University Malaysia of Computer Science & Engineering

Remote Access Policy	Created: 01/04/2013
Section of: Corporate Security Policies	Target Audience: Users, CIT
CONFIDENTIAL	Page 1 of 3

University Malaysia of Computer Science & Engineering is hereinafter referred to as "the university".
University network & internet access infrastructure is hereinafter referred to as "UniMyNet".

1.0 Overview

It is often necessary to provide access to university information resources to employees or others working outside the UniMyNet. While this can lead to productivity improvements it can also create certain vulnerabilities if not implemented properly. The goal of this policy is to provide the framework for secure remote access implementation.

2.0 Purpose

This policy is provided to define standards for accessing university information technology resources from outside the network. This includes access for any reason from the employee's home, remote working locations, while traveling, etc. The purpose is to define how to protect information assets when using an insecure transmission medium.

3.0 Scope

The scope of this policy covers all employees, contractors, and external parties that access company resources over a third-party network, whether such access is performed with university-provided or non-university-provided equipment.

4.0 Policy

4.1 Prohibited Actions

Remote access to university systems is only to be offered through a university-provided means of remote access in a secure fashion. The following are specifically prohibited:

- Installing a modem, router, or other remote access device on a company system without the approval of the Head of Campus IT.

- Use of non-university-provided remote access software.

• Split Tunneling to connect to an insecure network in addition to the UniMyNet, or in order to bypass security restrictions.

4.2 Use of non-company-provided Machines

Accessing the UniMyNet through home or public machines can present a security risk, as the company cannot completely control the security of the system accessing the network. Use of non-university-provided machines to access the UniMyNet is permitted as long as this policy is adhered to, and as long as the machine meets the following criteria:

• It has up-to-date antivirus software installed

• Its software patch levels are current

• It is protected by a firewall

When accessing the network remotely, users must not store confidential information on home or public machines.

4.3 Client Software

The university will supply users with remote access software that allows for secure access and enforces the remote access policy. The software will provide traffic encryption in order to protect the data during transmission as well as a firewall that protects the machine from unauthorized access.

4.4 Network Access

The university will limit remote users' access privileges to only those information assets that are reasonable and necessary to perform his or her job function when working remotely (i.e., email). The entire network must not be exposed to remote access connections.

4.5 Idle Connections

Due to the security risks associated with remote network access, it is a good practice to dictate that idle connections be timed out periodically. Remote connections to the university's network must be timed out after 1 hour of inactivity.

4.6 Applicability of Other Policies

This document is part of the university's cohesive set of security policies. Other policies may apply to the topics covered in this document and as such the applicable policies should be

reviewed as needed.

5.0 Enforcement

This policy will be enforced by the Head of Campus IT and/or Executive Team. Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities or theft of university property (physical or intellectual) are suspected, the university may report such activities to the applicable authorities.

6.0 Definitions

Modem A hardware device that allows a computer to send and receive digital information over a telephone line.

Remote Access The act of communicating with a computer or network from an off-site location. Often performed by home-based or traveling users to access documents, email, or other resources at a main site.

Split Tunneling A method of accessing a local network and a public network, such as the Internet, using the same connection.

Timeout A technique that drops or closes a connection after a certain period of inactivity.

Two Factor Authentication A means of authenticating a user that utilizes two methods: something the user has, and something the user knows. Examples are smart cards, tokens, or biometrics, in combination with a password.

7.0 Revision History

Revision 1.0, 01/04/2013