Revision History

Version	Date
Acceptable Usage of Information Resources Policy, 1.0	29 July 2021

ACCEPTABLE USAGE OF INFORMATION POLICY

I. Introduction

This Policy establishes the accountability of all Users (as defined in the USEIC Data Protection Charter (the "Charter")) of USEIC's Information Resources. It addresses the confidentiality, integrity, and availability of such Resources in support of the Organization's missions, codifies appropriate usage and establishes the need for Users to respect the rights of others and to be in compliance with other organizational policies, policies of external networks and resources, and all applicable national and international laws and regulations.

The Organization's Information Resources are provided to support the missions of the Organization and its supporting administrative functions.

Inappropriate use of these Information Resources threatens the atmosphere for the sharing of information, the free exchange of ideas and the security of an environment for creating and maintaining Information Resources.

This Policy applies to the access and use of the Organization's Information Resources, whether originating from Organization or non-Organization Information Resources, including personal computers, as well as the access and use of Information Resources provided by customers or vendors to, or leased or hired by, Organization Users.

Additional terms apply to the use of email at the Organization, as described in the USEIC Email Usage Policy.

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

II. Policy

A. Privacy Expectations

The Organization respects the privacy of individuals and maintains User files and emails on central Organizational Systems as private as possible. However, to protect the integrity of its Information Resources and the rights of all Users, the Organization reserves the right to monitor access to Information Resources, communications on the Organizational Network and use of Systems and Organizational Data, as described in more detail in Section III(C) of the Charter.

For reasons relating to compliance, security, or legal proceedings (e.g., subpoenas) or in an emergency or in exceptional circumstances, the Executive Management may authorize the reading, blocking, or deleting of Organizational Data. In particular, in the context of a litigation or an investigation, it may be necessary to access Organizational Data with potentially relevant information. Any such action taken must be immediately reported to the Executive Management.

B. Prohibited Actions

No User of Information Resources may take any of the following actions:

1. Use Information Resources in violation of the Data Protection Policies;
2. Violate any organizational policies or procedures or use Information Resources for unethical, illegal, or criminal purposes;
3. Violate the privacy of co-workers, or customers;
4. Violate the rights of any person protected by copyright, trade secret, patent or other intellectual property or similar laws and regulations (i.e., installing or distributing pirated or other inappropriately licensed software);
5. Copy, distribute or transmit copyrighted materials unless authorized;
6. Obstruct Organization work by consuming excessive amounts of Network bandwidth and other System resources or by deliberately degrading performance of a computer;
7. Create any program, web form or other mechanism that asks for a USEIC user identity and password other than user authentication mechanisms authorized by the Data Protection Officer;
8. Intimidate, harass, threaten, or otherwise do harm to other Users or internal or external Information Resources;
9. Transmit materials in violation of the Organization's Human Resources policies;
10. Make offers of products, items or services that are fraudulent;
11. Intentionally cause a security incident (e.g., log into an account or access Organizational Data that the User is not authorized to access, etc.);
12. Intercept or monitor Organizational Data not intended for the User unless specifically authorized by the Data Protection Officer;
13. Attempt to avoid the User authentication or security of Systems or Endpoints;
14. Allow any unauthorized person to use the Organization's computers for personal use;
15. Violate the policies of external networks and resources while using such external resources;
16. Create or intentionally release computer viruses or worms or otherwise compromise a computer;
17. Engage in frivolous, disruptive, or inconsiderate conduct in computer labs or terminal areas;
18. Use an Organizational Network to gain unauthorized access to a System or Organizational Data or to escalate privileges on a System; or
19. Use Information Resources for commercial purposes, except when explicitly approved by the applicable Executive Manager. Prohibited uses include, but are not limited to, development of programs, data processing or computations for commercial use, preparation and presentation of advertising material and the running of a Server connected to the Organizational Network.

C. Required Actions

Each User of Information Resources must take the following actions:

1. Ensure that his/her account or password is properly used and is not transferred to or used by another individual;
2. Log off from a System or Endpoint after completing access at any location where such System or Endpoint may potentially have multiple Users;
3. Ensure that Sensitive Data is protected with a password and encrypted while in transit or storage;
4. Report the loss or theft of any Endpoint or System containing Sensitive Data in accordance with the USEIC Electronic Data Security Breach Reporting and Response Policy;
5. Use Organizational Email Systems only in compliance with the USEIC Email Usage Policy; and
6. Take responsibility for any traffic that appears on the Organizational Network that originates from a network jack assigned to such User or from his/her wireless device(s) and/or network(s).