CAMPUS POLICY DIRECTIVE

MARITIME REMOTE ACCESS POLICY

Policy Number	Responsible Department	Effective Date	Page
13-001	Information Technology	May 10, 2013	Page 1 of 3

1. PURPOSE

The purpose of this campus policy is to define the requirements for connecting to Maritime's Data Network (or any network managed by SUNY Maritime) from an outside entity. These requirements are designed to minimize the potential exposure to Maritime from damages which may result from unauthorized use of Maritime's resources. Damages include the loss of sensitive or confidential information, damage to our public image and damage to critical Maritime internal systems.

2. SCOPE

This policy applies to all Maritime employees, contractors, 3rd party vendors and agents with a Maritime owned or personally owned computers used to connect to Maritime's campus network. This policy also applies to remote access connections used to perform work on behalf of Maritime including reading or sending email, programming, remote support and viewing intranet web resources.

3. POLICY

3.1-General

1) Storage of confidential information on any non-state owned device is prohibited. Confidential information may not be stored on any state owned device without prior written approval from designated authority. Approved storage on any portable device must be encrypted.
2) It is the responsibility of Maritime's employees and contractors with remote access and privileges to Maritime's campus network to ensure that their remote access connection is given the same consideration as the user's on site connection to Maritime.
3) All remote access users are expected to comply with Maritime's policies; this includes not performing any illegal activities or by using the remote access capabilities for outside business interests.

3.2-Requirements

1) Remote access must be strictly controlled by the use of unique user credentials. For information on creating strong passwords please review Maritime's Cyber security policy detailing password guidelines.
2) Remote access passwords are to be used only by the individual to whom they were assigned and may not be shared.
3) All remote access connections that utilize a shared infrastructure, such as the internet, must utilize some form of encryption or secure IP sec Tunnel.
4) Reconfiguration of a home user's equipment for the purpose of split-tunneling or dual homing is not permitted at any time.
5) All hosts that are connected to Maritime's internal networks via remote access technologies must have anti-virus software implemented.
6) All hosts that are connected to Maritime's internal networks via remote access technologies must have current operating system security patches installed.
7) Personal equipment that is used to connect to Maritime's data networks must meet the requirements of Maritime owned equipment for remote access.
8) Organizations or individuals who wish to implement non-standard Remote Access solutions to the Maritime network must have prior written approval

4. ENFORCEMENT

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. Deliberate, unauthorized disclosure of confidential information may result in civil and/or criminal penalties.

5. DEFINITIONS

Term	Definition
Cable Modem	Cable companies provide Internet access over Cable TV coaxial cable. A cable modem accepts this coaxial cable and can receive data from the Internet.
Dial-in Modem	A peripheral device that connects computers to each other for sending communications via the telephone lines.
Dual Homing	Having concurrent connectivity to more than one network from a computer or network device. Internet service provider (ISP).
DSL	Digital Subscriber Line (DSL) is a form of high-speed Internet access competing with cable modems
Remote Access	Any access to Maritime's corporate network through a non-Maritime controlled network, device, or medium.
Split-tunneling	Virtual Private Network (VPN) is simultaneous direct access to a non-IT network(such as the Internet, or a home network) from a remote device (PC, PDA, WAP phone, etc.) while connected into Maritime's corporate network via a VPN tunnel. VPN a method for accessing a remote network via "tunneling" through the Internet.
Wi-Fi	Wireless networking technology that uses radio waves to provide wireless high-speed Internet and network connections. A Wi-Fi enabled device such as a PC, mobile phone, or PDA can connect to the Internet when within range of a wireless network.

.
Revisions: