Revision History

Version	Date
External Hosting Policy, 1.0	30 July 2021

EXTERNAL HOSTING POLICY

I. Introduction

This Policy describes the requirements for appropriate and approved use of externally hosted USEIC Systems and/or Data (as each is defined in the USEIC Data Protection Charter (the "Charter")).

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

II. Policy

External hosting of Systems and/or Data can be categorized as the following models:

1. **Software as a Service (SaaS)** is a software distribution model in which applications are hosted by a vendor or service provider and made available to customers over a network, typically the Internet.
2. **Platform as a Service (PaaS)** is a way to rent hardware, operating systems, storage, and network capacity over the Internet. The service delivery model allows the customer to rent virtualized servers and associated services for running existing applications or developing and testing new ones.
3. **Infrastructure as a Service (IaaS)** is a provision model in which an organization outsources the equipment used to support operations, including storage, hardware, servers, and networking components. The service provider owns the equipment and is responsible for housing, running, and maintaining it.

For the purpose of this document, the term cloud computing services is used to encompass SaaS, PaaS, and IaaS

For external hosted Systems and/or Data, each System Owner shall ensure that the Systems protections described in Section B and, if applicable, Sections C, D and E of the Registration and Protection of Systems Policy are implemented as well as compliance with requirements in the Data Classification Policy.

If Sensitive Data and/or Confidential Data are stored on cloud computing services, the relevant contracts must be approved by the Data Protection Officer (DPO) and such System's protections must be assessed by the DPO prior to implementation and reassessed on a periodic basis, thereafter, as determined by the level of risk.

In addition to other organizational policies, the following requirements which must be followed in the use of cloud computing services:

Pre-requisite Requirements

A. Consult with appropriate data owners, process owners, stakeholders, and subject matter experts during the evaluation process. Also, consult with the Legal Counsel or the DPO for guidance.
B. Standard Requirements:
    1. Both the Organization and vendor must declare the type of Data that they might transfer back and forth because of their relationship. A contract must have clear terms that define the Data owned by each party. The parties also must clearly define Data that must be protected.

2. The contract must specifically state what Data the Organization owns. It must also classify the type of Data shared in the contract according to the USEIC Data Classification Policy requirements. Staff must exercise caution when sharing Sensitive or Confidential Data (as defined by the USEIC Data Classification Policy) within a cloud computing service.
3. The contract must specify how the vendor can use Organizational Data. Vendors cannot use Organizational Data in any way that violates the law or the Organization's policies.

C. Ensure a Service Level Agreement (SLA) with the vendor exists that requires:
- Clear definition of services;
- Agreed upon service levels;
- Performance measurement;
- Problem management;
- Customer duties;
- Disaster recovery;
- Termination of agreement;
- Protection of sensitive information and intellectual property; and
- Definition of vendor versus customer responsibilities, especially pertaining to backups, incident response, and data recovery.
- Cloud computing services should not be engaged without developing an exit strategy for disengaging from the vendor and/or service while integrating the service into normal internal business practices and/or business continuity and disaster recovery plans. The Organization must determine how Data would be recovered from the vendor.
- A proper risk assessment must be conducted by the DPO prior to any third-party hosting or cloud computing service arrangement.

Intellectual property and copyright materials

- USEIC marks, images, and symbols are owned by USEIC and may not be used or reproduced without the permission of USEIC.
- Users must understand the appropriate use of intellectual property including copyrights, trademarks, and patents.

Privacy and data security

- Information that the Organization has classified as "Sensitive Data", "Confidential Data", "Internal Data", or "Public Data" may be used only in accordance with the policy related to the classification of information which may be found in the USEIC Data Classification Policy.
- Personally Identifiable Information (PII) may only be used in compliance with information protected by national and international laws and regulations or industry standards, such as PDPA and GDPR.
- Customer information may only be used in compliance with PDPA guidelines.

Data availability and records retention

- Ensure that all financial, administrative, or related data are retained according to the records retention requirements.
- Back-up data regularly to ensure that records are available when needed, as many providers assume no responsibility for data-recovery of content.

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.