

# University Malaysia of Computer Science & Engineering

Data Classification Policy	Created: 01/04/2013
Section of: Corporate Security Policies	Target Audience: Users, CIT
CONFIDENTIAL	Page 1 of 5

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**

Information assets are assets to the university just like physical property. In order to determine the value of the asset and how it should be handled, data must be classified according to its importance to university operations and the confidentiality of its contents. Once this has been determined, the university can take steps to ensure that data is treated appropriately.

## **2.0 Purpose**

The purpose of this policy is to detail a method for classifying data and to specify how to handle this data once it has been classified.

## **3.0 Scope**

The scope of this policy covers all university data stored on university-owned, university-leased, and otherwise company-provided systems and media, regardless of location. Also covered by the policy are hardcopies of university data, such as printouts, faxes, notes, etc.

## **4.0 Policy**

### **4.1 Data Classification**

Data residing on university systems must be continually evaluated and classified into the following categories:

1. Personal: includes user's personal data, emails, documents, etc. This policy excludes personal information, so no further guidelines apply.
2. Public: includes already-released marketing material, commonly known information, etc. There are no requirements for public information.
3. Operational: includes data for basic business operations, communications with vendors,

# University Malaysia of Computer Science & Engineering

Data Classification Policy	Created: 01/04/2013
Section of: Corporate Security Policies	Target Audience: Users, CIT
CONFIDENTIAL	Page 2 of 5

employees, etc. (non-confidential). The majority of data will fall into this category.

4. Critical: any information deemed critical to business operations (often this data is operational or confidential as well). It is extremely important to identify critical data for security and backup purposes.

5. Confidential: any information deemed proprietary to the business. See the Confidential Data Policy for more detailed information about how to handle confidential data.

## **4.2 Data Storage**

The following guidelines apply to storage of the different types of university data.

### **4.2.1 Personal**

There are no requirements for personal information.

### **4.2.2 Public**

There are no requirements for public information.

### **4.2.3 Operational**

Operational data must be stored where the backup schedule is appropriate to the importance of the data, at the discretion of the user.

### **4.2.4 Critical**

Critical data must be stored on a server that gets the most frequent backups (refer to the Backup Policy for additional information). System- or disk-level redundancy is required.

### **4.2.5 Confidential**

Confidential information must be removed from desks, computer screens, and common areas unless it is currently in use. Confidential information should be stored under lock and key (or keycard/keypad), with the key, keycard, or code secured.

## **4.3 Data Transmission**

The following guidelines apply to transmission of the different types of company data.

### **4.3.1 Personal**

There are no requirements for personal information.

# University Malaysia of Computer Science & Engineering

Data Classification Policy	Created: 01/04/2013
Section of: Corporate Security Policies	Target Audience: Users, CIT
CONFIDENTIAL	Page 3 of 5

## **4.3.2 Public**

There are no requirements for public information.

## **4.3.3 Operational**

No specific requirements apply to transmission of Operational Data, however, as a general rule, the data should not be transmitted unless necessary for business purposes.

## **4.3.4 Critical**

There are no requirements on transmission of critical data, unless the data in question is also considered operational or confidential, in which case the applicable policy statements would apply.

## **4.3.5 Confidential**

Confidential data must not be 1) transmitted outside the UniMyNet without the use of strong encryption, 2) left on voicemail systems, either inside or outside the UniMyNet.

## **4.4 Data Destruction**

The following guidelines apply to the destruction of the different types of university data.

### **4.4.1 Personal**

There are no requirements for personal information.

### **4.4.2 Public**

There are no requirements for public information.

### **4.4.3 Operational**

There are no requirements for the destruction of Operational Data, though shredding is encouraged.

### **4.4.4 Critical**

There are no requirements for the destruction of Critical Data, though shredding is encouraged. If the data in question is also considered operational or confidential, the applicable policy statements would apply.

### **4.4.5 Confidential**

Confidential data must be destroyed in a manner that makes recovery of the information impossible. The following guidelines apply:

- Paper/documents: cross cut shredding is required.

# University Malaysia of Computer Science & Engineering

Data Classification Policy	Created: 01/04/2013
Section of: Corporate Security Policies	Target Audience: Users, CIT
CONFIDENTIAL	Page 4 of 5

- Storage media (CD's, DVD's): physical destruction is required.
- Hard Drives/Systems/Mobile Storage Media: at a minimum, data wiping must be used. Simply reformatting a drive does not make the data unrecoverable. If wiping is used, the university must use the most secure commercially-available methods for data wiping. Alternatively, the university has the option of physically destroying the storage media.

## **4.5 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**

**Authentication** A security method used to verify the identity of a user and authorize access to a system or network.

**Backup** To copy data to a second location, solely for the purpose of safe keeping of that data.

**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 Data Device** A data storage device that utilizes flash memory to store data. Often called a USB drive, flash drive, or thumb drive.

**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

# University Malaysia of Computer Science & Engineering

Data Classification Policy	Created: 01/04/2013
Section of: Corporate Security Policies	Target Audience: Users, CIT
CONFIDENTIAL	Page 5 of 5

biometrics, in combination with a password.

## **7.0 Revision History**

Revision 1.0, 01/04/2013