DATA CLASSIFICATION POLICY

1. Purpose

The Data Management and Classification Policy requires Data Owners to classify their data according to its sensitivity and criticality. This procedure sets out how this classification is to be performed.

2. Roles and Responsibilities

The Data Owner will classify their data and ensure that the data inventory with respect to their data is accurate and up to date.

3. Scope

This procedure applies to all Data Owners as described in the Data Management Policy. This procedure applies to electronic data only, for data classification of non-electronic data, please refer to TCIS records management policy.

4. Data Classification Procedure

As per ISO 27002 the purpose of information classification is to ensure that information/data receives an appropriate level of protection.

Following on from this, TCIS classifies its data based on the level of impact that would be caused by inappropriate access and/or data loss.

There are three classifications as follows:

- Confidential data
- Internal Use Only data
- Public

Classification of data is independent of its format.

The following table provides an indication of how classifications get assigned through considering the impact of various risks.

Risk ↓	IMPACT IS CONSIDERED FROM FOUR MAIN PERSPECTIVES- LEGAL, REPUTATIONAL, FINAN AND OPERATIONAL (REFER TO APPENDIX II FOR FURTHER GUIDANCE)		
Inappropriate access causing breach of confidentiality/data protection rules	Minor	Moderate	Serious
Inappropriate access resulting in unauthorised amendments	Minor	Moderate	Serious
Data loss	Minor	Moderate	Serious
UNAUTHORISED DISCLOSURE	Minor	Moderate	Serious
	↓	↓	↓
RESULTING DATA CLASSIFICATION	**Public Data**	**Internal Use Only**	**Confidential Data**
	↓	↓	↓
DATA CLASSIFICATION EXAMPLES	1: Public Websites. 2: Social media data.	1: Internal Notices /Training data 2: Internal telephone contact list 3: Financial Department and company Budgets.	1: Finance Data. 2:HR Data. 3: Customer Personal Data

Data that is not yet been classified should be considered confidential until the owner assigns the classification. Long term classification of Data as confidential for this reason is not acceptable.

Public Data

Public data is information that may be open to the general public. It is defined as information with no existing local, national, or international legal restrictions on access or usage. Public data can be made available to all Rugby School Thailand employees –and to all individuals and entities external to the TCIS

By way of illustration only, some examples of public data include:

- Publicly posted content on all external facing web sites.
- Publicly posted press release.
- Publicly posted TCIS Marketing and press releases

Internal Only Use

Internal only use data is confidential information that must be protected due to proprietary, ethical, or privacy considerations, and must be protected from unauthorized access, modification, transmission, storage, or other use. Internal use data is information that is restricted to members of TCIS employees who have a legitimate purpose for accessing such data.

By way of illustration only, some examples of official use data include:

- Internal Notices /Training data
- Internal telephone contact list
- Financial budgets

Confidential Data

Confidential data is information or data protected by statutes, regulations, UCC or contractual obligation. Confidential data may be disclosed to authorized individuals on a need-to-know basis only.

The following table describes the types of Confidential Data and gives examples of each type. The examples given in this table are by way of illustration only and this is not an exhaustive list.

Confidential Data Type:	Description:	Example:
Company secret data	Commercially sensitive data for which we have an	High value data that comprises intellectual properties, for business, commercials or

	institutional obligation to protect	research projects i.e. trade secret, formular, commercial contracts
Personal Data	Data relating to a living individual who is or can be identified from the data	Name Address Credit Card Number CCTV Footage Customer Records Personnel and Payroll Records Bank Account Details
Special Categories of Personal Data	There are specific categories of data which are defined by the PDPA (Personal Data Protection Act) as sensitive personal data	Physical or mental health data, disability, racial, ethnic, origin, political opinions, cult, religious or philosophical beliefs, sexual behavior, criminal records, biometric data, genetic data, Trade Union information.

Confidential data, when stored in an electronic format, must be protected with strong passwords, and stored on servers that have appropriate access control measures in order to protect against loss, theft, unauthorized access and unauthorized disclosure.

Technical considerations for electronically storing Special Categories of Personal Data should be considered on a case-by-case basis, the Data Owner should engage with the CTO/Director of IT and DPO to ensure the appropriate technical protections and control measures are in place for protecting this type of data in line with TCIS obligations under the Data Protection and Data Security Policy

Confidential data must not be disclosed to parties without explicit management authorization from the data owner, Confidential data must only be used for the purpose for which it was originally gathered. For additional information on Data Protection, please refer to TCIS Data Protection and Data Security Policy

Classification Record of the data inventory as per the template in Appendix One should clearly indicate the data classification assigned to individual data sets for TCIS processes. It is the responsibility of individual data owners to input into the data inventory. It is the responsibility of the CTO/Director of IT to coordinate and update this data inventory.

Appendix One

Process Name	Data Set	Data Owner	Data Storage Location	Data Processor name	Data Classification: Public, internal, Confidential	Data Retention Period	Data Disposal Technique

Appendix II

Impact Assessment - Guidance on classifying data

Internal, Confidential and Sensitive information must be classified appropriately to protect it from unauthorised access, interception, copying, modification, transmission, or destruction.

- Strategic business strategy, Intellectual property, and other information - only available to members of the project and those that clearly need access. ***Confidential***,
- Company-wide project communications - ***Internal***
- Sensitive roadmap, financial, forecasting, customer, or other information - ***Sensitive***, only available to key project members or specific departments

Classification Level	**Financial**	**Reputational**	**Personnel / Safety**	**Operational**	**Legal**
Confidential **+ Sensitive**	Serious commercial disadvantage or loss, including financial or legal penalties	Serious reputational damage - will lead to negative perception and company value drop	Danger to personal safety or rights/freedoms. Will significantly impact rights and freedoms of individuals on a large scale Prolonged distress, discomfort, or embarrassment to an individual	Long-term disruption to operations and service, including likely loss of business contracts	Major breach of a statutory obligation (such as Data Protection)