The University of British Columbia Board of Governors	**Policy No.:** **SC14**
Long Title: Acceptable Use and Security of UBC Electronic Information and Systems	
Short Title: **Information Systems Policy**	

Background & Purposes:

This policy is intended to outline the responsibilities of members of the University community with respect to the acceptable use and security of University electronic information and the services, devices and facilities that store or transmit this information.

The Responsible Executive may adopt standards and procedures consistent with this policy, all of which are posted at http://cio.ubc.ca/securitystandards. In addition, faculties and departments may adopt implementation procedures that reflect local circumstances, provided they too are consistent with this policy.

The University is committed to the principle of academic freedom. This policy should be interpreted in that context.

Nothing in this policy should be interpreted in a manner that is inconsistent with the University's legal obligations, including its obligations under collective agreements with faculty and staff and the terms of employment applicable to non-unionized staff.

1. General

1.1 All Users of UBC Electronic Information and Systems are responsible for using them appropriately and maintaining their security.

1.2 The Chief Information Officer or delegate (the "**CIO**") shall perform a coordinating role in the implementation, administration, and support of this policy by:

1.2.1 providing guidance on compliance with the policy;

1.2.2 providing an ongoing security awareness program; and

1.2.3 assisting, where appropriate, in the investigation of breaches and potential breaches of the policy.

1.3 If a User becomes aware that UBC Electronic Information and Systems are not being used appropriately, the User should bring this to the attention of the relevant administrative head of unit or to the CIO so that appropriate action can be taken to address the situation.

1.4 Users who breach this policy may be subject to the full range of disciplinary actions. In addition to any other sanctions that the University may impose in the event of a violation, the University may restrict or withdraw access to UBC Electronic Information and Systems, including computing privileges and network access.

1.5 Records containing teaching materials or research information of persons teaching or carrying out research at the University are not subject to the B.C. *Freedom of Information and Protection of Privacy Act*. However, the University wishes to ensure that all UBC Electronic Information, including teaching materials and research information, is properly secured and the integrity of UBC Systems is maintained. Therefore, this policy applies to all UBC Electronic Information, except as otherwise provided by paragraph 1.6.

1.6 Where a UBC System is not intended to be used for University Business, the CIO must, in consultation with the Office of the University Counsel, approve separate terms of use that govern the use of such system. Upon such approval, this policy will not apply to such system.

2. Acceptable Use of UBC Electronic Information and Systems

2.1 UBC Electronic Information and Systems may only be used in a manner that is consistent with:

2.1.1 applicable laws, including but not limited to the Canadian *Criminal Code*, the Canadian *Copyright Act*, the B.C. *Civil Rights Protection Act*, the B.C. *Freedom of Information and Protection of Privacy Act,* and the B.C. *Human Rights Code*;

2.1.2 this policy and other applicable University policies, including but not limited to the Discrimination Policy, the Respectful Environment Statement, and the Records Management Policy;

2.1.3 collective agreements with faculty and staff; and

2.1.4 the terms of employment applicable to non-unionized staff.

2.2 Incidental personal use of UBC Electronic Information and Systems is acceptable provided that such use does not interfere with the User's job performance and is not a prohibited use as per paragraph 2.3 of this policy. Except for the foregoing, these resources may only be used for University Business.

2.3 Prohibited uses of UBC 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:

2.3.1 breaching applicable laws or University policies;

2.3.2 sending threatening, harassing or discriminatory messages;

2.3.3 misrepresenting the User's identity as sender of messages;

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

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

2.3.6 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;

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

2.3.8 failing to maintain the confidentiality of passwords, access codes or identification numbers used to access UBC Electronic Information and Systems;

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

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

2.3.11 destroying, altering, dismantling, disfiguring or disabling UBC Electronic Information and Systems without authorization;

2.3.12 damaging or altering the hardware or physical components of UBC Systems without authorization;

2.3.13 attempting to circumvent security controls on UBC Electronic Information and Systems without authorization;

2.3.14 knowingly introducing a worm or virus; and

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

2.4 Nothing in paragraph 2.3 shall be construed as preventing or restricting duly authorized system administrators or other technical personnel from carrying out their duties.

3. Security of UBC Electronic Information and Systems

3.1 All Users must comply with the Information Security Standards established under this policy regarding the security of UBC Electronic Information and Systems.

3.2 The CIO is responsible for:

3.2.1 developing and issuing the Information Security Standards, which must be consistent with this policy;

3.2.2 publishing the Information Security Standards on the UBC Information Technology web site for access by all Users; and

3.2.3 reviewing the Information Security Standards on a bi-annual basis or at such other interval as the CIO determines.

3.3 A committee (the "**Advisory Committee**") will be established by the CIO and will consist of representatives from the Office of the University Counsel, Human Resources, Faculty Relations, and the units responsible for maintaining and/or operating significant UBC Electronic Information and Systems. The Advisory Committee will provide advice to the CIO on the development of and ongoing updates to the Information Security Standards and will also provide advice to the relevant Responsible Executive with respect to any disagreements referred to him or her pursuant to paragraph 3.6 of this policy. In developing the Information Security Standards, the Advisory Committee and the CIO must consider best practices, resource availability and implementation schedules.

3.4 Academic and administrative units that wish to deviate from the Information Security Standards are required to request the authorization of the CIO before proceeding.

3.5 Where the Information Security Standards do not address the reasonable requirements of a unit's use of and access to UBC Electronic Information or Systems, the CIO may authorize a variance or update the Information Security Standards as appropriate.

3.6 If a disagreement arises and cannot be resolved in a timely manner between the CIO and the head of an academic or administrative unit in respect of the requested deviation then either party may refer the disagreement to the relevant Responsible Executive, who will decide the matter. This Responsible Executive may consult with the Advisory Committee and/or the other Responsible Executive if he or she determines it would be appropriate to do so.

4. Use of Non-University Systems for University Business

4.1 To maintain the security of UBC Electronic Information, Users intending to conduct University Business using systems other than UBC Systems must do so in accordance with the Information Security Standards.

5. Privacy of Users

5.1 Since paragraph 2.2 of this policy authorizes the incidental personal use of UBC Electronic Information and Systems, the University recognizes that these resources may contain records relating to this personal use, e.g. personal emails, documents, voicemails, text messages, and records of internet and social media use (the "**Personal Use Records**").

5.2 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 UBC Systems or remain confidential. To protect their Personal Use Records from inadvertent access, disclosure or destruction, Users are encouraged to store them separately from UBC Electronic Information and back them up on a regular basis. Where Users intermingle Personal Use Records with UBC Electronic Information, they increase the risk that the University will unintentionally access the Personal Use Records in the course of accessing UBC Electronic Information for University Business purposes.

5.3 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 UBC Systems. University system administrators and other technical personnel also perform routine maintenance of UBC Systems. This routine monitoring and maintenance may unintentionally reveal Personal Use Records.

5.4 The University will not intentionally access, use or disclose Personal Use Records unless it has the consent of the User, or:

5.4.1 securing the User's consent would compromise (a) the health or safety of an individual or a group of people, (b) the availability or accuracy of the information, or (c) an investigation or a proceeding related to a breach of law or policy or the employment of the User;

5.4.2 such access has been authorized by the head of the relevant unit and the University Counsel, or their delegates, in accordance with the procedure set out in the Information Security Standards; and

5.4.3 the University is legally authorized to do so.

5.5 Notwithstanding anything in paragraph 5.4, the University will take such actions as are necessary to comply with any legal obligations.

5.6 Users should be aware that electronic information does not necessarily disappear after it has been deleted. The University may, in accordance with this policy, retrieve or reconstruct Personal Use Records generated, stored, or maintained on UBC Systems even after they have been deleted.

6. Administrative Responsibilities

6.1 Administrative heads of unit are responsible for establishing and maintaining UBC Electronic Information and Systems within their areas of responsibility. These responsibilities include:

6.1.1 ensuring that UBC Electronic Information and Systems are secured with adequate controls, with particular care concerning User identification and validation measures;

6.1.2 ensuring, as appropriate or required, that UBC 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 standards;

6.1.3 authorizing access for individuals to UBC Electronic Information and Systems within their area of responsibility;

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

6.1.5 ensuring that a contingency plan, including appropriate data back-up systems and recovery systems, is being used within their unit;

6.1.6 ensuring that breaches and potential breaches of this policy occurring within their unit are resolved and/or referred to the CIO, as appropriate, and that where they are so referred, continuing to assist in the investigation, preserving evidence where required;

6.1.7 ensuring that technical staff within their unit are aware of and adhere to this policy, and that they support University standards in the design, installation, maintenance, training, and use of UBC Electronic Information and Systems;

6.1.8 working with UBC Information Technology to make training and other information and resources necessary to support this policy available to Users in their unit; and

6.1.9 taking immediate and appropriate action when they become aware of violations of this policy or its procedures.

7. Definitions

7.1 *"***Academic Freedom***"* is defined in the UBC Vancouver and UBC Okanagan calendars.

7.2 "**UBC Electronic Information***"* is electronic information needed to conduct University Business.

7.3 *"***UBC Electronic Information and Systems***"* includes UBC Electronic Information and UBC Systems.

7.4 *"***UBC Systems***"* are services, devices, and facilities that are owned, leased or provided by the University, and that are used to store, process or transmit electronic information. These include, but are not limited to:

7.4.1 computers and computer facilities;

7.4.2 computing hardware and equipment;

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

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

7.4.5 communications gateways and networks;

7.4.6 email systems;

7.4.7 telephone and other voice systems; and

7.4.8 software.

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

7.6 *"***Users***"* are faculty, staff, students, and any other individuals who use UBC Electronic Information and Systems.