Revision History

Version	Date
Registration and Protection of Systems Policy, 1.0	30 July 2021

REGISTRATION AND PROTECTION OF SYSTEMS POLICY

I. Introduction

This Policy describes the requirements for security controls to protect Systems that process, transmit and/or store Organizational Data (as each is defined in the USEIC Data Protection Charter (the "Charter")). Such requirements differ depending on whether such Data is Sensitive Data, Confidential Data, Internal Data or Public Data (as each is defined in the Charter).

Any System that processes, transmits and/or stores Organizational Data must be registered in accordance with Section II(A), risk assessed and certified in accordance with Section II(B) and have the minimum protections set forth in Section II(C) and, if applicable, Sections II(D), (E), (F), (G), (H) and/or (I), in each case for the most restricted class of Organizational Data that is processed, transmitted or stored on such System.

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

II. Policy

A. Registration of Systems

Systems at the Organization must be registered with the Data Protection Officer (DPO). Registration will be carried out in accordance with the procedures established by the DPO.

B. Risk Assessment and Certification Requirements for Systems

If required by the DPO, each System is subject to risk assessment, remediation, if necessary, by the System Owner and certification in accordance with procedures established by the DPO. Each certified System shall be recertified on a periodic basis, as determined by the level of risk, by the DPO.

C. General Protection Requirements for Systems

Each System Owner will ensure that the following protections, at a minimum, are implemented for each System:

1. An IT Custodian has been appointed for the System by the System Owner. Contact information for Systems should be provided to dpo@useic.org.
2. The facility that houses the System's Servers, including primary and backup equipment, is environmentally controlled and physically secured from unauthorized access.
3. Each Server is physically labelled with a name or other identification.
4. All Organizational Data files on a Server are backed up regularly in accordance with the USEIC Business Continuity and Disaster Recovery Policy.
5. Each of the System's production Servers has a UPS that can provide emergency power and shut the Server down in case of a power outage.

6. Standard configurations, as defined by the DPO, are used to establish a secure configuration baseline.
7. Access to the System's Servers and the Organizational Data residing on the System is restricted and is maintained in accordance with the USEIC Information Resource Access Control and Log Management Policy.
8. The System's Servers are not used for general desktop functions, such as web browsing, conducting personal email or other USEIC business or non-business functions.
9. The System's Servers are running vendor-supported operating systems and have up-to- date security patches installed.
10. The System's Servers are accessible only for the services provided and only to as much of the Network as is required to provide such services, and firewalls or equivalent protections prevent unauthorized access. To the extent practicable, anti-virus, anti- spyware and System monitoring programs are installed to protect and/or prohibit unauthorized access.
11. Any Peer-to-Peer Program is used only for organizational purposes, is configured properly as directed by the DPO and does not permit general purpose file sharing over the Internet.
12. Only required services that run on the System's Servers are enabled. Unneeded services are disabled.
13. Each System used for organizational purposes is disposed of in accordance with the USEIC Sanitization and Disposal of Information Resources Policy.

D. Additional Protection Requirements for Systems Containing Sensitive Data

Each System Owner shall ensure that, in addition to the protections described in Section C above, the following protections are implemented for each System that processes, transmits and/or stores Sensitive Data:

1. A record is kept of what type of Sensitive Data are stored on the System's Servers and of all changes to the configuration of the Server, and such documentation is kept in a secure, locked location away from the Server.
2. In web-based Systems that are exposed to the Internet, protection mechanisms are implemented to prevent common web-based attacks. Examples of protection elements include web-based firewalls and/or source code security reviews.
3. Sensitive Data are encrypted while in transit and in storage.
4. Removable Media containing Sensitive Data are encrypted.
5. In Relational Database Management Systems, Sensitive Data are encrypted in a way that permits database administrators to perform their management functions without access to such Data in a readable format.
6. The System's Servers are maintained in appropriate Data centers, Server closets or Data closets that meet or exceed the following physical requirements:
    - Video camera surveillance;
    - Badge reader (rather than key) access;
    - Use of a visitor log to document all visitors who accompany an authorized User, which is posted by the main ingress/egress point of the secure facility;
    - Alarms on the door that alert USEIC staff if (x) the door is left ajar, (y) the door is forced open or (z) the security lock malfunctions; and
    - An emergency power shut off button that can cut off power to all circuits in the case of a fire or other physical threat.

It is recommended, but not required, that Confidential Data be protected with a password while in transit or in storage.

E. Additional Protection Requirements for Registered Systems

Each System Owner of any System that is registered in accordance with Section II (A) must follow the specific procedures relating to Systems in the USEIC Data Protection Procedures.

F. Additional Protections for Email Systems

Each email System Owner shall ensure that, in addition to the protections described in Section C and, if applicable, Sections D and E above, the following protections are implemented for such System:

1. Virus, spam, and phishing protection for inbound and outbound messages is implemented through the use of mail filtering software that includes features such as content analysis and real time blacklists.
2. SMTP relay is performed only for authenticated Users or Systems.
3. Monitoring to detect compromised email accounts is implemented and such accounts are disabled on a timely basis.
4. Data loss prevention is implemented to ensure that unencrypted Sensitive Data are transmitted only within the Organizational Network.
5. Detection or prevention mechanisms are implemented to monitor the use of automatic forwarding, redirection or other automated delivery of email as required by the USEIC Email Usage Policy.

G. Waivers and Exemptions

Any System Owner may request that a System that contains Sensitive Data but cannot use encryption because of technology or business limitations be granted a waiver of the provisions of this Policy by the DPO. Such a waiver may only be granted if the DPO determines that there are compensating controls in place to address all major information security risks.

H. Supplemental Requirements

The requirements lists set forth in this Policy are not comprehensive and supplemental controls may be required by the Organization to enhance security as necessary.