PL02 - Remote Access

Version: 1.0
Issued: 4/12/2017

PURPOSE

The purpose of this policy is to define the process and requirements for connecting to the ***Fitchburg State University (FSU)*** network from any remote system. These requirements are designed to minimize potential damages to the ***FSU*** network, which may result from such remote access and/or unauthorized use of university resources. Damages include, but are not limited to, the breach of confidential, sensitive, or organizational information and intellectual property, damage to public image, damage to critical internal systems, the compromise of system functionality , or the corruption of information integrity. This policy must be read in conjunction with the Acceptable Use of Information Technology Resources Policy.

SCOPE

This policy applies to all ***FSU*** employees, students, contractors, and third parties who may access ***FSU*** applications, systems, or hardware remotely. This policy does not apply to external (public) facing systems designed to be used via the web.

POLICY

All remote access to ***FSU*** applications, systems and hardware shall be authorized and approved in advance, and any access not explicitly authorized and approved is prohibited. Remote access to specific applications, systems, components and technology infrastructure shall only be granted to users with a legitimate business or academic need for such access. The level of access granted and privileges assigned shall be limited to the minimum required to perform assigned duties.

Employees and third parties authorized to utilize remote connections shall ensure that unauthorized users are not allowed access to the ***FSU*** internal network utilizing these connections. All individuals and machines, while accessing the network, including university - owned and personal equipment, are an extension of ***FSU 's*** network.

All devices, including personally-owned computers, that are connected to the network via remote access technologies must use the most up-to-date anti-virus software, and be up-to-date on available patches. Security patches for installed operating systems (with auto-update enabled), web browsers, and common applications shall be applied. A firewall must be enabled on each applicable device.

Remote access services may be used only to conduct of business-related work. Personal, private, or commercial use of any service available remotely is not permitted.

Users agree to protect ***FSU*** information assets from unauthorized access, viewing, disclosure, alteration, loss, damage, or destruction.

Remote access to data or services may not be used to copy private or personal information such as that residing on a privately-owned computer, to university file shares, or other university-owned information systems.

Remote access to data or services may not be used to store university information on a personal system, file share or other non-university owned system without prior approval from management.

ENFORCEMENT

Any employee found to have violated, intentionally or unintentionally, this policy may be subject to disciplinary action, up to and including termination of employment.

PL02 - Remote Access

Version: 1.0
Issued: 4/12/2017

ROLES AND RESPONSIBILITIES

ROLE	RESPONSIBILITY
Information Security Officer	Ensure awareness and compliance with this policy. Ensure that this policy and all component policies and procedures are maintained and implemented.
IT Staff	Ensure that individuals assigned to remotely access their applications are authorized and assigned duties require access capabilities. Ensure that the IT infrastructure is protected against unauthorized remote access. Administer the setup of newly added devices to be used for remote access.
Management Team	Determine which employees need remote access to their resources.
All Users	Understand and adhere to this policy. Safeguard their user IDs and passwords. Immediately report suspected violations of this policy to their manager or the IT Manager.

REFERENCES

Framework COBIT 4.1	Regulations and Requirements PCI DSS - MA 201	Supporting Standards and Procedures
DS5.3 Identity Management DS5.4 User Account Management	PCI Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters Requirement 8: Identify and authenticate access to system components. Requirement 12: Maintain a policy that addresses information security for all personnel. MA 201 CMR 17:00 Section 17.04	

REVISION HISTORY

This section contains comments on any revisions that were made to this document and the date they were made.

Version Number	Issued Date	Approval	Description of Changes
1.0	7/28/2015	Compass ITC	Initial Draft