University Malaysia of Computer Science & Engineering

Mobile Device Policy	Created: 01/04/2013
Section of: Corporate Security Policies	Target Audience: Users, CIT
CONFIDENTIAL	Page 1 of 4

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

Generally speaking, a more mobile workforce is a more flexible and productive workforce. For this reason, business use of mobile devices is growing. However, as these devices become vital tools to the workforce, more and more sensitive data is stored on them, and thus the risk associated with their use is growing. Special consideration must be given to the security of mobile devices.

2.0 Purpose

The purpose of this policy is to specify company standards for the use and security of mobile devices.

3.0 Scope

This policy applies to university data as it relates to mobile devices that are capable of storing such data, including, but not limited to, laptops, notebooks, PDAs, smart phones, and USB drives. Since the policy covers the data itself, ownership of the mobile device is irrelevant. This policy covers any mobile device capable of coming into contact with university data.

4.0 Policy

4.1 Physical Security

By nature, a mobile device is more susceptible to loss or theft than a non-mobile system. The university should carefully consider the physical security of its mobile devices and take appropriate protective measures, including the following:

- Laptop locks and cables can be used to secure laptops when in the office or other fixed locations.

- Mobile devices should be kept out of sight when not in use.

- Care should be given when using or transporting mobile devices in busy areas.

- As a general rule, mobile devices must not be stored in cars. If the situation leaves no other viable alternatives, the device must be stored in the trunk, with the interior trunk release locked; or in a lockable compartment such as a glove box.

- The university should evaluate the data that will be stored on mobile devices and consider remote wipe/remote delete technology. This technology allows a user or administrator to make the data on the mobile device unrecoverable.

- The university should continue to monitor the market for physical security products for mobile devices, as it is constantly evolving.

4.2 Data Security

If a mobile device is lost or stolen, the data security controls that were implemented on the device are the last line of defense for protecting university data. The following sections specify the university's requirements for data security as it relates to mobile devices.

4.2.1 Laptops

Use of encryption is not required but it is encouraged if data stored on the device is especially sensitive. Laptops should require a username and password or biometrics for login.

4.2.2 PDAs/Smart Phones

Use of encryption is not required on PDAs/smart phones but it encouraged if data stored on the device is especially sensitive. PDAs/smart phones must require a password for login.

4.2.3 Mobile Storage Media

This section covers any USB drive, flash drive, memory stick or other personal data storage media. Storage of university data on such devices is discouraged, but their use is permitted and encryption is not required.

4.2.4 Portable Media Players

No university data can be stored on personal media players.

4.2.5 Other Mobile Devices

Unless specifically addressed by this policy, storing university data on other mobile devices, or connecting such devices to university systems, is expressly prohibited. Questions or requests for clarification on what is and is not covered should be directed to the Head of Campus IT.

4.3 Connecting to Unsecured Networks

Users must not connect to any outside network without a secure, up-to-date software firewall configured on the mobile computer. Examples of unsecured networks would typically, but not always, relate to Internet access, such as access provided from a home network, access provided by a hotel, an open or for-pay wireless hotspot, a convention network, or any other network not under direct control of the university.

4.4 General Guidelines

The following guidelines apply to the use of mobile devices:

- Loss, Theft, or other security incident related to a university-provided mobile device must be reported promptly.

- Confidential data should not be stored on mobile devices unless it is absolutely necessary. If confidential data is stored on a mobile device it must be appropriately secured and comply with the Confidential Data policy.

- Data stored on mobile devices must be securely disposed of in accordance with the Data Classification Policy.

- Users are not to store company data on non-company-provided mobile equipment. This does not include simple contact information, such as phone numbers and email addresses, stored in an address book on a personal phone or PDA.

4.5 Audits

The university must conduct periodic reviews to ensure policy compliance. A sampling of mobile devices must be taken and audited against this policy on a yearly basis.

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 company may report such activities to the applicable authorities.

6.0 Definitions

Encryption The process of encoding data with an algorithm so that it is unintelligible without the key. Used to protect data during transmission or while stored.

Mobile Devices A portable device that can be used for certain applications and data storage. Examples are PDAs or Smartphones.

Mobile Storage Media A data storage device that utilizes flash memory to store data. Often called a USB drive, flash drive, or thumb drive.

Password A sequence of characters that is used to authenticate a user to a file, computer, or network. Also known as a passphrase or passcode.

PDA Stands for Personal Digital Assistant. A portable device that stores and organizes personal information, such as contact information, calendar, and notes.

Portable Media Player A mobile entertainment device used to play audio and video files. Examples are mp3 players and video players.

Smartphone A mobile telephone that offers additional applications, such as PDA functions and email.

7.0 Revision History

Revision 1.0, 01/04/2013