USEIC

Revision History

Version	Date
Data Protection Charter, 1.0	29 July 2021

DATA PROTECTION CHARTER

I. Introduction

While conducting its business operations, United States Education Information Center ("USEIC" or the "Organization") collects many different types of data, including financial, academic, human resources and other personal information. USEIC appreciates the ability to communicate and share data appropriately. Such data is an important resource of USEIC and any person who uses information collected by USEIC has a responsibility to maintain and protect this resource. Government regulations, as well as industry standards, also impose obligations on USEIC to protect the confidentiality, integrity and availability of data relating to staff, partners, and customers. In addition, terms of certain contracts and organizational policy require appropriate safeguarding of data.

This Charter and the data protection policies adopted by USEIC (collectively, the "Data Protection Policies") define the principles and terms of USEIC's Data Protection Program and the responsibilities of USEIC and its partners in carrying out the Data Protection Program. The current Data Protection Policies are listed in Appendix A.

The information resources (the "Information Resources") included in the scope of the Information Security Policies are:

- All Organizational Data (as defined below) regardless of the storage medium (e.g., paper, disk, CD, DVD, external drive, etc.) and regardless of form (e.g., text, graphic, video, audio, etc.);
- The computing hardware and software Systems (as defined below) that process, transmit and store Organizational Data; and
- The Networks (as defined below) that transport Organizational Data.

The Data Protection Policies are Organization-wide policies that apply to all individuals who access, use or control Information Resources at USEIC, including staff as well as contractors, consultants, and other agents of USEIC and/or individuals authorized to access Information Resources by affiliated institutions and Organizations.

II. Charter

The mission of the Data Protection Program is to protect the confidentiality, integrity, and availability of Organizational Data. Confidentiality means that information is only accessible to authorized users. Integrity means safeguarding the accuracy and completeness of Organizational Data and processing methods. Availability means ensuring that authorized users have access to Organizational Data and associated Information Resources when required.

This Charter establishes the various functions within the Data Protection Program and authorizes the persons described under each function to carry out the terms of the Data Protection Policies.

The functions are:

A. Executive Management

Executive Managers are senior Organization officials, including the Director, and Senior Business Officers, who are responsible for overseeing data protection for the Organization and ensuring compliance with all Data Protection Policies. Such responsibilities include, but are not limited to:

- Ensuring that each System Owner and Data Owner in their respective areas of responsibility appropriately identify and classify Organizational Data in accordance with the USEIC Data Classification Policy;
- Ensuring that each such System Owner and Data Owner receives training on how to handle Sensitive Data; and
- Ensuring that each IT Custodian in his/her area of responsibility provides periodic reports with respect to the inventory of Information Resources used in such area to the Owner of USEIC.

B. Security Management

Security Managers are personnel at USEIC who are responsible for the day-to-day management of the Data Protection Program, including:

- Developing, documenting, and disseminating the Data Protection Policies;
- Educating and training organizational personnel in data protection matters;
- Communicating information regarding the Data Protection Policies;
- Developing and executing the Risk Management Program;
- Translating the Data Protection Policies into technical requirements, standards, and procedures;
- Collaborating with Data Owners and System Owners to determine the appropriate means of using Information Resources; and
- Authorizing any required exceptions to any Data Protection Policy or any associated technical standards or procedures and reporting such exceptions to USEIC's legal counsel.

In addition to the responsibilities listed above, the Executive Managers have granted the authority to Security Managers to conduct the following activities:

- Monitoring communications and Organizational Data that use the Organization's Network or Systems for transmission or storage;
- Monitoring use of the USEIC's Information Resources;
- Conducting vulnerability scanning of any Information Resources connected to the Organization's Network;
- Conducting security assessments of internal and external vendor Systems, Server centers and Data centers;
- Disconnecting Information Resources that present a security risk from the Organization's Network;
- Erasing all Organizational Data stored on personal Endpoints previously used for business, as requested, or required; and
- Leading and managing the Response Team in connection with any breach or compromise of Sensitive Data, to the extent provided for in the USEIC Electronic Data Security Breach Reporting and Response Policy.

The Data Protection Officer (DPO) is responsible for management of the Data Protection Program ("DDP Management") and for overseeing all DPP Management activities conducted by Security Managers.

C. Data Ownership

Data Owners are personnel who are responsible for determining Data classifications, performing risk assessments, and developing the appropriate procedures to implement the Data Protection Policies in their respective areas of responsibility. Such responsibilities include, but are not limited to:

- Appropriately identifying and classifying Organizational Data in their respective areas of responsibilities in accordance with the USEIC Data Classification Policy;
- Establishing and implementing security requirements for Organizational Data in consultation with the applicable Security Managers;
- Where possible, clearly labeling Sensitive Data and Confidential Data;
- Approving appropriate access to Organizational Data; and
- Ensuring that the USEIC Sanitization and Disposal of Information Resources Policy is followed.

D. System Ownership

System Owners are personnel who are responsible for determining computing needs, and applicable System hardware and software, in their respective areas of responsibility and ensuring the functionality of each such system. Such responsibilities include, but are not limited to:

- Classifying each System in their respective areas of responsibility based on the identification and classification of Organizational Data by the applicable Data Owner;
- Ensuring that each such System that contains Sensitive Data is scheduled for risk assessment in accordance with the USEIC Information Security Risk Management Policy;
- Establishing and implementing security requirements for each such System in consultation with the applicable Security Manager;
- Ensuring that each System is operated in accordance with the Data Protection Policies;
- Documenting and implementing audit mechanisms, timing of log reviews and log retention periods;
- Maintaining an inventory of such Systems;
- Approving appropriate access to such Systems; and
- Ensuring that the USEIC Sanitization and Disposal of Information Resources Policy is followed.

E. Technical Ownership

IT Custodians are personnel who are responsible for providing a secure infrastructure in support of Organizational Data, including, but not limited to, providing physical security, backup, and recovery processes, granting access privileges as authorized by Data Owners or System Owners and implementing and administering controls over Organizational Data in their respective areas of responsibility. Such responsibilities include, but are not limited to:

- Maintaining an inventory of all Endpoints used in their respective areas of responsibility;
- Conducting periodic security checks of Systems and Networks, including password checks, in their respective areas of responsibility;
- Documenting and implementing audit mechanisms, timing of log reviews and log retention periods;
- Performing self-audits and reporting metrics to the applicable Data Protection Office and monitoring assessments and appropriate corrective actions; and
- Ensuring that the USEIC Sanitization and Disposal of Information Resources Policy is followed.

F. System or Data Storage

Users are persons who use Information Resources. Users are responsible for ensuring that such Resources are used properly in compliance with the USEIC Acceptable Usage of Information Resources Policy, information is not made available to unauthorized persons and appropriate security controls are in place.

III. Definitions

As used in the Information Security Policies, the following terms are defined as follows:

AES: the Advanced Encryption Standard adopted by the U.S. government.

Confidential Data: any information that is contractually protected as confidential information and any other information that is considered by the University appropriate for confidential treatment. See the USEIC Data Classification Policy for examples of Confidential Data**.**

Data Owner: as defined in Section II(C) of this Charter.

DHCP: Dynamic Host Configuration Protocol, which is a Network protocol that enables a Server to automatically assign an IP address to a Network enabled device from a defined range of numbers (i.e., a scope) configured for a given Network.

DNS: Domain Name System, which is a protocol within the set of standards for the exchange of Organizational Data on the Internet or on a private Network. The Domain Name System translates a user-friendly domain name such as http://www.useic.org into an IP address such as "129.60.106.25" that is used to identify computers on a Network.

Email System: a System that transmits, stores, and receives emails.

Endpoint: any desktop or laptop computer (i.e., Windows, Mac, Linux/Unix), Mobile Device or other portable device used to connect to the Organization's wireless or wired Network, access USEIC email from any local or remote location or access any System either owned by the Organization or by an individual and used for organizational purposes.

IDEA: the International Data Encryption Algorithm.

Information Resources: as defined in Section I of this Charter.

Data Protection Policies: as defined in Section I of this Charter.

Internal Data: as defined in the USEIC Data Classification Policy**.**

IP: Internet Protocol.

IT: Information Technology.

IT Custodian: as defined in Section II(E) of this Charter.

Key Business System: as defined in the USEIC Business Continuity and Disaster Recovery Policy.

MAC: Media Access Control.

MFA: Multi Factor Authentication.

Mobile Device: a smart/cell phone (i.e., iPhone, Blackberry, Android, Windows phone), tablet (i.e., iPad, Nexus, Galaxy Tab, and other Android based tablet) or USB/removable drive.

Network: electronic Information Resources that are implemented to permit the transport of Organizational Data between interconnected Endpoints. Network components may include routers, switches, hubs, cabling, telecommunications, VPNs, and wireless access points.

Organizational Data: all items of information that are created, used, stored, or transmitted by the organizational community for the purpose of carrying out the Organization's mission and all data used in the execution of the Organization's required business functions.

Organizational Network: the Network owned and operated by the Organization, including the USEIC Network.

Peer: a network participant that makes a portion of its resources, such as processing power, disk storage or network bandwidth, directly available to other network participants, without the need for central coordination by Servers or stable hosts. Examples include KaZaa, BitTorrent, Limewire and Bearshare.

Peer-to-Peer File Sharing Program: a program that allows any computer operating the program to share and make available files stored on the computer to any machine with similar software and protocol.

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 the Republic of Singapore's laws and regulations or industry standards.

Public Data: as defined in the USEIC Data Classification Policy.

Removable Media: CDs, DVDs, USB flash drives, external hard drives, Zip disks, diskettes, tapes, smart cards, medical instrumentation devices and copiers.

Risk Analysis: the process of identifying, estimating and prioritizing risks to organizational operations, assets, and individuals. "Risk Assessment" is synonymous with "Risk Analysis".

Risk Management Program: the combined processes of Risk Analysis, Risk Remediation and Risk Monitoring.

Risk Monitoring: the process of maintaining ongoing awareness of an organization's information security risks via the risk management program.

Risk Remediation: the process of prioritizing, evaluating, and implementing the appropriate risk-reducing security controls and countermeasures recommended from the risk management process. "Risk Mitigation" or "Corrective Action Planning" is synonymous with "Risk Remediation".

RSA: the Rivest-Shamir-Adleman Internet encryption and authentication system.

Sensitive Data: any information protected by the Republic of Singapore's laws and regulations and industry standards, such as PDPA. See the USEIC Data Classification Policy for examples of Sensitive Data.

Server: any computing device that provides computing services, such as Systems and Applications, to Endpoints over a Network.

Service Account: a special User account for a System used to make configuration changes to the System.

SMTP: Simple Mail Transfer Protocol, which is an internet transportation protocol designed to ensure the reliable and efficient transfer of emails and is used by Email Systems to deliver messages between email providers.

SSL: the Secure Sockets Layer security protocol that encapsulates other network protocols in an encrypted tunnel.

System: Server based software that resides on a single Server or multiple Servers and is used for organizational purposes. "Application" or "Information System" is synonymous with "System".

System Administrator: a person who is responsible for the configuration, operation, and maintenance of a System.

System Owner: as defined in Section II(D) of this Charter.

UPS: Uninterruptible Power Supply.

USEIC or the Organization: as defined in Section 1 of this Charter.

User: as defined in Section II(F) of this Charter.

User ID: a User Identifier.

VPN: Virtual Private Network.

IV. Enforcement

Violations of the Data Protection Policies may result in corrective actions which may include: (a) the immediate suspension of computer accounts and network access; (b) mandatory attendance at additional training; (c) a letter to the employee's personnel file; (d) administrative leave without pay; (e) termination of employment or contract or non-renewal of contract or employee status; or (f) civil or criminal prosecution.

V. Applicable Laws, Regulations, and Industry Standards

The laws and regulations and industry standards and certain international laws and regulations that are applicable to data protection at the Organization are listed in Appendix A.

Appendix A

Applicable Laws and Regulations

National

Republic of Singapore Personal Data Protection Act 2012 (PDPA)

International

European Union (EU) General Data Protection Regulation (GDPR)