Revision History

Version	Date
Registration and Protection of Endpoints Policy, 1.0	29 July 2021

REGISTRATION AND PROTECTION OF ENDPOINTS POLICY

I. Introduction

This Policy describes the requirements for security controls to protect Endpoints 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).

No distinction is made in this Policy between an Endpoint owned by the Organization, or one personally owned. All Information Security Policies will apply to a personally owned Endpoint used for organizational business.

Any Endpoint that processes, transmits and/or stores Organizational Data must have the minimum protection requirements set forth in Section II(A) or (B) and, if applicable, Sections II(C), for the most restricted class of Organizational Data that is processed, transmitted, or stored on such Endpoint.

Capitalized terms used herein without definition are defined in the Charter.

II. Policy

A. General Protection Requirements for Desktop and Laptop

Each User shall ensure that the following protections, at a minimum, are implemented for each Endpoint that is a desktop or laptop computer:

1. Access to the Endpoint is password protected and conforms to the USEIC Information Resource Access Control and Log Management Policy.
2. The Endpoint is running vendor-supported operating systems that are automatically updated and has up-to-date security patches installed.
3. A firewall is activated and configured on the Endpoint.
4. Anti-virus, anti-spyware and monitoring programs are installed to perform continuous and/or scheduled scanning to detect and/or prohibit unauthorized access. The virus definition list is updated at least once daily.
5. The Endpoint is configured to lock after 15 minutes of inactivity.
6. All Organizational Data files used for organizational purposes are backed up regularly.
7. The Endpoint is physically protected and not shared with unauthorized persons.
8. Each Endpoint that stores Organizational Data is disposed of in accordance with the USEIC Sanitization and Disposal of Information Resources Policy.

B. General Protection Requirements for Mobile Devices

Each User shall ensure that the following protections, at a minimum, are implemented for each Endpoint that is a Mobile Device:

1. Access to the Endpoint is password protected in accordance with the USEIC Information Resource Access Control and Log Management Policy.
2. The Endpoint contains a mechanism to encrypt all Organizational Data stored on the device.
3. The Endpoint is configured to lock after 5 minutes or less of inactivity.
4. The Endpoint has a mechanism for a secure remote wipe if it is lost or stolen.
5. The Endpoint erases data after 10 or fewer failed password or log in attempts.
6. Each Endpoint that stores Organizational Data is disposed of in accordance with the USEIC Sanitization and Disposal of Information Resources Policy.

In addition, it is recommended, but not required, that the Endpoint contain a device recovery mechanism using a GPS tracking system.

C. Additional Protection Requirements for Endpoints Containing Sensitive Data

Each User shall ensure that, in addition to the protections described in Section A or B above, the following protections are implemented for any Endpoint that processes, transmits and/or stores Sensitive Data:

1. A record of what Sensitive Data is stored on the Endpoint is maintained separately from the Endpoint.
2. Sensitive Data are encrypted while in transit and in storage, including such Data stored on Removable Media.
3. Only encryption technologies that are based on standard algorithms that have no inherent security flaws (e.g., AES, RSA, IDEA, etc.) are used.
4. At a minimum, a 256-bit encryption cipher key is used.
5. If the Endpoint is a desktop or laptop computer, it is encrypted leveraging full disk encryption.
6. The Endpoint does not use Peer-to-Peer Programs unless such use and the configuration of the Program are approved by the Data Protection Officer (DPO).

It is recommended, but not required, that any Confidential Data stored on an Endpoint be accounted for and be password protected while in transit or in storage.

D. Waivers and Exceptions

Any Security Manager may request that an Endpoint 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.

E. Supplemental Requirements

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