



---

<b>SUBJECT</b>	Proposed Amendments to the Information Systems Policy (SC14) and Wireless Network Policy (SC11)
<b>SUBMITTED TO</b>	Audit Committee
<b>MEETING DATE</b>	November 24, 2025
<b>SESSION CLASSIFICATION</b>	Recommended session criteria from Board Meetings Policy: OPEN
<b>REQUEST</b>	For input only - No action requested
<b>LEAD EXECUTIVE</b>	Hubert Lai, K.C., University Counsel
<b>SUPPORTED BY</b>	Gage Averill, Provost and Vice-President, Academic (UBC Vancouver) Lesley Cormack, Deputy Vice-Chancellor and Principal (UBC Okanagan) Erika Brimacombe, Legal Counsel (Policy Development Committee Chair) Matthew Murray, Legal Counsel (Policy Development Committee Secretary)

---

#### PRIOR SUBMISSIONS

The subject matter of this submission has not been considered previously by the Audit Committee.

---

#### EXECUTIVE SUMMARY

This briefing sets out proposed amendments to the Information Systems Policy (SC14) and repeal of the Wireless Network Policy (SC11). The Audit Committee is receiving this briefing because it is anticipated that the Governance Committee, under its delegated authority from the Board of Governors, will approve the reassignment of these policies from the Learning & Research Committee to the Audit Committee, at its meeting on November 20, 2025.

The Wireless Network Policy (SC11) was first approved by the Board of Governors (the “**Board**”) on January 26, 2006. The Information Systems Policy (SC14) was first approved by the Board on June 4, 2013 through the combination of Board Policy #104 (Responsible Use of Information Technology Facilities and Services) and Board Policy #106 (Access to and Security of Administrative Information), which were repealed and replaced by the current policy.

Neither the Information Systems Policy nor the Wireless Network Policy have been substantially updated since they were approved, and there are no Procedures associated with the Policies.

The Responsible Executive for the Wireless Network Policy is the Provost and Vice-President, Academic (UBC Vancouver). The Responsible Executives for the Information Systems Policy are the Provost and Vice-President, Academic (UBC Vancouver) and the Deputy Vice-Chancellor and Principal (UBC Okanagan). The Responsible Board Committee for both Policies is currently the Learning & Research Committee.

At the request of the Responsible Executives, the Office of the University Counsel (“**OUC**”) convened a Policy Development Committee (“**PDC**”) to review both Policies and make recommendations to the Board regarding proposed amendments to them. A list of the members of the PDC is attached to this submission as **Supplemental Material 1**.

A primary objective of the PDC was to propose amendments to the Policies to align with best practices, and to ensure consistency with other Board Policies. Key elements of the PDC’s recommendations and proposed amendments are as follows:

1. **Change to Responsible Board Committee:** the PDC recommends that the Responsible Board Committee for both Policies be changed from the Learning & Research Committee to the Audit Committee. The OUC has consulted with the Chairs of the Learning & Research Committee, the Audit Committee, and the Governance Committee, all of whom are supportive. The OUC has therefore provided a separate submission to the Governance Committee to request approval of this change. In anticipation of the Governance Committee’s approval, a submission is being made to the Learning & Research Committee to ensure that it is also informed and members of the Learning & Research Committee are invited to attend the meeting of the Audit Committee, should they wish to participate in the discussion of the proposed amendments to these Policies. This submission is provided to the Audit Committee for its information and input.
2. **Cybersecurity Incidents:** the proposed amendments include obligations for reporting cybersecurity incidents and allow the Chief Information Officer (“**CIO**”) and Chief Information Security Officer (“**CISO**”) to take immediate action in response to a cybersecurity incident. The proposed amendments also require the CIO to report cybersecurity incidents that have significant reputational, operational, or financial impacts or are otherwise material, to the Responsible Executives.
3. **Reporting and Investigation of Policy Breaches:** the proposed amendments include obligations for reporting breaches of the Policy and ties into the Investigations Policy (SC8) to explicitly provide for investigations into such breaches.
4. **Office of the Chief Information Officer (“**OCIO**”):** the proposed amendments provide clarity on roles of the OCIO, CIO, and CISO in the administration of the Policy.
5. **Creation of Rules:** the proposed amendments align with the Regulatory Framework Policy (GA2) and allow the Responsible Executives, on the recommendation of the Chief Information Officer, to establish and maintain Rules related to the subject matter of the Policy and Procedures. The Rules will replace the current Information Security Standards, which will be deemed Rules under the proposed Policy, until they are amended, replaced, or repealed.
6. **Addition of Procedures:** the proposed amendments align with the Regulatory Framework Policy and include a Procedures section to provide direction regarding the operational application of the Policy.
7. **Repeal of the Wireless Network Policy:** In the view of the PDC, the subject matter of the Wireless Network Policy would be more appropriately handled as Rules established by the Responsible Executives, under the Information Systems Policy. Therefore, the PDC is recommending the repeal of the Wireless Network Policy, to be replaced by Rules under the amended Information Systems Policy.

The PDC's proposed amendments to the Information Systems Policy (SC14) are attached to this submission as **Appendix 1**. In addition, a blacklined version showing the proposed changes in comparison to the current Policy is attached as **Supplemental Material 2**.

### **Next Steps**

Subject to any feedback from the Audit Committee, the next step will be to post the proposed Information Systems Policy and the repeal of the Wireless Network Policy on the website of the OUC and in UBC Today to solicit input from the UBC community. The consultation period is expected to run for approximately one and a half months, from November 25, 2025 to January 9, 2026, for public comment by the UBC community. The PDC will reconvene after the consultation period to consider the comments received. The PDC anticipates that a final recommendation will be submitted to the Board in March 2026.


---

### **APPENDICES**

1. Proposed Amendments to the Information Systems Policy (SC14)

### **SUPPLEMENTAL MATERIAL (optional reading for Governors)**

1. List of Members of the Policy Development Committee
2. Black-line of proposed amendments to the Information Systems Policy (SC14)
3. Current version of the Wireless Network Policy (SC11)

 <p><b>The University of British Columbia Board of Governors</b></p>	<p><b>Policy No.:</b> <b>SC14</b></p>
<p><b>Long Title:</b> Acceptable Use, Management, and Security of UBC Electronic Information and Systems</p>	
<p><b>Short Title:</b> <b>Information Systems Policy</b></p>	

### Background & Purposes:

This Policy is intended to outline the responsibilities of members of the UBC community with respect to the acceptable use, management, and security of:

- electronic information that UBC controls, creates, receives, uses or maintains to conduct activities in support of the administrative, academic, and research mandates of UBC (“**UBC Electronic Information**”); and
- the services, devices, and facilities that are owned, leased or provided by UBC and are used to store, process, or transmit electronic information (“**UBC Systems**”).

Together, these are referred to as “**UBC Electronic Information and Systems**”. This Policy governs the use of UBC Electronic Information and Systems in a manner consistent with:

- 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*;
- UBC policies, including but not limited to the Discrimination Policy (SC7), Equipment/Services Use Policy (UP5), and the Records Management Policy (GA4);
- collective agreements with faculty and staff; and
- the terms of employment applicable to non-unionized staff.

## 1. General

- 1.1 This Policy applies to all users of UBC Electronic Information and Systems, including UBC students and learners (including persons registered in non-credit educational activities at UBC); all UBC employees and appointees, including staff members, student employees, faculty members, temporary or sessional instructors, clinical or honorary professors, and adjunct professors; all individuals holding UBC emeritus status; all volunteers engaged in a UBC activity; all service providers, contractors, or persons acting for or on behalf of UBC or under the auspices of UBC; guests, visitors, and anyone contractually obligated to comply with this Policy (“**Users**”).

- 1.2 Users must use UBC Electronic Information and Systems appropriately and maintain the security and integrity of UBC Electronic Information and Systems in compliance with this Policy.
- 1.3 Users may only access, use, copy, share, alter, or delete UBC Electronic Information when necessary for the performance of their UBC duties, and/or when appropriately authorized by UBC, as applicable.
- 1.4 Users must not engage in any activity that disrupts, interferes with, or impairs the intended use of UBC Electronic Information and Systems. Examples of activities that are prohibited uses are provided in the Procedures to this Policy.

### 2. Office of the Chief Information Officer

- 2.1 The Office of the Chief Information Officer (the “**OCIO**”) and the Chief Information Officer (the “**CIO**”) will perform a coordinating role in the administration of this Policy, including by providing guidance, training, and compliance support.
- 2.2 The CIO may require the suspension, restriction, or shutting down of access to UBC Electronic Information and Systems when the CIO determines it is necessary to protect the security, integrity, or lawful use of UBC Electronic Information and Systems.
- 2.3 The OCIO will address cybersecurity incidents and breaches of this Policy in accordance with the Procedures to this Policy.

### 3. Rules

- 3.1 The Responsible Executive(s) may, upon the recommendation of the CIO, issue and maintain mandatory rules (“**Rules**”) regarding the subject matter of the Policy and its associated Procedures, provided that such Rules must be consistent with the Policy or its associated Procedures. The creation of Rules is at the discretion of the Responsible Executive(s), upon the recommendation of the CIO, where the CIO believes there is benefit to enumerate detailed processes and requirements for Users. The Rules may be contained in one or more documents and may vary depending on the needs of different UBC units or types of activity or systems. The Responsible Executive(s) and the CIO do not require the existence of a Rule to exercise their authority with respect to the subject matter of this Policy and its associated Procedures.
- 3.2 Prior to creating or substantively revising the Rules, the Responsible Executive(s) will establish one or more advisory committees, which will be chaired by the CIO or their delegate(s), and consist of persons from the applicable campuses who are representative of the academic and administrative units responsible for the subject matter of the Rules and the primary UBC constituencies that would be impacted by the Rules. Any proposed new Rules or substantive amendments to existing Rules must be published publicly for a period of at least two weeks on a UBC website designated by the Responsible Executive(s) with a request for feedback to the advisory committee. The advisory committees, upon receipt and consideration of such feedback, will provide advice to the Responsible Executive(s) on the form and content of the new Rule or amended Rule.

- 3.3 Without limiting the foregoing, the Rules may include requirements for UBC Electronic Information and Systems related to:
- 3.3.1 cybersecurity;
  - 3.3.2 architectural requirements and standardization;
  - 3.3.3 management of digital identities and User access;
  - 3.3.4 adoption of artificial intelligence and other developing electronic information technologies;
  - 3.3.5 network connectivity;
  - 3.3.6 data stewardship, access, and governance.
- 3.4 Any Rules issued by the Responsible Executive(s) will be published in accordance with the Regulatory Framework Policy (GA2).
- 3.5 Where the Rules conflict with the reasonable requirements of a unit's use of and access to UBC Electronic Information and Systems, the administrative head of unit ("**Head of Unit**") may request that the Responsible Executive(s) authorize a variance or update the Rules as appropriate.
- 3.6 Information Security Standards issued by the CIO as at [date] are deemed to be Rules under this Policy and remain in effect unless and until they are amended, replaced, or repealed in accordance with this section 3.

#### 4. System Owners

- 4.1 The OCIO will maintain an inventory of all UBC Systems that:
- 4.1.1 are designated as enterprise systems;
  - 4.1.2 contain high or very-high risk UBC Electronic Information;
  - 4.1.3 are classified as part of a high or very-high risk electronic services; or
  - 4.1.4 are otherwise required by the CIO to be inventoried.
- 4.2 The inventory will include information regarding the core attributes and identify the individual with primary decision-making authority over the UBC System (the "**System Owner**"). If no System Owner is designated in the inventory, the Head of Unit with decision-making authority over the UBC System will be considered the System Owner. The OCIO may require System Owners and Users to provide information necessary to keep the inventory current.
- 4.3 System Owners must ensure that UBC Electronic Information and Systems under their authority comply with UBC policies, including:
- 4.3.1 ensuring, as appropriate or required, that UBC Electronic Information and Systems are implemented, operated, and maintained in a secure and consistent manner that adheres

to all relevant UBC policies;

- 4.3.2 ensuring that appropriate User authorizations are in place for access to UBC Electronic Information and Systems;
- 4.3.3 ensuring that User authorizations are renewed, retired, and revoked in accordance with this Policy;
- 4.3.4 ensuring that a contingency plan, including appropriate data back-up systems and recovery systems is in place;
- 4.3.5 ensuring that breaches and potential breaches of this Policy are resolved and/or referred to the OCIO in accordance with the Procedures to this Policy, and that where they are so referred, continuing to assist in the investigation, preserving evidence where required;
- 4.3.6 providing information on the relevant UBC Systems to their Head of Unit and the OCIO, upon request;
- 4.3.7 working with UBC Information Technology to make training and other information and resources necessary to support this Policy available to Users; and
- 4.3.8 taking immediate and appropriate action when they become aware of violations of this Policy or its associated Procedures.

## 5. Incidental Personal Use of UBC Systems and Personal Use Records

- 5.1 Incidental personal use of UBC Systems is acceptable provided that such use does not interfere with the User's job performance, consume an unreasonable amount of UBC resources, pose a risk to UBC Electronic Information and Systems, or is not otherwise prohibited under this Policy or any other UBC policy.
- 5.2 Since this Policy and the Equipment/Services Use Policy (UP5) permit the incidental personal use of UBC Systems, UBC recognizes that UBC Systems 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**"). Records created or stored through UBC Systems by students (e.g., UBC student email accounts) are generally considered Personal Use Records, unless used by a student in their capacity as an employee, volunteer, or researcher acting on behalf of UBC.
- 5.3 While UBC takes reasonable measures to back up information and protect it from loss, UBC 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 UBC may access the Personal Use Records in the course of accessing UBC Electronic Information for UBC business purposes.

- 5.4 Users should understand that UBC routinely monitors network transmission patterns such as source/destination, address/port, flags, packet size, packet rate, and other indicia of traffic on UBC Systems. UBC system administrators and other technical personnel also perform routine maintenance of UBC Systems. This routine monitoring and maintenance may reveal Personal Use Records.
- 5.5 UBC will not intentionally access, use or disclose Personal Use Records outside of the foregoing circumstances unless it has the consent of the User, or:
  - 5.5.1 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;
  - 5.5.2 such access has been authorized by the relevant Head of Unit and the University Counsel, or their delegate(s), in accordance with the Rules; and
  - 5.5.3 UBC is legally authorized to do so.
- 5.6 Notwithstanding the foregoing, UBC will take such actions as are necessary to comply with any legal obligations.
- 5.7 Users should be aware that electronic information does not necessarily disappear after it has been deleted. UBC 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.



## PROCEDURES ASSOCIATED WITH THE INFORMATION SYSTEMS POLICY

*Pursuant to the Regulatory Framework Policy, the President may approve Procedures or the amendment or repeal of Procedures. Such approvals must be reported at the next meeting of the UBC Board of Governors or as soon thereafter as practicable.*

*Capitalized terms used in these Procedures that are not otherwise defined herein shall have the meanings given to such terms in the accompanying Policy, being the Information Systems Policy.*

### 1. Examples of UBC Electronic Information and Systems

1.1 The following are representative examples of UBC Systems:

- 1.1.1 computers and computer facilities;
- 1.1.2 computing hardware and equipment;
- 1.1.3 mobile computing devices such as laptop computers, smartphones, and tablet computers;
- 1.1.4 electronic storage media such as CDs, USB memory sticks, and portable hard drives;
- 1.1.5 communications gateways and networks;
- 1.1.6 email systems;
- 1.1.7 telephone and other voice systems;
- 1.1.8 software, including AI-enabled applications;
- 1.1.9 Internet of Things (IoT) devices and systems;
- 1.1.10 industrial control systems (ICS) and supervisory control and data acquisition (SCADA) systems; and
- 1.1.11 cloud-hosted platforms and services.

1.2 The following are representative examples of UBC Electronic Information:

- 1.2.1 student records, including admissions, enrollment, grades, and transcripts;
- 1.2.2 personnel and employment records;
- 1.2.3 research records;

- 1.2.4 emails and messages created or received by UBC employees, service providers, or volunteers that are related to UBC business; and
- 1.2.5 content published by UBC on UBC websites.

### **2. Examples of Prohibited Use of UBC Electronic Information and Systems**

- 2.1 The following are representative examples of activities that are prohibited uses of UBC Electronic Information and Systems when not appropriately authorized by UBC:
  - 2.1.1 breaching applicable laws or UBC policies;
  - 2.1.2 sending threatening, harassing or discriminatory messages;
  - 2.1.3 misrepresenting the User's identity as sender of messages;
  - 2.1.4 intercepting or examining the content of messages, files, or communications;
  - 2.1.5 infringing upon the copyright of computer programs, data compilations and all other works (literary, dramatic, artistic or musical);
  - 2.1.6 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;
  - 2.1.7 making copies of proprietary software, or offering unauthorized copies of proprietary software to others;
  - 2.1.8 failing to maintain the confidentiality of passwords, access codes or identification numbers used to access UBC Electronic Information and Systems;
  - 2.1.9 seeking information on passwords or information belonging to another User;
  - 2.1.10 accessing or examining other accounts, files, programs, communications or information;
  - 2.1.11 destroying, altering, dismantling, disfiguring or disabling UBC Electronic Information and Systems;
  - 2.1.12 damaging or altering the hardware or physical components of UBC Systems;
  - 2.1.13 attempting to circumvent security controls on UBC Electronic Information and Systems;
  - 2.1.14 knowingly introducing malicious software such as keyloggers, worms or viruses;
  - 2.1.15 engaging in any uses that result in the loss of another User's information; and

- 2.1.16 collecting, generating, or manipulating information, including through bots, scripts, or AI agents, in a manner that threatens the security, privacy, or integrity of UBC Electronic Information and Systems.
- 2.2 Nothing in paragraph 2.1 shall be construed as preventing or restricting duly authorized system administrators or other technical personnel from carrying out their duties.

### 3. Policy Breaches



- 3.1 If a User becomes aware of a breach or potential breach of this Policy, the User must promptly report such activity to the relevant System Owner and the OCIO at [security@ubc.ca](mailto:security@ubc.ca).
- 3.2 Notwithstanding section 3.1, technical personnel who identify breaches during the performance of their support duties will assist Users and System Owners by providing guidance and corrective actions. Technical personnel must report material breaches to the System Owner and the OCIO.
- 3.3 Where the CIO, or their delegate(s), determines that an investigation is required into a breach of this Policy, the investigation will be conducted in accordance with the Investigations Policy (SC8).
- 3.4 Subject to UBC's policies, legal privilege, and any applicable legal, contractual, and privacy obligations, the CIO, or their delegate(s), in order to conduct investigations into breaches of this Policy, may:
  - 3.4.1 access any relevant UBC records or information; and
  - 3.4.2 interview Users and other individuals as necessary to gather evidence.
- 3.5 In cases where access to information may be restricted, the CIO will seek direction from the Office of the University Counsel, which will consult with Human Resources as appropriate.
- 3.6 If an employee is the subject of an investigation, or, during an interview of a UBC employee, the investigator becomes aware of potential willful breaches of this Policy by that employee, the investigator will pause the interview and consult with Human Resources.
- 3.7 Breaches of this Policy will be addressed in a manner appropriate to the circumstances, including through remediation, guidance, or corrective actions. However, UBC retains the full discretion to restrict or withdraw access to UBC Electronic Information and Systems, including computing privileges and network access, and to impose the full range of disciplinary actions on Users who are found to have breached this Policy. The degree of intent, along with along with mitigating factors such as early reporting, transparency, and full cooperation, may be considered in determining appropriate consequences, along with any other relevant factors that are normally considered in determining appropriate outcomes.

#### 4. Cybersecurity Incidents

- 4.1 A “**Cybersecurity Incident**” is any real or threatened event that could compromise the confidentiality, integrity, or availability of UBC Electronic Information and Systems, regardless of whether it involves a violation of this Policy.
- 4.2 All Users must immediately report Cybersecurity Incidents to the System Owner (if known) and the OCIO at [security@ubc.ca](mailto:security@ubc.ca).
- 4.3 The OCIO must inform the relevant System Owner of any material Cybersecurity Incidents affecting UBC Systems under the System Owner’s authority.
- 4.4 The Chief Information Security Officer (“**CISO**”) will develop and maintain a plan for responding to Cybersecurity Incidents.
- 4.5 In response to a Cybersecurity Incident, the CIO or the CISO may:
  - 4.5.1 authorize immediate and direct action, including accessing any system or information, disabling accounts, terminating network connections, or shutting down systems; and
  - 4.5.2 issue directions to Systems Owners, Heads of Unit, or other individuals to implement specific technical measures, containment procedures, or system configuration changes necessary to protect UBC Electronic Information and Systems, which must be promptly implemented.
- 4.6 Where the CIO, in consultation with the CISO, determines that a Cybersecurity Incident has significant reputational, operational, or financial impacts or is otherwise material, the CIO will promptly report it to the Responsible Executive(s).

**Information Systems Policy (SC14) and Wireless Network Policy (SC11)  
Policy Development Committee Membership**

1. Erika Brimacombe, *Legal Counsel* (Chair)
2. Matthew Murray, *Legal Counsel* (Secretary)
3. Scott Baker, *Manager, Sensitive Research, Advanced Research Computing*
4. Elisa Baniassad, *Professor of Teaching, Department of Computer Science*
5. Jennifer Burns, *Chief Information Officer*
6. Larry Carson, *Associate Director, Information Security Management*
7. Aaditya Golash, *Director-at-Large, Student Union of UBC Okanagan Nominee*
8. Jan Hare, *Dean, Faculty of Education*
9. Riley Huntley, *President, Alma Mater Society of The University of British Columbia Vancouver Nominee*
10. Anthony Knezevic, *Associate Director, IT Service Delivery*
11. Lael Parrott, *Dean, Irving K. Barber Faculty of Science*

	 <b>The University of British Columbia Board of Governors</b>	<b>Policy No.:</b> SC14
<b>Long Title:</b> Acceptable Use, <u>Management</u> , and Security of UBC Electronic Information and Systems		
<b>Short Title:</b> <b>Information Systems Policy</b>		

**Background & Purposes:**

This ~~policy~~ Policy is intended to outline the responsibilities of members of the ~~University~~ UBC community with respect to the acceptable use, management, and security of ~~University~~ :

- ~~electronic information and the services, devices and facilities that UBC controls, creates, receives, uses or maintains to conduct activities in support of the administrative, academic, and research mandates of UBC ("UBC Electronic Information"); and~~
- ~~the services, devices, and facilities that are owned, leased or provided by UBC and are used to store, process, or transmit this~~ electronic information ("UBC Systems").

~~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.~~

Field Code Changed

~~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~~ Together, these are referred to as "UBC Electronic Information and Systems". This Policy governs the 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~~ UBC policies, including but not limited to the Discrimination Policy (SC7), ~~the Respectful Environment Statement~~ Equipment/Services Use Policy (UP5), and the Records Management Policy (GA4);
- ~~2.1.3~~ collective agreements with faculty and staff; and
- ~~2.1.4~~ the terms of employment applicable to non-unionized staff.

**1. General**

1.1 This Policy applies to all users of UBC Electronic Information and Systems, including UBC students and learners (including persons registered in non-credit educational activities at UBC); all UBC employees and appointees, including staff members, student employees, faculty members, temporary or sessional instructors, clinical or honorary professors, and adjunct professors; all individuals holding UBC emeritus status; all volunteers engaged in a UBC activity; all service providers, contractors, or persons acting for or on behalf of UBC or under the auspices of UBC; guests, visitors, and anyone contractually obligated to comply with this Policy (“Users”).

1.2 Users must use UBC Electronic Information and Systems appropriately and maintain the security and integrity of UBC Electronic Information and Systems in compliance with this Policy.

~~1.3 2.2 Incidental personal use of~~ Users may only access, use, copy, share, alter, or delete UBC Electronic Information and Systems is acceptable provided that such use does not interfere with when necessary for 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 of their UBC duties, and/or when appropriately authorized by UBC, as applicable.

~~2.3 Prohibited uses~~

1.4 Users must not engage in any activity that disrupts, interferes with, or impairs the intended use 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~~ Examples of activities that are prohibited uses are provided in the Procedures to this Policy.

2. Office of the Chief Information Officer

2.1 The Office of the Chief Information Officer (the "OCIO") and the Chief Information Officer (the "CIO") will perform a coordinating role in the administration of this Policy, including by providing guidance, training, and compliance support.

2.2 The CIO may require the suspension, restriction, or shutting down of access to UBC Electronic Information and Systems

~~3.1 All Users must comply with the Information Security Standards established under this policy regarding when the CIO determines it is necessary to protect the security, integrity, or lawful use 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.~~

2.3 The OCIO will address cybersecurity incidents and breaches of this Policy in accordance with the Procedures to this Policy.

3. Rules

3.1 The Responsible Executive(s) may, upon the recommendation of the CIO, issue and maintain mandatory rules (“Rules”) regarding the subject matter of the Policy and its associated Procedures, provided that such Rules must be consistent with the Policy or its associated Procedures. The creation of Rules is at the discretion of the Responsible Executive(s), upon the recommendation of the CIO, where the CIO believes there is benefit to enumerate detailed processes and requirements for Users. The Rules may be contained in one or more documents and may vary depending on the needs of different UBC units or types of activity or systems. The Responsible Executive(s) and the CIO do not require the existence of a Rule to exercise their authority with respect to the subject matter of this Policy and its associated Procedures.

3.2 Prior to creating or substantively revising the Rules, the Responsible Executive(s) will establish one or more advisory committees, which will be chaired by the CIO or their delegate(s), and consist of persons from the applicable campuses who are representative of the academic and administrative units responsible for the subject matter of the Rules and the primary UBC constituencies that would be impacted by the Rules. Any proposed new Rules or substantive amendments to existing Rules must be published publicly for a period of at least two weeks on a UBC website designated by the Responsible Executive(s) with a request for feedback to the advisory committee. The advisory committees, upon receipt and consideration of such feedback, will provide advice to the Responsible Executive(s) on the form and content of the new Rule or amended Rule.

~~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. Without limiting the foregoing, the Rules may include requirements for UBC Electronic Information and Systems related to:~~

3.3.1 cybersecurity;

3.3.2 architectural requirements and standardization;

3.3.3 management of digital identities and User access;

3.3.4 adoption of artificial intelligence and other developing electronic information technologies;

3.3.5 network connectivity;

3.3.6 data stewardship, access, and governance.

- 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. Any Rules issued by the Responsible Executive(s) will be published in accordance with the Regulatory Framework Policy (GA2).~~
- 3.5 Where the ~~Information Security Standards do not address~~ Rules conflict with the reasonable requirements of a unit's use of and access to UBC Electronic Information ~~or and~~ Systems, the ~~CIO may~~ administrative head of unit ("Head of Unit") may request that the Responsible Executive(s) authorize a variance or update the ~~Information Security Standards~~ Rules 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~~

~~3.6 Information Security Standards issued by the CIO as at [date] are deemed to be Rules under this Policy and remain in effect unless and until they are amended, replaced, or repealed in accordance with this section 3.~~

4. System Owners

- 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. The OCIO will maintain an inventory of all UBC Systems that:~~
  - 4.1.1 are designated as enterprise systems;
  - 4.1.2 contain high or very-high risk UBC Electronic Information;
  - 4.1.3 are classified as part of a high or very-high risk electronic services; or
  - 4.1.4 are otherwise required by the CIO to be inventoried.
- 4.2 The inventory will include information regarding the core attributes and identify the individual with primary decision-making authority over the UBC System (the "System Owner"). If no System Owner is designated in the inventory, the Head of Unit with decision-making authority over the UBC System will be considered the System Owner. The OCIO may require System Owners and Users to provide information necessary to keep the inventory current.

4.3 System Owners must ensure that UBC Electronic Information and Systems under their authority comply with UBC policies, including:

4.3.1 ensuring, as appropriate or required, that UBC Electronic Information and Systems are implemented, operated, and maintained in a secure and consistent manner that adheres to all relevant UBC policies;

4.3.2 ensuring that appropriate User authorizations are in place for access to UBC Electronic Information and Systems;

4.3.3 ensuring that User authorizations are renewed, retired, and revoked in accordance with this Policy;

4.3.4 ensuring that a contingency plan, including appropriate data back-up systems and recovery systems is in place;

4.3.5 ensuring that breaches and potential breaches of this Policy are resolved and/or referred to the OCIO in accordance with the Procedures to this Policy, and that where they are so referred, continuing to assist in the investigation, preserving evidence where required;

4.3.6 providing information on the relevant UBC Systems to their Head of Unit and the OCIO, upon request;

4.3.7 working with UBC Information Technology to make training and other information and resources necessary to support this Policy available to Users; and

4.3.8 taking immediate and appropriate action when they become aware of violations of this Policy or its associated Procedures.

**5. ~~Privacy of Users~~ Incidental Personal Use of UBC Systems and Personal Use Records**

5.1 Incidental personal use of UBC Systems is acceptable provided that such use does not interfere with the User's job performance, consume an unreasonable amount of UBC resources, pose a risk to UBC Electronic Information and Systems, or is not otherwise prohibited under this Policy or any other UBC policy.

5.2 ~~5.1~~ Since ~~paragraph 2.2 of this policy authorizes~~ Policy and the Equipment/Services Use Policy (UP5) permit the incidental personal use of UBC ~~Electronic Information and~~ Systems, ~~the University~~ UBC recognizes that ~~these resources~~ UBC Systems 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**"). Records created or stored through UBC Systems by students (e.g., UBC student email accounts) are generally considered Personal Use Records, unless used by a student in their capacity as an employee, volunteer, or researcher acting on behalf of UBC.

5.3 ~~5.2~~ While ~~the University~~UBC takes reasonable measures to back up information and protect it from loss, ~~the University~~UBC 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~~UBC ~~may~~ access the Personal Use Records in the course of accessing UBC Electronic Information for ~~University Business~~UBC ~~business~~ purposes.

5.4 ~~5.3~~ Users should understand that ~~the University~~UBC 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~~UBC system administrators and other technical personnel also perform routine maintenance of UBC Systems. This routine monitoring and maintenance may ~~unintentionally~~ reveal Personal Use Records.

5.5 ~~5.4~~ ~~The University~~UBC will not intentionally access, use or disclose Personal Use Records outside of the foregoing circumstances unless it has the consent of the User, or:

5.5.1 ~~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;

5.5.2 ~~5.4.2~~ such access has been authorized by the ~~head of the relevant unit~~Head of Unit and the University Counsel, or their ~~delegates~~delegate(s), in accordance with the ~~procedure set out in the Information Security Standards~~Rules; and

5.5.3 ~~5.4.3~~ ~~the University~~UBC is legally authorized to do so.

5.6 ~~5.5~~ Notwithstanding ~~anything in paragraph 5.4, the University~~the foregoing, UBC will take such actions as are necessary to comply with any legal obligations.

5.7 ~~5.6~~ Users should be aware that electronic information does not necessarily disappear after it has been deleted. ~~The University~~UBC may, in accordance with this ~~policy~~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.~~

5.7.1



**PROCEDURES ASSOCIATED WITH THE  
INFORMATION SYSTEMS POLICY**

Pursuant to the Regulatory Framework Policy, the President may approve Procedures or the amendment or repeal of Procedures. Such approvals must be reported at the next meeting of the UBC Board of Governors or as soon thereafter as practicable.

Capitalized terms used in these Procedures that are not otherwise defined herein shall have the meanings given to such terms in the accompanying Policy, being the Information Systems Policy.

**1. ~~7.3~~ “UBC Electronic Information and Systems” includes Examples of UBC Electronic Information and UBC Systems.**

**1.1 ~~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: The following are representative examples of UBC Systems:**

- 1.1.1 ~~7.4.1~~ computers and computer facilities;**
- 1.1.2 ~~7.4.2~~ computing hardware and equipment;**
- 1.1.3 ~~7.4.3~~ mobile computing devices such as laptop computers, smartphones, and tablet computers;**
- 1.1.4 ~~7.4.4~~ electronic storage media such as CDs, USB memory sticks, and portable hard drives;**
- 1.1.5 ~~7.4.5~~ communications gateways and networks;**
- 1.1.6 ~~7.4.6~~ email systems;**
- 1.1.7 ~~7.4.7~~ telephone and other voice systems; ~~and~~**
- 1.1.8 ~~7.4.8~~ software, including AI-enabled applications;**

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

**1.1.9 Internet of Things (IoT) devices and systems;**

[1.1.10 industrial control systems \(ICS\) and supervisory control and data acquisition \(SCADA\) systems; and](#)

[1.1.11 cloud-hosted platforms and services.](#)

[1.2 The following are representative examples of UBC Electronic Information:](#)

[1.2.1 student records, including admissions, enrollment, grades, and transcripts;](#)

[1.2.2 personnel and employment records;](#)

[1.2.3 research records;](#)

[1.2.4 emails and messages created or received by UBC employees, service providers, or volunteers that are related to UBC business; and](#)

[1.2.5 content published by UBC on UBC websites.](#)

## **[2. Examples of Prohibited Use of UBC Electronic Information and Systems](#)**

[2.1 The following are representative examples of activities that are prohibited uses of UBC Electronic Information and Systems when not appropriately authorized by UBC:](#)

[2.1.1 breaching applicable laws or UBC policies;](#)

[2.1.2 sending threatening, harassing or discriminatory messages;](#)

[2.1.3 misrepresenting the User's identity as sender of messages;](#)

[2.1.4 intercepting or examining the content of messages, files, or communications;](#)

[2.1.5 infringing upon the copyright of computer programs, data compilations and all other works \(literary, dramatic, artistic or musical\);](#)

[2.1.6 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;](#)

[2.1.7 making copies of proprietary software, or offering unauthorized copies of proprietary software to others;](#)

[2.1.8 failing to maintain the confidentiality of passwords, access codes or identification numbers used to access UBC Electronic Information and Systems;](#)

[2.1.9 seeking information on passwords or information belonging to another User;](#)

[2.1.10 accessing or examining other accounts, files, programs, communications or information;](#)

2.1.11 destroying, altering, dismantling, disfiguring or disabling UBC Electronic Information and Systems;

2.1.12 damaging or altering the hardware or physical components of UBC Systems;

2.1.13 attempting to circumvent security controls on UBC Electronic Information and Systems;

2.1.14 knowingly introducing malicious software such as keyloggers, worms or viruses;

2.1.15 engaging in any uses that result in the loss of another User's information; and

2.1.16 collecting, generating, or manipulating information, including through bots, scripts, or AI agents, in a manner that threatens the security, privacy, or integrity of UBC Electronic Information and Systems.

2.2 Nothing in paragraph 2.1 shall be construed as preventing or restricting duly authorized system administrators or other technical personnel from carrying out their duties.

### **3. Policy Breaches**

3.1 If a User becomes aware of a breach or potential breach of this Policy, the User must promptly report such activity to the relevant System Owner and the OCIO at security@ubc.ca.

3.2 Notwithstanding section 3.1, technical personnel who identify breaches during the performance of their support duties will assist Users and System Owners by providing guidance and corrective actions. Technical personnel must report material breaches to the System Owner and the OCIO.

3.3 Where the CIO, or their delegate(s), determines that an investigation is required into a breach of this Policy, the investigation will be conducted in accordance with the Investigations Policy (SC8).

3.4 Subject to UBC's policies, legal privilege, and any applicable legal, contractual, and privacy obligations, the CIO, or their delegate(s), in order to conduct investigations into breaches of this Policy, may:

3.4.1 access any relevant UBC records or information; and

3.4.2 interview Users and other individuals as necessary to gather evidence.

3.5 In cases where access to information may be restricted, the CIO will seek direction from the Office of the University Counsel, which will consult with Human Resources as appropriate.

3.6 If an employee is the subject of an investigation, or, during an interview of a UBC employee, the investigator becomes aware of potential willful breaches of this Policy by that employee, the investigator will pause the interview and consult with Human Resources.

3.7 Breaches of this Policy will be addressed in a manner appropriate to the circumstances, including through remediation, guidance, or corrective actions. However, UBC retains the full discretion to restrict or withdraw access to UBC Electronic Information and Systems, including computing privileges and network access, and to impose the full range of disciplinary actions on Users who are found to have breached this Policy. The degree of intent, along with along with mitigating factors such as early reporting, transparency, and full cooperation, may be considered in determining appropriate consequences, along with any other relevant factors that are normally considered in determining appropriate outcomes.

#### 4. Cybersecurity Incidents

4.1 A “Cybersecurity Incident” is any real or threatened event that could compromise the confidentiality, integrity, or availability of UBC Electronic Information and Systems, regardless of whether it involves a violation of this Policy.

4.2 All Users must immediately report Cybersecurity Incidents to the System Owner (if known) and the OCIO at security@ubc.ca.

4.3 The OCIO must inform the relevant System Owner of any material Cybersecurity Incidents affecting UBC Systems under the System Owner’s authority.

4.4 The Chief Information Security Officer (“CISO”) will develop and maintain a plan for responding to Cybersecurity Incidents.

4.5 In response to a Cybersecurity Incident, the CIO or the CISO may:

4.5.1 authorize immediate and direct action, including accessing any system or information, disabling accounts, terminating network connections, or shutting down systems; and

4.5.2 ~~7.6 “Users” are faculty, staff, students, and any~~ issue directions to Systems Owners, Heads of Unit, or other individuals ~~who use~~ to implement specific technical measures, containment procedures, or system configuration changes necessary to protect UBC Electronic Information and Systems, which must be promptly implemented.

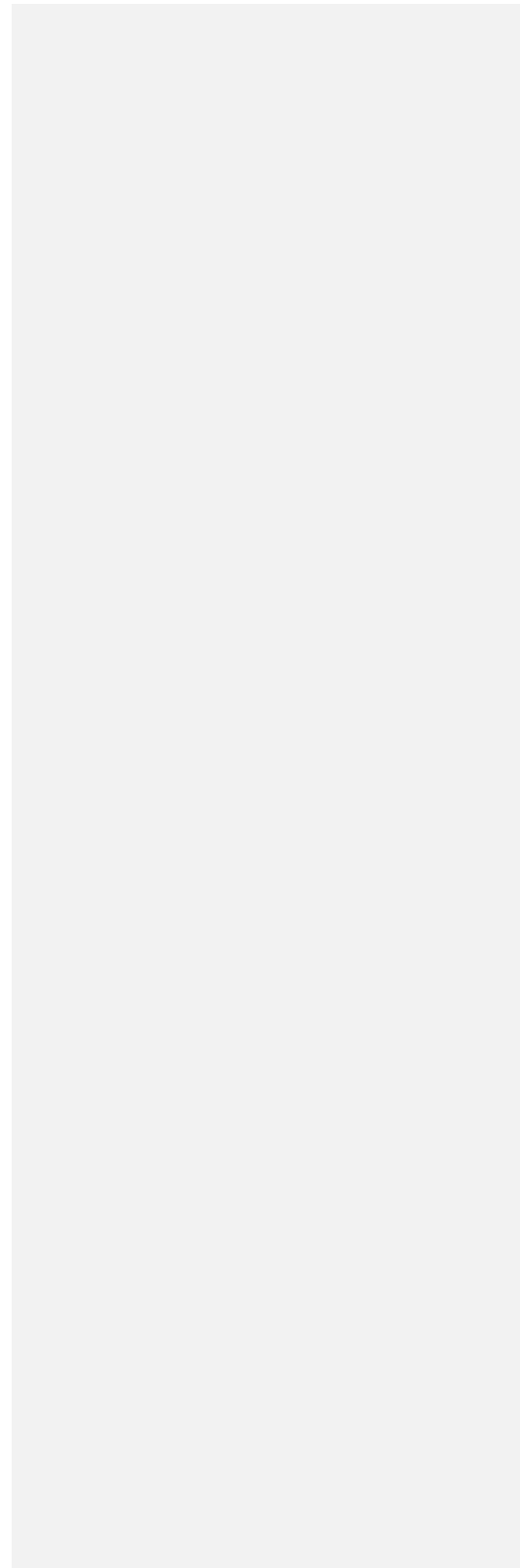
4.6 Where the CIO, in consultation with the CISO, determines that a Cybersecurity Incident has significant reputational, operational, or financial impacts or is otherwise material, the CIO will promptly report it to the Responsible Executive(s).

Document comparison by Workshare Compare on Tuesday, October 28, 2025  
10:01:06 AM

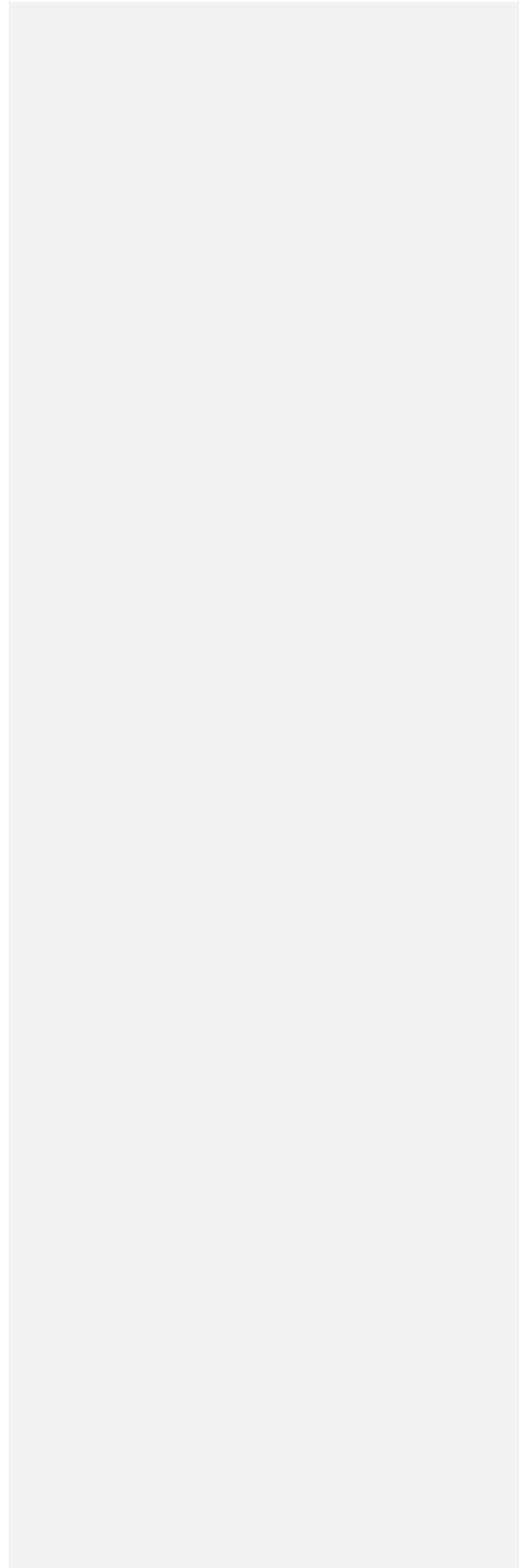
Input:	
Document 1 ID	file://G:\Public\Matthew Murray\Policies\Board Policies\Information Systems (SC14)\Board Submissions\SC14 - Information Systems - 104.docx
Description	SC14 - Information Systems - 104
Document 2 ID	file://G:\Public\Matthew Murray\Policies\Board Policies\Information Systems (SC14)\Board Submissions\Final\Proposed Amendments to the Information Systems Policy (SC14).docx
Description	Proposed Amendments to the Information Systems Policy (SC14)
Rendering set	Standard


Legend:	
<u>Insertion</u>	
<del>Deletion</del>	
<del>Moved from</del>	
<u>Moved to</u>	
Style change	
Format change	
<del>Moved deletion</del>	
Inserted cell	
Deleted cell	
Moved cell	
Split/Merged cell	
Padding cell	

Statistics:	
	Count
Insertions	258
Deletions	187
Moved from	33
Moved to	33
Style changes	0



Format changes	0
Total changes	511



 <p><b>The University of British Columbia Board of Governors</b></p>	<p><b>Policy No.:</b> <b>SC11</b></p>
<p><b>Long Title:</b> Management of the Wireless Network</p>	
<p><b>Short Title:</b> <b>Wireless Network Policy</b></p>	

### **Background & Purposes:**

#### The Problem

UBC makes use of radio frequency bands for research, teaching and communication as part of its functions and duties. The UBC wireless network, provided by UBC IT, is part of UBC's telecommunications and data network. Devices that operate in the same frequency bands as the UBC wireless network, such as wireless networking devices, cordless phones, microwave ovens, audio speakers, still cameras, video cameras, and other equipment, can interfere with the UBC wireless network, and can introduce performance, reliability, usability, sustainability, and security problems.

#### The Purpose

UBC IT has responsibility for the UBC wireless network and must be empowered to resolve electromagnetic interference with the UBC wireless network in order to ensure the highest level of service while minimizing support costs.

While interference can also be caused to teaching and research activities by non-university equipment or by the UBC wireless network this interference is to be resolved outside the scope of this policy.

## **1. Governing Principles**

Where *UBC IT* provides wireless network connectivity reliability, usability, sustainability, security and cost are paramount to the user and the provider.

## **2. Scope**

### **2.1 Locations and Devices Affected By This Policy**

- 2.1.1 This policy governs the deployment and use of electronic devices that operate in any licence-exempt radio frequency band used for high-speed wireless network connectivity (which for the sake of clarity include the 2.400-2.483, 5.15-5.35, 5.470-5.725, and 5.725-5.825 GHz bands).

2.1.2 This policy applies in all areas where wireless access points installed by *UBC IT* provide wireless coverage, except as excluded elsewhere in this policy.

### 2.2 Exclusions

2.2.1 This policy does not apply where wireless coverage is not provided by *UBC IT*.

2.2.2 This policy does not apply to devices within a specific facility or area operated by the *UBC* Department of Housing and Conferences if:

- (a) the affected area is entirely within the specific facility or area it operates; and
- (b) the Director, or Director's designate, of the *UBC* Department of Housing and Conferences determines that *UBC IT* wireless network connectivity is not required in the affected area.

2.2.3 This policy does not apply to devices in specific locations to the extent that the Associate Vice-President, Information Technology or his/her designate determines that wireless network security will not be compromised and reliable connectivity is not required in the affected area.

2.2.4 This policy does not apply to devices in specific locations to the extent that the Associate Vice-President, Information Technology and the Associate Vice-President, Research and Innovation, or their respective designates, determine that a device that is necessary to teaching or a research project is interfering with or subject to interference by:

- (a) the *UBC IT* wireless network; and
- (b) the interference is not reasonably resolvable other than by *UBC IT* disconnection of its access point at issue.

### 3. Rights and Responsibilities

3.1 If *UBC IT* detects electromagnetic interference with the *UBC* wireless network, or with teaching or research activities, it may act to identify and evaluate devices that might be causing the interference, and in doing so may request that any device capable of electromagnetic interference:

3.1.1 not be used and be disconnected and/or powered off until the interference is eliminated; or

3.1.2 be temporarily deposited with *UBC IT* for testing and evaluation.

3.2 If, after the procedures outlined in section 3.1, *UBC IT* determines that a device continues to interfere with the *UBC* wireless network, or with teaching or research activities, and is causing any of the following problems:

- 3.2.1 security or confidentiality concerns (which may include concern about theft of services);
- 3.2.2 reliability issues (which may include data loss, bandwidth, speed, coverage, up-time, and security); or
- 3.2.3 significant maintenance or operating costs;

then *UBC IT* may act to address the problem by:

- 3.2.4 disabling services or access points;
- 3.2.5 disconnecting the device or cables;
- 3.2.6 requiring removal of the device; and/or temporary deposit of the device with *UBC IT*; or
- 3.2.7 agreeing to undertake, at the request and cost of the owner or operator of the device, to alter the *UBC* wireless network or the device to address any of the problems outlined above.

- 3.3 *UBC IT* must return any device on deposit with it upon demand of the owner of the device. Devices on deposit with *UBC IT* for longer than 2 years will be deemed abandoned and surrendered to *UBC IT*.

#### 4. Appeal Process

- 4.1 Anyone who is asked to remove a device, deposit a device with *UBC IT*, or pay related costs and has been unable to negotiate a satisfactory resolution with *UBC IT*, may appeal. Appeals are to be handled as follows:
  - 4.1.1 Appeals are to be filed with the *Responsible Executive* or his/her designate(s).
  - 4.1.2 Appeals are to be convened and heard by the *Responsible Executive*, or his/her designate(s), as arbitrator at a meeting of the relevant parties. The decision of the arbitrator will be final and binding.
  - 4.1.3 The *Responsible Executive* may have more than one designate if he/she determines that local consideration of appeals at *UBC Vancouver* or *UBC Okanagan* campuses is desirable.

#### 5. Definitions

In this policy the following terms have the meaning defined below, and shall have the same meaning in any administration and management procedures under this policy:

Term	Definition
<i>Responsible Executive</i>	means: 1) the individual(s) specified under the heading “Responsible Executive” in the heading information table above section 1 of this policy; and  2) any person delegated to fulfill that person(s) role except to the extent that delegation is specifically excluded.
<i>UBC</i>	means: The University of British Columbia
<i>UBC IT</i>	means: The University of British Columbia Information Technology Department