University Malaysia of Computer Science & Engineering

Retention 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

The need to retain data varies widely with the type of data. Some data can be immediately deleted and some must be retained until reasonable potential for future need no longer exists. Since this can be somewhat subjective, a retention policy is important to ensure that the university's guidelines on retention are consistently applied throughout the organization.

2.0 Purpose

The purpose of this policy is to specify the university's guidelines for retaining different types of data.

3.0 Scope

The scope of this policy covers all university data stored on university-owned, university-leased, and otherwise university-provided systems and media, regardless of location.

Note that the need to retain certain information can be mandated by local, industry, or federal regulations. Where this policy differs from applicable regulations, the policy specified in the regulations will apply.

4.0 Policy

4.1 Reasons for Data Retention

The university does not wish to simply adopt a "save everything" mentality. That is not practical or cost-effective, and would place an excessive burden on the IT Staff to manage the constantly-growing amount of data.

Some data, however, must be retained in order to protect the university's interests, preserve evidence, and generally conform to good operational practices. Some reasons for data retention include:

- Litigation
- Accident investigation
- Security incident investigation
- Regulatory requirements
- Intellectual property preservation

4.2 Data Duplication

As data storage increases in size and decreases in cost, universities often err on the side of storing data in several places on the network. A common example of this is where a single file may be stored on a local user's machine, on a central file server, and again on a backup system. When identifying and classifying the university's data, it is important to also understand where that data may be stored, particularly as duplicate copies, so that this policy may be applied to all duplicates of the information.

4.3 Retention Requirements

This section sets guidelines for retaining the different types of university data.

Personal There are no retention requirements for personal data. In fact, the university requires that it be deleted or destroyed when it is no longer needed.

Public Public data must be retained for 1 year.

Operational Most university data will fall in this category. Operational data must be retained for 2 years.

Critical Critical data must be retained for 3 years.

Confidential Confidential data must be retained for 3 years.

4.4 Retention of Encrypted Data

If any information retained under this policy is stored in an encrypted format, considerations must be taken for secure storage of the encryption keys. Encryption keys must be retained as long as the data that the keys decrypt is retained.

4.5 Data Destruction

Data destruction is a critical component of a data retention policy. Data destruction ensures that the university will not get buried in data, making data management and data retrieval more complicated and expensive than it needs to be. Exactly how certain data should be destroyed is covered in the Data Classification Policy.

When the retention timeframe expires, the university must actively destroy the data covered by this policy. If a user feels that certain data should not be destroyed, he or she should identify the data to his or her supervisor so that an exception to the policy can be considered. Since this decision has long-term legal implications, exceptions will be approved only by a member or members of the university's executive team.

The university specifically directs users not to destroy data in violation of this policy. Particularly forbidden is destroying data that a user may feel is harmful to himself or herself, or destroying data in an attempt to cover up a violation of law or university policy.

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

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 and secure without the key. Used to protect data during transmission or while stored.

Encryption Key An alphanumeric series of characters that enables data to be encrypted and decrypted.

7.0 Revision History

Revision 1.0, 01/04/2013