University of Prince Edward Island	**Policy No.** admitgnl0001	**Revision No.** 0
Policy Title: UPEI Electronic Information and Systems		**Page 1 of 8**
Creation Date: September 26, 2023	**Version Date:** September 26, 2023	**Review Date:** September 26, 2028
Policy Approval Authority: Board of Governors	**Designated Executive Officer:** Chief Information Officer	**WWW Access:** Yes

1. Purpose

The purpose of this Policy is to establish the responsibilities of members of the University community with respect to the acceptable use and security of the University's electronic information and the services, devices and facilities that store or transmit the University's electronic information.

2. Scope

This Policy applies to all University faculty, staff and students, as well as contractors or agents engaged by the University or any individual or organization who uses UPEI's Electronic Information and Systems, whether on-campus or remotely.

3. Definitions

3.1. **ITS Standards** mean standard operating procedures issued by the Chief Information Officer

3.2. **Systems** mean the services, devices, and facilities that are used to store, process or transmit electronic information. These include, but are not limited to:

3.2.1. computers and computer facilities;

3.2.2. computing hardware and equipment including servers, routers, and switches;

3.2.3. software including any and all desktop, server-based or cloud technologies;

3.2.4. mobile computing devices such as laptop computers, smartphones, and tablet computers;

3.2.5. electronic storage media such as CDs, USB memory sticks, and portable hard drives;

3.2.6. communications gateways and networks;

3.2.7. email systems;

3.2.8. telephone and other voice systems;

3.2.9. printers;

3.2.10. faxes;

3.2.11. building controls, radio systems and video surveillance.

3.3. **Unit** means a department, faculty, school, centre or institute of the University.

3.4. **Unit Head** means the head of a Unit including a head of an academic department, a director of a non-teaching unit or department, a director of a centre, institute or school, a dean, an associate vice-president, or the registrar, as the case may be.

3.5. **UPEI** or the **University** means the University of Prince Edward Island.

3.6. **UPEI Electronic Information** means electronic information needed to conduct University Business.

3.7. **UPEI Electronic Information and Systems** includes UPEI Electronic Information and UPEI Systems as defined herein.

3.8. **UPEI Systems** means Systems that are owned, leased or provided by the University.

3.9. **University Business** means activities in support of the administrative, academic, and research mandates of the University.

3.10. **University Executive** is currently defined as the President, Vice-President, Academic and Research, Vice-President Finance and Administration, Vice-President, People and Culture, and Chief Information Officer.

3.11. **Users** means University faculty, staff, students, as well as contractors or agents engaged by the University, or any individual or organization using UPEI Electronic Information and Systems, whether on-campus or remotely.

4. Responsibilities

4.1. This Policy is authorized by the Board of Governors.

4.2. The development, maintenance, implementation, administration and support of this Policy is the responsibility of the Chief Information Officer (CIO). Further, the CIO is responsible for:

4.2.1. developing and issuing the Information Technology and Security Standards (ITS Standards) and procedures, which shall be consistent with this Policy;

4.2.2. publishing the ITS Standards on the UPEI website for access by all Users;

4.2.3. reviewing the ITS Standards every two years, or at such other interval as the CIO determines appropriate.

4.3. The day-to-day administration of this Policy is the responsibility of the Unit Heads. These responsibilities include:

4.3.1. ensuring, as appropriate or required, that UPEI Electronic Information within their area of responsibility is maintained, transmitted, and stored in a secure and consistent manner that adheres to all relevant University policies and the ITS Standards;

4.3.2. authorizing access for individuals to UPEI Electronic Information and Systems within their area of responsibility;

4.3.3. renewing, retiring, and revoking User authorizations within their area of responsibility;

4.3.4. ensuring that, after consultation with the CIO or the CIO's designate, for appropriate application of technology and process, and other relevant departments, a business continuity plan is in place for the Unit to operate in the event of a UPEI Systems outage;

4.3.5. ensuring that breaches and potential breaches of this Policy occurring within their Unit are resolved and/or referred to the appropriate authority as provided in this Policy, and that where they are so referred, continuing to assist the investigation, preserving evidence where required;

4.3.6. ensuring that staff within their Unit are aware of and adhere to this Policy, and that they support the ITS Standards in the design, installation, maintenance, training, and use of UPEI Electronic Information and Systems;

4.3.7. working with UPEI Information Technology Systems and Services to make training and other information and resources necessary to support this Policy available to Users in their Unit;

4.3.8. taking immediate and appropriate action, as provided in this Policy, when they become aware of violations of this Policy, its procedures, or the ITS Standards.

5. Policy

General

5.1. All Users of UPEI Electronic Information and Systems are responsible for using them appropriately, responsibly and in accordance with this Policy, and maintaining their security.

Acceptable Use of UPEI Electronic Information and Systems

5.2. UPEI Electronic Information and Systems may only be used in a manner that is consistent with:

5.2.1. all applicable laws and regulations including, but not limited, to the *Criminal Code of Canada*, the Canadian *Copyright Act*, the P.E.I. *Freedom of Information and Protection of Privacy Act* and the P.E.I. *Human Rights Act*;

5.2.2. this Policy and other applicable University Policies;

5.2.3. the collective agreements with faculty and staff;

5.2.4. the terms of employment applicable to non-unionized staff;

5.2.5. the ITS Standards

5.3. **Personal Use**

Incidental personal use of UPEI Systems is acceptable provided that such use does not interfere with the User's job performance and is not a prohibited use as set out in paragraph 5.4 of this Policy or conflict with any other University Policy. Except for the foregoing, UPEI Electronic Information and Systems may only be used for University Business.

5.4. **Prohibited Use**

Prohibited uses of UPEI Electronic Information and Systems are any uses that disrupt or interfere with the use of the resources for their intended purpose. The following are representative examples of prohibited uses:

5.4.1. breaching applicable laws;

5.4.2. breaching University Policies;

5.4.3. sending threatening, harassing or discriminatory messages;

5.4.4. misrepresenting the User's identity as sender of messages;

5.4.5. intercepting or examining the content of messages, files, or communications without authorization;

5.4.6. infringing upon the copyright of computer programs, data compilations and all other works (literary, dramatic, artistic or musical);

5.4.7. infringing upon the legal protection provided by trademark law and the common law for names, marks, logos, and other representations that serve to distinguish the goods or services of one person from another;

5.4.8. making unauthorized copies of proprietary software, or offering unauthorized copies of proprietary software to others;

5.4.9. failing to maintain the confidentiality of passwords, access codes or identification numbers used to access UPEI Electronic Information and Systems;

5.4.10. seeking information on passwords or information belonging to another User without authorization;

5.4.11. accessing or examining other accounts, files, programs, communications or information without authorization;

5.4.12. destroying, altering, dismantling, disfiguring or disabling UPEI Electronic Information and Systems without authorization;

5.4.13. damaging or altering the hardware or physical components of UPEI Electronic Information and Systems without authorization;

5.4.14. attempting to circumvent security controls on UPEI Electronic Information and Systems without authorization;

5.4.15. knowingly introducing malware;

5.4.16. engaging in any uses that result in the loss of another User’s information without authorization.

5.5. Any breach under paragraph 5.4 must be immediately reported to the CIO and the Vice-President responsible for the area affected by the breach or the President.

5.6. Nothing in paragraph 5.4 shall be construed as preventing or restricting duly authorized system administrators or other authorized personnel or contractors from carrying out their duties.

Security of UPEI Electronic Information and Systems

5.7. All Users must comply with the ITS Standards established under this Policy regarding the security of UPEI Electronic Information and Systems.

5.8. Any User or Unit that seeks to deviate from the ITS Standards are required to obtain written authorization of the CIO before proceeding.

5.9. Where the ITS Standards do not address the reasonable requirements of a User or Unit's use of and access to UPEI Electronic Information and Systems, the Unit Head may submit a request to review the ITS Standards to the CIO.

5.10. A User or Unit that seeks to deviate from the ITS Standards is required to obtain written authorization of the CIO before proceeding.

6. Use of Non-University Systems for University Business

6.1. To maintain the security of UPEI Electronic Information, Users intending to conduct University Business using Systems other than UPEI Systems must do so in accordance with the ITS Standards. If the User's intended use is not considered under the ITS Standards or under this Policy, the User must obtain the CIO's approval before proceeding. The CIO may reject the request if the intended use goes against this Policy.

7. Privacy of Users

7.1. Since paragraph 5.3 of this Policy allows the incidental personal use of UPEI Systems, the University recognizes that these resources may contain records relating to personal use, e.g. personal emails, documents, voicemails, text messages, and records of internet and social media use (Personal Use Records).

7.2. While the University takes reasonable measures to back up information and protect it from loss, the University cannot guarantee that Personal Use Records will be retained in the UPEI Systems. Users are encouraged to store them separately from UPEI Electronic Information and back them up on a regular basis.

7.3. Users should understand that the University routinely monitors network transmission patterns such as source/destination, address/port, flags, packet size, packet rate, and other indicia of traffic on UPEI Systems. University system administrators and other technical personnel also perform routine maintenance of UPEI Systems. This routine monitoring and maintenance may unintentionally reveal Personal Use Records.

7.4. The University may access Users' records in relation to University Business in accordance with the procedure set out in the ITS Standards.

7.5. The University will only intentionally access, use or disclose Personal Use Records in accordance with the procedure set out in the ITS Standards.

7.6. Users should be aware that electronic information may still be retrievable even if it has been deleted by the User.

7.7. The University may, in accordance with this Policy, retrieve or reconstruct Personal Use Records generated, stored, or maintained on UPEI Systems even after they have been deleted.

8. Non-Compliance

8.1. If a User becomes aware that UPEI Electronic Information and Systems are not being used appropriately, the User shall bring this to the attention of the relevant Unit Head or to the CIO so that appropriate action can be taken to address the situation.

8.2. Users who breach this Policy may be subject to the full range of disciplinary actions under UPEI Policies, UPEI faculty and staff collective agreements and prevailing legislation. In addition to any other sanctions that the University may impose in the event of a violation, the University may restrict or withdraw the User’s access to UPEI Electronic Information and Systems, including computing privileges and network access.

9. CIO Authority

9.1. The CIO or the CIO’s designate have the authority to investigate suspected or alleged non-compliance with this Policy or the ITS Standards on behalf of the University. The CIO will assess the significance of any alleged non-compliance, and determine a course of action through consultation with appropriate University Executive. Serious non-compliance will be referred to the appropriate disciplinary body or process, in accordance with UPEI Policies, UPEI faculty and staff collective agreements and prevailing legislation.

9.2. The CIO or the CIO’s designate have the authority to enact emergency measures, the sole purpose of which is to contain a serious situation or mitigate a serious risk. Examples of such situations include, but are not limited to:

9.2.1. damage to University property has occurred or is likely to occur;

9.2.2. the integrity of the campus network or computing infrastructure is in jeopardy;

9.2.3. an individual's personal safety, or the privacy of personal or confidential information, is threatened;

9.2.4. there has been an alleged violation of the law.

9.3. Immediate emergency measures may include immediate restriction in or a complete suspension of a User’s access to UPEI Electronic Information and Systems, and/or disconnection of a system or device which threatens the security or integrity of UPEI Electronic Information and Systems. Such measures will remain in effect until it has been determined that the non-compliance has been appropriately dealt with and any risks have been mitigated or eliminated.

9.4. The CIO will report to the President or the President’s designate all instances of emergency measures taken as soon as it is reasonable to do so.

10. Review

10.1. This Policy is to be reviewed every five (5) years.