The University of British Columbia Board of Governors	**Policy No.:** **104**	**Approval Date:** [April 2013 Anticipated]
	Responsible Executive: Vice-President, Academic and Provost Deputy Vice-Chancellor (UBC Okanagan)	

Title:

Acceptable Use and Security of UBC Electronic Information and Systems

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. In addition, faculties and departments may adopt implementation procedures that reflect local circumstances, provided they too are consistent with this policy.

1. General

1.1. Faculty, staff and students rely on UBC Electronic Information and Systems for academic, research and administrative purposes. Users of these resources 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 in the investigation of 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. The CIO may designate UBC Systems to which this policy does not apply. Where the CIO determines that such a designation is appropriate, the CIO must, in consultation with the Office of the University Counsel, approve separate terms of use that govern the use of the designated UBC Systems.

2. Acceptable Use of UBC Electronic Information and Systems

2.1. The University does not and will not attempt to limit the Academic Freedom of those who use UBC Electronic Information and Systems, provided that Users utilize these resources 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 and Harassment Policy 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. UBC Electronic Information and Systems may only be used for their intended purposes. Incidental personal use of these resources is acceptable provided that such use:

2.2.1. does not interfere with the User's job performance; and
2.2.2. is not an unacceptable use as per paragraph 2.3 of this policy.

2.3. Unacceptable 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 unacceptable uses:

2.3.1. engaging in illegal activities;
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 in transit;
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;
2.3.10. accessing or examining other Users' accounts, files, programs, communications or information;
2.3.11. destroying, altering, dismantling, disfiguring or disabling UBC Electronic Information and Systems;
2.3.12. damaging or altering the hardware or physical components of UBC Systems;
2.3.13. attempting to circumvent security controls on UBC Electronic Information and Systems;
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.

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 acceptable use and 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 units responsible for maintaining and/or operating significant UBC Electronic Information and Systems, as well as a representative of the Office of the University Counsel. 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.

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 deviation or update the Information Security Standards as appropriate.

3.6. If a disagreement arises and cannot be resolved informally 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, University business must only be conducted using UBC Systems, except as otherwise permitted by 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, internet use logs and voicemails (the "Personal Use Records").

5.2. While the University takes reasonable measures to back up information and protect it from loss, the University does not warrant that Personal Use Records will be retained in the UBC Systems or remain confidential. To protect their Personal Use Records from inadvertent destruction or disclosure, Users are encouraged to clearly mark them as personal, store them separately from UBC Electronic Information, and back them up on a regular basis.

5.3. While the University does not, as a routine matter, review Personal Use Records generated, stored, or maintained on UBC Systems, the University retains the right to inspect, review, or retain the Personal Use Records for legitimate University purposes. These purposes include, but are not limited to:

5.3.1. responding to lawful subpoenas or court orders;
5.3.2. investigating misconduct and determining compliance with University policies; and
5.3.3. searching for electronic messages, data, files, or other records that are required for University business continuity purposes.

5.4. Users should understand that electronic information does not necessarily disappear after it has been deleted. The University may, in accordance with paragraph 5.3 of this policy, retrieve or reconstruct records from UBC Systems, which may include Personal Use Records, even after they have been deleted.

5.5. Users should also be aware 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 its networks and systems. This routine monitoring may inadvertently reveal information about the personal use of the UBC Electronic Information and Systems.

5.6. Except in emergencies or other unusual situations, the University will seek the consent of a User before intentionally accessing his or her Personal Use Records. If the University is required to gain access without the individual's consent, such access must be authorized by the head of the relevant unit and the CIO, in accordance with the procedure set out in the Information Security Standards.

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 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;
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; and
6.1.8. 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. *Confidential* UBC Electronic Information is information that is highly sensitive. This includes, but is not limited to:

7.2.1. personal information (not including the name and business contact information of faculty and staff members);
7.2.2. financial information; and
7.2.3. information the release of which could reasonably be expected to harm the security of individuals, systems or facilities.

7.3. *Information Security Standards* means the standards established under this policy regarding the acceptable use and security of UBC Electronic Information and Systems. The Information Security Standards are published on the UBC Information Technology Office website at: http://www.it.ubc.ca/sites/it.ubc.ca/files/uploads/__shared/assets/UBC_Information_Security_Manual.pdf.

7.4. *Sensitive* UBC Electronic Information is information that is not Confidential, but cannot be released to the general public. This includes, but is not limited to:

7.4.1. information supplied in confidence;
7.4.2. research data that does not contain Confidential information;
7.4.3. information relating to plans, projects or proposals that have not been made public; and
7.4.4. contractually protected information, such as electronic library resources.

7.5. *UBC Electronic Information* is electronic information needed to conduct University business (administrative, academic or research).

7.6. *UBC Electronic Information and Systems* includes UBC Electronic Information and UBC Systems.

7.7. *UBC Systems* are services, devices and facilities that are owned or leased by the University, that are used for a University purpose, and that store or transmit UBC Electronic Information. These include, but are not limited to:

7.7.1. computers and computer facilities;
7.7.2. computing hardware and equipment;
7.7.3. mobile computing devices such as laptop computers, smartphones and tablet computers;
7.7.4. electronic storage media such as CDs, USB memory sticks and portable hard drives;
7.7.5. communications gateways and networks;
7.7.6. email systems;
7.7.7. telephone and other voice systems; and
7.7.8. software.

7.8. *Users* are faculty, staff, students and any other individuals who have access to UBC Electronic Information and Systems.