Standard

Information Security Classification

1 Introduction

1.1 Purpose

SCE holds many significant information assets that must be protected against unauthorized access, disclosure or modification, or other misuse. Different types of information require different security measures, making proper classification of information assets critical to effective enterprise security. SCE's information classification policy is designed to provide information owners with guidance as to how to classify information assets properly.

1.2 Scope

This document covers the levels of security classification for information and limited recommendations for its protection.

It does not attempt to classify any particular information nor does it have any bearing on the legal requirements for document retention or record classification.

This document must be read in conjunction with the Records Management Policy and Information Security Policy.

1.3 Background

SCE handles many different types of information. As part of the development of both the Records Management Policy and Information Security Policy, a need was identified that a standard for classifying the sensitivity of information was required to go with a set of recommendations on how to store this information.

Individual creators, owners or handlers of SCE information must apply this classification system to their information.

2 Responsibilities

Information Owners are responsible for assessing information and classifying its sensitivity. They should then apply the appropriate controls to protect that information.

All SCE staff and students must respect the security classification of any information and, if any information is found with a security classification, in an inappropriate place, they must report this to Data Protection officer as soon as possible.

3 Security Information Classification

3.1 Overview of policy:

Information owners must assign one of the following four classifications (see Table 1) to any information assets under their control:

1. **Public**

   Public information can be disclosed or disseminated without any restrictions on content, audience or time of publication. However, the disclosure or dissemination of the information must not violate any applicable laws or regulations — such as privacy rules — and modification must be restricted to individuals who have been explicitly approved by information owners to

modify that information, and who have successfully authenticated themselves to the computer system.

2. **Internal**

   Internal use information can be disclosed or disseminated to appropriate members of SCE, partners and other individuals, as appropriate by information owners without any restrictions on content or time of publication.

3. **Restricted**

   Restricted information is subject to access restrictions of some type. These restrictions may apply to all or part of the content, to the intended audience for the information, or to the time of publication. All access to confidential information requires that the users first successfully authenticate themselves to the computer system. Disclosure or dissemination of this information is not intended, but it would not result in severe damage to SCE.

4. **Confidential**

   Confidential information has significant value for SCE, and unauthorized disclosure or dissemination would result in severe damage to SCE. All information that is not explicitly classified as public, internal use or restricted is to be considered confidential. Access to confidential information must be controlled by strong authentication — user ID and password are not sufficient — and is permitted only for specific named individuals. All access attempts must be logged. Storage and transmission of confidential information must be protected by encryption.

Designating information as confidential involves significant costs to SCE. For this reason, information owners making classification decisions must balance the damage that could result from unauthorized access to or disclosure of the information against the cost of additional hardware, software or services required to protect it.

The default level for unclassified data is *Internal Use*.

3.2 Overview of classifications

Classification	Examples of Information	Typical Amount	Security Costs	Examples of Security Measures
Public	Programme & course information on SCE's website	Many documents	Negligible	Write-protected file format
Internal Use	Company policies & procedures	Many documents	Low	Windows, SharePoint & One Drive directory access. Kept in drawer
Restricted	Project or personal documents, individual student records	Majority of documents	Medium	Windows, SharePoint & One Drive directory access. Kept in locked drawer
Confidential	Large amounts of HR systems, SCE central data	Selected documents	Very high	Secure access, password protected,

				intrusion prevention tools.

3.3 Delegation of roles and responsibilities

By default, information is owned by the person or role that created or obtained it. However, departments may delegate ownership, and information owners may delegate ownership further, defining ownership on a more detailed level. However, such delegation must be:

3.3.1 Explicit

The default information owner must specifically identify the affected information assets (for example, room, folder or database) and notify the new information owner of the change. The current owner must identify respective information resources and must notify the new owner of the change. Implicit delegation (for example, by job description) is not acceptable.

3.3.2 Written

Verbal delegation of information ownership is not acceptable.

3.3.3 Specific to an individual or role

Information ownership must be delegated to a specific person or to a role with which a specific person can be identified. Ownership cannot be delegated to a group.