Revision History

Version	Date
Data Classification Policy, 1.0	29 July 2021

DATA CLASSIFICATION POLICY

I. Introduction

As indicated in the USEIC Data Protection Charter (the "Charter"), any person who uses, stores, or transmits Organizational Data (as defined in the Charter) has a responsibility to maintain and safeguard such Data.

The first step in establishing the safeguards that are required for a particular type of Organizational Data is to determine the level of sensitivity applicable to such Data. Data classification is a method of assigning such levels and thereby determining the extent to which the Organizational Data need to be controlled and secured.

Capitalized terms used in this Policy without definition are defined in the Charter.

II. Policy

Data security measures must be implemented commensurate with the sensitivity of the Organizational Data and the risk to the Organization if such Data is compromised. It is the responsibility of the applicable Data Owner to evaluate and classify Organizational Data for which he/she is responsible according to the classification system adopted by the Organization and described below. If Organizational Data of more than one level of sensitivity exists in the same System or Endpoint, such Data shall be classified at the highest level of sensitivity.

A. Data Classification

The Organization has adopted the following four classifications of Organizational Data:

1. Sensitive Data: any information protected by national or international laws and regulations or industry standards, such as PDPA and GDPR.

For the purposes of this Policy and the other Data Protection Policies, Sensitive Data include, but are not limited to, Personally Identifiable Information, as defined below:

Personally Identifiable Information or PII: any information about an individual that (1) can be used to distinguish or trace an individual's identity, such as name, date and place of birth, mother's maiden name or biometric records, (2) is linked or linkable to an individual, such as medical, educational, financial and employment information, which if lost, compromised or disclosed without authorization, could result in harm to that individual and (3) is protected by national or international laws and regulations or industry standards.

Examples of Sensitive Data can be found in Appendix A.

2. Confidential Data: any information that is contractually protected as confidential by law or by contract and any other information that is considered by the Organization appropriate for confidential treatment.

For purposes of this Policy and the other Data Protection Policies, Confidential Data include, but are not limited to:

- Customer records that are directly related to prior and current customers and maintained by USEIC or an entity acting on USEIC's behalf;
- Human resources information, such as salary and employee benefits information;
- Information received under contracts subject to confidentiality requirements;
- Law enforcement or court records and confidential investigation records;
- Citizen or immigrations status;
- Unpublished research data;
- Unpublished organizational financial information and strategic plans;
- Information on facilities security systems;
- Nonpublic intellectual property, including invention disclosures and patent applications
- Customer financial information.

3. Internal Data: any information that is proprietary or produced only for use by members of the organizational community who have a legitimate purpose to access such data.

For purposes of this Policy and the other Data Protection Policies, Internal Data include, but are not limited to:

- Internal operating procedures and operational manuals;
- Internal memoranda, emails, reports and other documents;
- Technical documents such as system configurations and floor plans.

4. Public Data: any information that may or must be made available to the general public, with no legal restrictions on its access or use.

For purposes of this Policy and the other Data Protection Policies, Public Data include, but are not limited to:

- General access data on www.useic.org;
- Organization financial statements and other reports filed with national governments and generally available to the public;
- Copyrighted materials that are publicly available.

B. Protection of Organizational Data

The protection requirements applicable to each classification of Organizational Data can be found in the USEIC Registration and Protection of Systems Policy and/or the USEIC Registration and Protection of Endpoints Policy.

Appendix A

Examples of Sensitive Data

Examples of PII include, but are not limited to, any information concerning a natural person that can be used to identify such natural person, such as name, number, personal mark, or other identifier, in combination with any one or more of the following:

- Singapore National Registry Identification Number (NRIC), Foreign Identification Number (FIN) or Birth Certificate Number;
- Driver's license number;
- Account number, credit, or debit card number, in combination with any required security code, access code or password that would permit access to an individual's Singapore Personal Access (Singpass) or financial account;
- Passport number.