network services; or
- Criminal and/or civil prosecution.

OTHER APPLICABLE POLICIES:

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