SIMON FRASER UNIVERSITY
ENGAGING THE WORLD

TO:	Senate
FROM	Joy Johnson Chair – Senate Committee on Agenda and Rules
DATE:	November 17, 2022
SUBJECT:	Revision and Renaming of GP 24 - Fair Use of Information and Communications Technology

---

SCAR has reviewed this document and is bringing this to Senate for information.

SFU SIMON FRASER UNIVERSITY

EXECUTIVE TEAM MEETING – CONSENT ITEM BRIEFING NOTE

SUBJECT	GP 24, Acceptable Use and Security of Digital Information and Electronic Systems and Appendix A-Definitions
DATE	September 09, 2022
ET SPONSOR	Martin Pochurko, VP Finance and Administration
UNIT/DEPARTMENT	Information Security Department
PREPARED BY	Jastej Singh Aujla, Chief Information Security Officer

TOPIC

Revising and renaming GP 24: Acceptable Use and Security of Digital Information and Electronic Systems Policy.

BACKGROUND

REVISION to Fair Use of Information and Communications Technology ("ICT") (GP 24)

1. GP 24 was created in 1993 and last updated in 2009.

2. It establishes the responsibility of University faculty, staff, and students in maintaining the security of the Information and Communication Technology environment, the security of the information within it, and makes users accountable for their use of those resources.

   The revised GP 24, which we propose to rename, "Acceptable Use and Security of Digital Information and Electronic Systems" requires all users of University Digital Information and Electronic Systems to do so responsibly, lawfully, and ethically. It establishes the standards and guidelines necessary to:

   - secure the personal identifiable digital information that our electronic systems contain;
   - maintain the integrity of those electronic systems, and
   - safeguard the financial assets of the University.

3. The revised "Acceptable Use and Security of Digital Information and Electronic Systems" policy, outline the responsibilities of members of the University community with respect to maintaining the privacy, integrity, availability, and confidentiality of University Digital Information and Electronic Systems. It establishes the requirement of not only verifying identity to ensure users have appropriate access to University Digital Information and Electronic Systems, but also verifying that the level of access they are granted is in alignment with their role at the University.

4. The expansion of GP 24 will guide the Chief Information Security Officer (CISO) on stewardship of University Digital Information and Electronic Systems security. It provides the framework for supporting procedures, standards, controls, and guidelines needed to facilitate implementation of the policy. The policy also sets out the responsibilities of the CISO regarding risk, security, and compliance. Consultation period completed August 19, 2022.

Policy Updates prior to Consultation

GP 24, Acceptable Use and Security of Digital Information and Electronic Systems Policy and Appendix A-Definitions

1. add executive summary as required by new policy format
2. revised GP 24, which we propose to rename, "Acceptable Use and Security of Digital Information and Electronic Systems" policy requires all users of the digital information and electronic systems to do so responsibly, lawfully, and ethically
3. updated Appendix A to reflect the changes made in the policy
4. other edits to comply with new policy format

Consultation Feedback

The community consultation period was from July 25th to August 19th, 2022 for GP 24, "Acceptable Use and Security of Digital Information and Electronic Systems" Policy and "Appendix A-Definitions".

Summary of the findings is listed in the table below. Appendix A has the details of all the consultation feedback. Below two table lists the consultation feedback and management response.

Table1: Summary of Consultation Feedback and Response

Consultation Feedback	Management Response
Privacy office had recommended number of changes in the "Acceptable Use and Security of Digital Information and Electronic Systems" policy and Appendix A.	A meeting was setup to go over the recommendations. The change that were agreed upon are documented in Appendix A of this memo.
Digital Library Services had recommended number of changes in the "Acceptable Use and Security of Digital Information and Electronic Systems" policy	A meeting was setup to go over the recommendations. The change that were agreed upon are documented in Appendix A of this memo.
There were a couple of typographical error (Typos) identified.	Recommendation was incorporated

CONSIDERATIONS

1. The revised GP 24 restates in current terms the university's right to control and manage its Information Technology Service resources and more clearly makes users accountable for their use of those resources.
2. The revised policy will help University minimize its cyber-attack footprint, minimize the impact if we are attacked, develop the foundation of Role Base Access, and clarify the responsibility of all users with access to University digital information and electronic systems.
3. Through this approach we also address the concerns and shortcomings detailed in the recommendations of the Catalone and KPMG reports of 2020 and 2021.
4. The Legal Counsel, Office of the General Counsel and University Secretary reviewed this version of the policy that incorporates feedback from the community consultation.

NEXT STEPS

The changes to GP 24, Acceptable Use and Security of Digital Information and Electronic Systems Policy and Appendix A-Definitions from the community consultation, will be sent by the Board Office to Senate/SCAR meeting to be held in October followed by the Board of Governors in November.

ATTACHMENTS

- Current GP 24 Fair Use of Information Systems Policy
- Revised GP 24 Acceptable Use and Security of Digital Information and Electronic Systems
- Revised GP 24 Appendix A

Appendix A

Table 2: Summary of feedback received and incorporated in the GP 24, Acceptable Use and Security of Digital Information and Electronic Systems Policy

Consultation Feedback	Management Response
Privacy office had requested to change the following in the Executive summary section 1. mention University rather than SFU 2. to include sensitive information along with the personally identifiable information, in the first bullet point 3. to ensure that user will comply with the GP 24 policy or "any other relevant University policy or procedure "	All recommendations were incorporated
Privacy office had recommended in section 1.3 to add wording "to a degree that is reasonable and technically feasible and in accordance with FIPPA".	Recommendation was incorporated
Privacy office had recommended to move the section regarding breach of from 5.2.2 to 3.3. As this section would impact the entire user community.	Recommendation was incorporated
Digital Library Services had recommended to add under section 5.2.1 (a) "and in adherence to license agreements". Digital Library Services invoke GP 24 when end users contravene library policies or license agreements.	Recommendation was incorporated
Privacy office recommended to add the section in the policy under 5.3 "Disclosure of Information - Administrative Continuity" section was part of the old GP 24 policy. It was removed from the policy in the version posted for the community consultation and would have been added into the security standard's that will follow the policy. Privacy office refers to this particular section on a regular basis. There was a risk that the standard might not be made in time when the policy goes live could cause operational issues for the Privacy team. Recommendation was made to add this section back to the policy.	Recommendation was incorporated
Privacy office recommended to add the section in the policy under 5.3.4 "Role Account" section was part of the old GP 24 policy. It was removed from the policy this time and would have been added into the security standard's that will follow the policy. Privacy office refers to this particular section on a regular basis. There was a risk that the standard might not be made in time when the policy goes live could cause operational issues for the Privacy team.	Recommendation was incorporated

Recommendation was made to add this section back to the policy.	
Privacy office recommended to replace the word in section 5.4.1 “must” rather than “should choose to” for use of approved software.	Recommendation was incorporated
Privacy office recommended to the remove the wording “when available” from section 5.4.1 and replace it with “When approved Electronic Systems are not available” in section 5.4.2. This was recommended to provide clarity to the readers.	Recommendation was incorporated
Privacy office recommended to the add the word under section 6.1.1 (e) “Department” to the Archives and Records Management. This was to standardize the language.	Recommendation was incorporated
Privacy office recommended to add retention and disposition to section 6.2.1 (c). Digital information should be retained and disposed of according to an approved Records Retention Schedule and Disposition Authority. This was to ensure the entire lifecycle of digital information is addressed.	Recommendation was incorporated
An Analyst from Information Technology Services department had recommended to correct the Typo in section 6.2.1 (a) “The principle of least privilege should be abbreviated as PoLP instead of PLoP”	The abbreviation was removed as it was used in only one place and the full phrase was used “Principle of Least Privilege”.
Data Coordinator from Institution Research and Planning department notified about a Typo in Section 12.1 “This policy is administered under the authority of the policy is administered under the authority of the Vice-President Finance and Administration" to change to “This policy is administered under the authority of the Vice-President Finance and Administration”.	Recommendation was incorporated

Table 3: Summary of feedback received and incorporated in the Appendix A-Definitions

Consultation Feedback	Management Response
Privacy office had recommended to remove the definition of “Digital Information and Electronic Systems”, since there were separate definitions for “Digital information” and “Electronics Systems”. This was causing confusion for the readers.	Recommendation was incorporated
Privacy office had recommended to add the definition for “Executive team”. “Executive Team” is mentioned	Recommendation was incorporated in section 2.4

in the GP 24 section 5.5.2 and the definition was missing.	
Privacy office had recommended to add more examples in section 2.5 i.e. “transcripts, employee emails in their Computing-ID and role-based University email accounts, and employee emergency contact information”.	Recommendation was incorporated
Privacy office had recommended to add language defining the role of operational leader in section 2.6 “responsible for the overall procurement, development, integration, modification, operation, maintenance and retirement of Electronic Systems”.	Recommendation was incorporated
Privacy office had recommended to simplify the definition of “Principle of Least Privilege” in section 2.7.	Recommendation was incorporated
Privacy office had recommended to simplify the definition of “Regulated Information” in section 2.9.	Recommendation was incorporated
Privacy office had recommended to simplify the definition of “Service Provider” in section 2.11.	Recommendation was incorporated
Privacy office had recommended to simplify the definition of “Users” in section 2.15.	Recommendation was incorporated
Privacy office had recommended to add the definition of “Unit”.	Recommendation was incorporated in section 2.16
Disaster Recovery Coordinator from Information Technology Services recommended to either use the full name of the Department (IT services) or include ITS in the list of definition. There were two references to ITS in the draft of Appendix A for GP24 but ITS was not listed in the terms. These instances were in section “Regulated Information” 2.9 and section “Digital Information and Electronic Systems”.	For both the instances ITS was removed after consulting with Privacy team

SFU SIMON FRASER UNIVERSITY
ENGAGING THE WORLD

Policies and Procedures

Fair Use of Information and Communications Technology

SIMON FRASER UNIVERSITY
POLICIES AND PROCEDURES

Date	**Number**
March 23, 1993	GP 24
Revision Date	**Revision No.**
January 29, 2009	A

Preamble

This policy allows those who administer the University's Information and Communications Technology (ICT) resources to do so as transparently as possible, while providing users with essential guidance on their rights and responsibilities.

ICT resources (see section 6) include business tools that facilitate University processes and activities related to its research, teaching and community service mandates. The University recognizes those resources may be the pathway by which controversial points of view and new ideas are disseminated and tested by members of the community.

The University continuously strives to create an environment that provides members of the community with the resources needed to meet the objectives of their work and/or studies, and to create a working and learning environment that promotes full, free and responsible participation by all members.

1.0 Purpose:

1.1 The Purpose of this policy is to:

a) establish the University's right to control and manage its Information and Communications Technology (ICT) resources;

b) inform administrators and users of SFU's ICT resources of their rights and responsibilities regarding the management and use of these

fundamental resources; and

c) make users accountable for their use of the University's ICT resources.

2.0 Policy

2.1 Right of Access

2.1.1 Authorized users of the University's ICT resources have the right to access them without interference by others.

2.1.2 Where users misuse the University's ICT resources, their right of access may be restricted or removed. (See section 2.6.)

2.2 Confidentiality and Privacy Protection

2.2.1 General

The University respects the privacy of those who use the University's ICT resources and protects users' information by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or disposal. The University's ICT staff will comply with the FOIPOP Act and the University's information and privacy policies (I10 series) and will disclose a user's activities and personal information only as permitted or required by law.

2.2.2 Logging of Information

Most activities performed using the University's ICT resources are logged. Information in log files is owned by the University and is routinely examined by ICT support staff to monitor the performance, reliability and security of ICT resources. ICT support must not disclose information learned from or contained within these log files except when authorized in writing to do so by their Director in order to:

a) investigate an alleged violation of this Policy or other related University Policy using the procedure outlined in Appendix II; or to

b) respond to a request for information pursuant to proceedings under the auspices of another University Policy using the procedure outlined in Appendix II; or to

c) ensure administrative continuity (see sections 2.2.3 and 2.2.4).

2.2.3 Disclosure of Information - Administrative Continuity

In cases of the absence, retirement or termination of an employee engaged in administrative duties, there may be occasions where departments need access to that individual's emails or files to conduct business as permitted under section 33.2(c) FOIPOP Act. In such cases the Chair or unit head can obtain access by making a request to the Director, Client and Research Services (CaRS). Any information released under this provision may not be used for any employee discipline or other purpose except administrative continuity and any personal information shall be kept confidential.

2.2.4 Role Accounts

Role accounts (i.e., those granted to a role or organizational position rather than to an individual for business purposes) may be shared amongst authorized users as determined by the appropriate Department Chair/unit head. Information contained in these accounts may be

accessed and disseminated upon the request of the Chair/unit head to the Director, Client and Research Services (CaRS). Users are advised that role accounts should not be used to store personal information as they are subject to access should the University need to do so to conduct its operations.

2.3 Personal Use

2.3.1 Accounts to access ICT resources are issued for the sole use of the person to whom they are issued. Accounts are not to be shared, given, rented, sold or reassigned to any other individual or organization. Role accounts are exceptions to this provision

2.3.2 Incidental personal use of ICT resources is allowed provided that it does not: contravene the law and provisions of this or other University policies; interfere with access to ICT resources by authorized users; or cause the University to incur additional costs (e.g., excessive use of internet bandwidth).

2.4 Commercial Use

2.4.1 The University's ICT resources shall not be used for commercial purposes, for profit-making, or for the benefit of non-SFU organizations unless these purposes are authorized under, and consistent with, the appropriate University policies and procedures. This provision shall not restrict SFU researchers from pursuing their research activities and freely exchanging information.

2.5 Misuse

2.5.1 Misuse of the University's ICT Resources is explicitly prohibited. Activities included under the definition of "misuse" are set out in Section 6.0 Definitions below.

2.6 Protective Measures

2.6.1 The University reserves the right to limit, restrict or terminate user access, and to inspect, copy, remove or otherwise alter any data, files or other ICT resources covered by this policy.

2.6.2 At the direction of the Director, CaRS or designate, interim measures may be taken by duly authorized ICT staff in immediate response to allegations or awareness of misuse. These measures shall remain in force until the matter is resolved by the appropriate University Officer.

3.0 Scope:

3.1 This Policy applies to anyone using the University's ICT resources or using their SFU authorization credentials to access ICT resources provided by other organizations. In the latter case, users are responsible for making themselves aware of, and to comply with, the other organization's "acceptable use" policies.

3.2 This Policy covers all University-owned or -leased ICT resources, whether individually controlled or shared, standalone or networked, and to all activities of individuals accessing University-owned ICT resources from non-University-owned ICT resources (e.g., personal computer, PDA, or other devices).

3.3 From time to time the University may grant access to ICT resources to persons from other organizations through reciprocal sharing agreements with individual organizations or through participation in a federation of organizations. This privilege may be revoked solely at the discretion of the University.

4.0 Roles and Responsibilities:

4.1 The University's ICT resources will be provided and protected by the University to a degree that is reasonable and technically feasible under the guidelines set out by this policy, its associated procedures, section 30 of the FOIPOP Act and any other relevant University policy or procedure (see Appendix 1 for a partial list of such documents).

4.2 The University warrants that it makes reasonable security arrangements for the ICT resources offered; however, SFU stipulates that there are no guarantees regarding the accessibility, reliability or security of said resources.

4.3 The responsibilities of the ICT staff, in priority order, are to maintain the security of the information in the ICT environment, maintain the ICT environment in an operationally available state, and ensure that the ICT resources are accessible to the members of the user community. Where the security of information within the ICT environment is threatened, access to the environment may be restricted until the threat is resolved.

5.0 Authority:

5.1 This policy is administered under the authority of the Chief Information Officer.

6.0 Definitions

Authorization for File Access is the Form required to view information either owned by an Authorized User or pertaining to an Authorized User for which the User has not given permission, except for role accounts (section 2.2.4) or in situations dealing with Administrative continuity (section 2.2.3). An Authorization is normally required to support an investigation or process associated with the application of this or another University Policy.

Authorized Users are those who have current ICT identity credentials granted by an authorized 0fficer of the University.

Confidentiality means keeping personal information private or secret, safe from access, use or disclosure by people who are not authorized to handle that information. (BC Govt. FOIPOP Policy and Procedures Manual.)

FOIPOP Act refers to the Freedom of Information and Protection of Privacy Act and associated Regulations enacted by the Province of British Columbia. Also known as FOIPOP.

ICT Resources Information resources in this document are meant to include any information in digital format, or any hardware or software that make possible the electronic storage and use of such information. This includes, but is not limited to, electronic mail, local databases, externally accessed databases, CD-ROM, motion picture film, recorded magnetic media, photographs, and digitized information. For purposes of this Policy, the "appropriate use of ICT resources" does not refer to managing digital information in terms of its classification, organization, retention or disposal; this is not a records management policy.

Interim measures may include, but are not limited to:

- contact with respondents to establish the veracity of allegations;
- discussions with respondents to informally resolve problems;
- instruction to respondents to cease and desist alleged misuse within a time limit; or
- temporary disabling of respondents' computer accounts or other access.

It is understood that interim measures are to be preemptive and remedial rather than punitive, and will remain in force until the matter is resolved by the appropriate University Officer.

Misuse under this policy encompasses, but is not limited to:

Unlawful Activities:

- Any activity that contravenes federal or provincial legislation, whether or not the activity is reported to the police
- The evidence supporting a suspicion or allegation of unlawful activity will be assessed and misuse will be determined based on a 'Balance of Probabilities' standard
- Knowledge of and compliance with the law is the responsibility of the user

Threats to System Security or Integrity:

- Seeking to gain, or gaining, unauthorized access to ICT resources
- Possessing, creating, transmitting or storing tools, programs, attachments or other materials for the purpose of gaining unauthorized access
- Examining or using without authorization another user's files or programs in transit or in storage
- Unauthorized scanning of other computers on the network
- Preventing rightful access to computer-based information and ICT resources
- Altering, disrupting or otherwise interfering with the integrity of computer-based information and ICT resources, including the passing on of viruses, worms, "trojans" or other "malware"
- Endangering the finite capacity of any system through "chain mail," "flame wars," "bombing," "spamming" or using any method system administrators consider may endanger and/or restrict the access to their accounts by other authorized users
- Impersonating another user (regardless of whether the other user is real or fictitious) by altering individual system identity

Excessive Use of ICT Resources:

- Use of ICT resources in a manner that may result in additional cost to the University
- Use of ICT resources in a manner that consumes resources that would rightfully be available to others.

Contravention of University Policy

- Use of ICT Resources contrary to another University policy will be addressed as applicable under the relevant policy.

Personal is defined as relating to, concerning, or affecting a person as a private individual (rather than as a member of a group or the public, or in a public or professional capacity); individual, private; one's own.

Personal Information means recorded information about an identifiable individual other than contact information (FOIPOP Act).

Privacy means the state or condition of being alone, undisturbed, or free from public attention, as a matter of choice or right; seclusion, freedom from interference or intrusion. (BC Govt. FOIPOP Policy and Procedures Manual)

Record includes books, documents, maps, drawings, photographs, letters, vouchers, papers and any other thing on which information is

recorded or stored by graphic, electronic, mechanical or other means, but does not include a computer program or any other mechanism that produces records (FOIPOP Act). Note that this definition of "record" specifically excludes ICT resources (i.e., a computer program or any other mechanism that produces records).

APPENDIX I

This Policy should be read and understood in conjunction with the following University Policies and documents, and with the University's Statement on Values and Commitments:

A 30.01 Faculty Code of Ethics
AD 1.06 Commercial Activities and Advertising
AD 1.12 Selling, Serving and Advertising Liquor
GP 18 Human Rights
GP 25 Response to Violence and Threatening Behaviour
GP 30 Interpretation Policy
I 10.04 Access to Information and Protection of Privacy
R 30.03 Intellectual Property Policy
T 10.01 Code of Student Conduct
T 10.02 Code of Academic Honesty
Applicable Residence and Housing agreements/contracts

APPENDIX II – Procedure to Authorize File Access

An Authorization for File Access is required to view information either owned by an Authorized User or pertaining to an Authorized User for which the User has not given permission, except for role accounts (section 2.2.4) or in situations dealing with Administrative continuity (section 2.2.3). An Authorization is normally required to support an investigation or process associated with the application of this or another University Policy.

Log files and file directories are system resources and are routinely monitored by duly authorized system support staff to maintain the security, reliability, accessibility, and performance of the University's ICT resources. Notwithstanding these, systems staff must not divulge any information pertaining to the activities of an Authorized User to anyone other than other duly authorized system support staff.

Neither the Authorization forms nor the information arising from their use may be transmitted via any insecure communications media. E.g., email is neither acceptable nor sufficient.

1. If the Authorization for File Access is sought to support an allegation or suspicion of misuse under this policy, an Authorization for File Access Form must be completed by the person making the claim.

2. If the Authorization for File Access is sought to support the application of another University Policy, the Authorization for File Access Form shall be completed by the person duly appointed to investigate under the auspices of the applicable University Policy.

3. The Authorization for File Access must contain the following information:

The name of the applicant
The date of the application to access the files

The ID of the Authorized User for which the application is requested

The date that the file access must cease/end

The Name of the Authorized User for which the application is requested

The University Policy under which the application is requested

A description containing the reason for the request and the information requested

The names of staff/faculty who are authorized to access this information when it is produced

The name, phone number, and signature of the person requesting the information

4. The completed Authorization for File Access form should be taken to the Director, CaRS. The request will be reviewed to ensure that the information requested is possible to produce, that it is sufficient to meet the objective of the request, and that the resources required to produce the information are available. (Note: Requests for information from backup tapes or log files can take several days to produce.) If the Director, CaRS agrees with the technical aspects of the requests and has the resources available to produce the information the Director, CaRS will approve the form.

5. The Director, CaRS will then take the form to seek the approval of two University Vice-Presidents. The requestor may or may not accompany the Director when seeking the Vice-Presidents' approval.

6. The information will be assembled and two copies prepared on an appropriate storage media (usually a write once CD or DVD). The information will be assembled by the appropriate systems support person, who will initial the media in order to identify it later if necessary. One copy will be stored in a confidential file with the original of the approved Authorization for File Access form, and the second will be given to the requestor.

APPENDIX III – Authorization for File Access

Sample Form Attached

GP24_Request_for_Access_to_Personal_Information_Contained_In_ICT_Resources.pdf

Request for Access to Personal Information Contained in ICT Resources

SFU SIMON FRASER UNIVERSITY

POLICY AND PROCEDURES

ACCEPTABLE USE AND SECURITY OF DIGITAL AND ELECTRONIC SYSTEMS

Date	**Number**
March 23, 1993	GP-24 [NEW]
Date of Last Review/Revision	**Mandated Review**
January 29, 2002	[TBA]

Updated Discussion Draft: September 09, 2022

Policy Authority: Vice President Finance and Administration

Associated Procedure(s): See section 14 of this Policy

EXECUTIVE SUMMARY

Simon Fraser University (the "University" ~~"SFU"~~) is committed to protecting the Digital Information and Electronic Systems that are critical to teaching, research, business operations, and other University activities and that are vital ~~critical~~ to the communities we support. This policy establishes standards and guidelines to:

- secure the Regulated ~~personally identifiable~~ Digital Information that our Electronic Systems contain;
- maintain the integrity of those Electronic Systems, and
- safeguard the financial assets of the University.

Access to, and use of, Digital Information and Electronic Systems will be granted using Role-Based Access principles. This enables Users to access Digital Information and Electronic Systems only as required for their role at the University, and only at the level required to perform their role. Everyone who accesses or uses Digital Information and Electronic Systems must do so ethically, responsibly, lawfully, and in a manner consistent with the Procedures, Standards, Guidelines, Controls, and Processes associated with this and any other relevant University ~~p~~P~~olicy~~policy or procedure.

Commented [JA1]: New Comment: - Privacy office had recommended that we mention University rather than SFU. Recommendation was incorporated

Commented [JA2]: New Comment:- Privacy office recommended to change the word Critical as it was used twice in the same sentence. Recommendation was implemented with the change of "Critical" to "Vital"

Commented [JA3]: New Comment:- Privacy office recommended to add the term sensitive information as the security of both sensitive and personally identified information must be addressed.
Recommendation was incorporated by adding the word Regulated this in in compliance with the definition provided in Appendix A

Commented [JA4]: New Comment:- Privacy office had recommended that we add "any other relevant University policy or procedure".
Recommendation was incorporated

TABLE OF CONTENTS

Contents

1.0 PREAMBLE

1.1 The University will strive to balance the need for security with the open pursuit of academic activities. Security concerns may place limits on the way in which work is done, but not on the research or inquiry that is pursued. When limitations are needed, the University will make reasonable efforts to consult with person(s) impacted to attempt to find appropriate and workable solutions.

1.2 Proper management of the security risks associated with access to and use of Digital Information and Electronic Systems is imperative to support the University's academic, research, and administrative activities.

1.3 To ensure Digital Information and Electronic Systems remain secure, to a degree that is reasonable and technically feasible and in accordance with FIPPA, the University will grant access to Users by utilizing Role-Based Access principles and security controls.

1.4 Each User of Digital Information and Electronic Systems is responsible for abiding by the University's Role-Based Access principles and security controls.

2.0 PURPOSE

2.1 This policy, together with its associated Procedures, Standards, Guidelines, Controls, and Processes referenced in section 14, establishes the University's expectations for access to, and use of, Digital Information and Electronic Systems.

3.0 SCOPE AND JURISDICTION

3.1 This policy applies to all Digital Information and Electronic Systems

3.2 This policy applies to all Service Providers and members of the University Community who are authorized to access and use Digital Information and Electronic Systems. ~~for the purpose of creating, storing, transmitting, using, or disposing of SFU Digital Information.~~

~~This policy only applies to Ddigital Information and, Electronic Systems and the University's digital record-keeping processes.~~

3.3 A breach of this policy may result in the University restricting or withdrawing a User's access to Digital Information and Electronic Systems, including computing privileges and network access.

4.0 DEFINITIONS

4.1 See Appendix A for the definitions of words used in this policy and its associated Procedures, Standards, Guidelines, Controls, and Processes.

5.0 POLICY

Commented [JA5]: New Comment:- Privacy office had recommended to add wording "to a degree that is reasonable and technically feasible and in accordance with FIPPA". Recommendation was incorporated

Commented [JA6]: New Comment:- Privacy office had recommended to remove wording "both administrative and academic" from 3.1 and 3.2, as this was covered in the definition of Digital Information and Electronic Systems. Recommendations were implemented

Commented [JA7]: New Comment:- Privacy office had recommended to remove wording "for the purpose of creating , storing, transmitting, using, or disposing SFU Digital Information" from 3.2, as this was covered in the definition of Digital Information and Electronic Systems. Privacy office also recommended to add "Service Providers" in the sentence. Recommendations were implemented

Commented [JA8]: New Comment:- Privacy office had recommended to remove wording "for the purpose of creating , storing, transmitting, using, or disposing SFU Digital Information" from 3.2, as this was covered in the definition of Digital Information and Electronic Systems. Privacy office also recommended to add "Service Providers" in the sentence. Recommendations were implemented

Commented [JA9]: New Comment:- Privacy office had recommended to remove wording "This policy only applies to Digital Information and Electronic Systems and the University's digital record-keeping security processes." As this was covered in 3.1. and 3.2 Recommendation was implemented

Commented [JA10]: New Comment:- Privacy office had recommended to move this section from 5.2.2 to 3.3. As this section would impact the entire user community. Recommendation was incorporated

5.1 Role-Based Access to Digital Information and Electronic Systems

5.1.1 The University will utilize Role-Based Access principles to grant Users access to Digital Information and Electronic Systems. Role-Based Access enables Users to access information and systems only as required for their role at the University, and only at the level required to perform their role.

5.2 Use of Digital Information and Electronic Systems

5.2.1 All Users must:

a. use Digital Information and Electronic Systems responsibly, lawfully, ethically, in accordance with the User's Role-Based Access, and in adherence to license agreements.

~~b. ensure the security of the SFU's Digital Information and Electronic Systems by:~~

~~i. applying the Digital Information Classification Standard to determine which class of SFU's Digital Information is appropriate: Internal Information, Public Access Information or Regulated Information; and~~

~~ii. applying the Minimum Digital Information Security Standards for SFU's Digital Information and the Digital Information Domain Standards applicable to each classification of SFU's \ Digital Information.~~

~~5.2.2 A breach of this policy may result in the University restricting or withdrawing a User's access to SFU's Digital Information and Electronic Systems, including computing privileges and network access.~~

5.3 Security of Digital Information and Electronic Systems

5.3.1 All Users of Digital Information and Electronic Systems must take appropriate steps to ensure security by ~~(see section 5.2.1, above):~~

i. applying the Digital Information Classification Standard to determine which class of Digital Information is appropriate: Internal Information, Public Access Information or Regulated Information; and

ii. applying the digital information security and domain Standards applicable to each classification of Digital Information.

~~5.3.1~~5.3.2 All Operational Leaders ~~owners~~ and Service Providers of Digital Information and Electronic Systems, and those who are responsible for maintaining and administering them, must

Commented [JA11]: New Comment:- Digital Library Services had recommended to add "and in adherence to license agreement". Digital Library Services invoke GP 24 when end users contravene library policies or license agreements.
Recommendation was incorporated

Commented [JA12]: New Comment:- Privacy office had recommended to move this section from 5.2.1 b to 5.3.1. This section was referred from 5.3, this section is more suitable under the "Security of Digital Information and Electronic Systems".
Recommendation was implemented

Commented [JA13]: New Comment:- The term owner was overlapping with the Operational Leader. Privacy office recommended to remove owner and state Operational Leader. Operational Leader is also defined in Appendix
Recommendation was implemented

protect the systems from cybersecurity or other threats by managing and remediating any vulnerabilities throughout the Electronic System's lifecycle.

5.3.3 Disclosure of Information - Administrative Continuity

In cases of the absence, retirement or termination of an employee engaged in administrative duties, there may be occasions where Units need access to that individual's emails or files to conduct business as permitted under section FIPP Act (RSBC 1996, c. 165). In such cases the Unit head can obtain access by making a request to the Chief Privacy Officer. Any information released under this provision may not be used for any employee discipline or other purpose except administrative continuity and any personal information shall be kept confidential.

5.3.4 Role Accounts

Role accounts (that is, those accounts granted to a role or organizational position rather than to an individual for business purposes) may be shared amongst Users as determined by the appropriate Operational Leader. Role accounts must have one responsible owner as appointed by the Operational Leader but may be shared amongst Users as determined by the appropriate Operational Leader. Role accounts cannot be used to store Personal Information as they are subject to access by the University to conduct its operations. The Chief Information Security Officer has the authority to permit an Operational Leader to access and disseminate the information contained in a Role account. Role accounts cannot be used to share licensed software in a manner that may violate the license. Use of Role accounts may be prohibited in specific systems and processes if the use of Role accounts fails to meet regulatory or legislative requirements.

5.4 Use of Non-University Systems for University Business

5.4.1 To optimize the security of Digital Information and Electronic Systems and to ensure administrative effectiveness and the best use of University resources, Units ~~should choose to~~must use approved Electronic Systems~~, when available~~.

5.4.2 When approved Electronic Systems are not available Users or Units who wish to store, transmit, use, or dispose of Regulated Information or Internal Information using systems other than Electronic Systems must be pre-authorized by the Chief Information Security Officer ("CISO") to do so. Once approved, adherence to the Procedures, Standards, Guidelines, Controls, and Processes associated with this policy is required.

5.5 CISO - Emergency Authority

Commented [JA14]: New Comment:- "Disclosure of Information -Administrative Continuity" section was part of the old GP 24 policy. It was removed from the policy this time and would have been added into the security standard's that will follow the policy. Privacy office refers to this particular section on a regular basis. There was a risk that the standard might not be made in time when the policy goes live could cause operational issues for the Privacy team. Recommendation was made to add this section back to the policy.
Recommendation was incorporated

Commented [JA15]: New Comment:- "Role Account" section was part of the old GP 24 policy. It was removed from the policy this time and would have been added into the security standard's that will follow the policy. Privacy office refers to this particular section on a regular basis. There was a risk that the standard might not be made in time when the policy goes live could cause operational issues for the Privacy team. Recommendation was made to add this section back to the policy.
Recommendation was incorporated

Commented [JA16]: New Comment:- Privacy office recommended to
replace the word "must" rather than "should choose to" for use of approved software.
Recommendation was incorporated

Commented [JA17]: New Comment:- Privacy office recommended to
the remove the wording "when available" from section 5.4.1 and replace it with "When approved Electronic Systems are not available" in section 5.4.2. This was recommended to provide clarity to the readers.
Recommendation was incorporated

5.5.1 If an emergency arises that threatens the security of Digital Information or Electronic Systems, the CISO has the authority and responsibility to implement emergency response measures to shut down the risk and to mitigate further damage. Those affected by such actions shall be notified as soon as practicable.

5.5.2 The CISO will immediately report any such emergency response measures to the Executive Team. The Executive Team will work with the CISO to evaluate the risk and review next steps.

6.0 ROLES AND RESPONSIBILITIES

6.1 Chief Information Security Officer

6.1.1 The CISO (or delegate) shall perform a coordinating role in the implementation, administration, and support of this policy by:

a. developing, issuing, and regularly reviewing the Procedures, Standards, Guidelines, Controls, and Processes;

b. providing guidance on compliance with the policy;

c. providing an ongoing security awareness training program;

d. assisting in the investigation of breaches and potential breaches of the policy; and

e. consulting with the Access and Privacy Program at the Archives and Records Management Department to determine the potential privacy impact associated with any information security incident or breach.

Commented [JA18]: New Comment:- Privacy office recommended to
the add the word "Department" to the Archives and Records Management. This was to standardize the language
Recommendation was incorporated

6.2 Operational Leaders

6.2.1 Operational Leaders of Academic or Administrative Units are responsible for maintaining the security of their local Digital Information and Electronic Systems. Their responsibilities include:

a. assigning access, renewing, retiring, or revoking User authorizations within their area of responsibility based upon the User's role within the Unit (Role-Based Access) following the Principle of Least Privilege

b. ensuring that Digital Information and Electronic Systems are secured, with particular care concerning User identification and validation measures;

c. ensuring that Digital Information, within their area of responsibility, is maintained, transmitted, stored, retained and disposed in a secure and consistent manner that adheres to all relevant University policies including Procedures, Standards, Guidelines, Controls, and Processes, record retention schedules and disposal authorities and the *Freedom of Information and Protection of Privacy Act*;

Commented [JA19]:
New Comment:- Privacy office recommended to add retention and disposition to this section. Digital information should be retained and disposed of according to an approved Records Retention Schedule and Disposition Authority. This was to ensure the entire lifecycle of digital information is addressed.
Recommendation was Incorporated

d. ensuring that breaches and potential breaches of this policy occurring within their Unit are reported to the CISO, then continuing to assist in the investigation, while preserving evidence where required;

e. ensuring that technical staff within their Unit are aware of and adhere to this policy and its associated Procedures, Standards, Guidelines, Controls, and Processes;

f. ensuring their technical staff support University security standards in the design, installation, maintenance, training, and use of Digital Information and Electronic Systems; and

g. working with Chief Information Officer ("CIO") and CISO to make training, other information, and resources necessary to support this policy available to their Unit.

7.0 REPORTING

7.1 The CISO will report to the Audit, Risk, and Compliance Committee of the Board of Governors on matters related to the security and use of Digital Information and Electronic Systems.

8.0 RELATED LEGAL, POLICY AUTHORITIES AND AGREEMENTS

8.1 The legal and other University Policy authorities and agreements that may bear on the administration of this policy and may be consulted as needed include but are not limited to:

8.1.1 *University Act*, RSBC 1996, c 468

8.1.2 *Freedom of Information and Protection of Privacy Act*, RSBC 1996, c 165

8.1.3 Enterprise Risk Management (GP 42)

8.1.4 The University's Information Policy Series, including Protection of Privacy (I 10.11)

9.0 ACCESS TO INFORMATION AND PROTECTION OF PRIVACY

9.1 The information and records made and received to administer this policy are subject to the access to information and protection of privacy provisions of British Columbia's *Freedom of Information and Protection of Privacy Act* and the University's Information Policy series.

10.0 RETENTION AND DISPOSAL OF DIGITAL INFORMATION

10.1 Information and records made and received to administer this policy are evidence of the University's actions to guide access to, and the use and security of, Digital Information and Electronic Systems. Digital Information and records must be retained and disposed of in accordance with a records retention schedule approved by the University Archivist.

11.0 POLICY REVIEW

11.1 This policy must be reviewed every five years but may be reviewed as needed.

12.0 POLICY AUTHORITY

12.1 This policy is administered under the authority ~~of the policy is administered under the authority~~ of the Vice-President Finance and Administration.

Commented [JA20]: New Comment:- This sentence was repeated twice. Removed the repeating sentence

13.0 INTERPRETATION

13.1 ~~Nothing in~~ T~~t~~his policy should be interpreted in a manner that is ~~in~~consistent with the University's legal obligations, including its obligations under any relevant collective agreement or employment policy with non-unionized employees.

13.2 Questions of interpretation or application of this policy shall be referred to the Vice-President Finance and Administration ~~who will decide~~for determination, and whose decision shall be final.

14.0 PROCEDURES AND OTHER ASSOCIATED DOCUMENTS

14.1 Appendix A contains the definitions applicable to this policy and its associated Procedures, Standards, Guidelines, Controls, and Processes.

14.2 The Procedures, Standards, Guidelines, Controls, and Processes associated with this policy include but are not limited to:

14.2.1 Digital Information Classification Standard;

14.2.2 Acceptable Use of Electronic Systems Standard;

14.3 The associated Procedures, Standards, Guidelines, Controls, and Processes listed above will be published on the [Web Site TBD].

APPENDIX A - DEFINITIONS - Acceptable Use and Security of Digital Information and Electronic Systems

Date	Number
[TBA]	GP-24 [NEW]
Date of Last Review/Revision	**Mandated Review**
[TBA]	[TBA]

Updated Discussion Draft – September09, 2022

Policy Authority: Vice President Finance and Administration

Parent Policy: Acceptable Use and Security of Digital Information and Electronic Systems (GP-NEW)

1.0 PURPOSE

1.1 The purpose of this Appendix is to define the words used in the Acceptable Use and Security of Digital Information and Electronic Systems Policy [GP-NEW] and its associated procedures, standards, guidelines, controls, and processes.

2.0 DEFINITIONS

2.1 **Chief Information Security Officer ("CISO")** means the position at SFU responsible for Digital Information and Electronic Systems in relation to risk, security, ~~privacy,~~ security technology standards, compliance, and enterprise security architecture.

2.2 **Digital Information** means information that is stored or processed by Electronic Systems to conduct University Business.

2.3 **Electronic Systems** means all electronic devices, computers, applications, storage, networking, infrastructure, or processes used to create, store, transfer, secure, exchange or dispose of all forms of Digital Information, within the services, devices and facilities that are owned, leased, or provided by the University, and that are used to store, process, or transmit Digital Information.

Commented [JA1]: New Comment:- Privacy office had recommended to remove the word "privacy" as there is a Privacy Office and they are responsible for the Privacy regulation. Recommendation was implemented

Commented [JA2]: New Comment:- Privacy office had recommended to remove the definition of "Digital Information and Electronic Systems", since there were separate definitions for "Digital information" and "Electronics Systems". This was causing confusion for the readers.
Recommendation was incorporated

This includes, but is not limited to:

- computers and computing facilities;
- computing hardware and equipment;
- mobile computing devices;
- digital storage media;
- communication gateways and networks;
- email systems;
- telephones or other communication systems; and
- software.

Executive Team is the senior management team of SFU chaired by the President.

2.4

2.5 Internal Information means a class of Digital Information that access is limited to employees and other authorized Users and is stored within a controlled access system. This is the default category, used for information that is not Public Access Information or Regulated Information. Internal Information is available to those employees with a need for access as part of their job duties. Examples of Internal Information include student transcripts, employee emails in their Computing-ID and role-based University email accounts, and employee emergency contact information.

~~Internal Information is means a class of SFU Digital Information that access is limited to employees and other authorized Users and is stored within a controlled access system. This is the default category, used for information that is not Public Access Information or Regulated Information. Internal Information is available to those employees with a need for access as part of their job duties. Restrictions are applied based on a need-to-know basis. Access is assigned by the employee's job responsibilities. Examples of Internal Information include student grades transcripts, employee emails in their Computing-ID and role-based University email accounts, and personal employee emergency contact information.~~

~~2.2~~2.6 **Operational Leader of an Academic or Administrative Unit** means a person who oversees the day- to-day use of Digital Information and Electronic Systems within their faculty or Unit ~~department~~ of the U~~u~~niversity responsible for the overall procurement, development, integration, modification, operation, maintenance and retirement of Electronic Systems. The responsibilities of an Operational Leader may be ~~assigned~~ delegated to a system administrator, a service owner, an academic or non-academic Director or to another position within a specific area of the University.

~~2.3~~2.7 **Principle of Least Privilege** means the concept that a User should only have access rights to information as needed to perform their responsibilities, and no more.

~~2.4~~2.8 **Public Access Information** means a class of Digital Information that is information that is generally available to the public. This information is deemed to be public by legislation or policy. Examples include information contained in the University's annual report, published convocation lists, statistical reports on enrolment and information about an employee's position, function, or remuneration.

Commented [JA3]: New Comment:- The definition for "Executive team" was missing. "Executive Team" is mentioned in the GP 24 section 5.5.2.
Recommendation was implemented

Commented [JA4]: New Comment:- Privacy office had recommended to add more examples i.e. "transcripts, employee emails in their Computing-ID and role-based University email accounts, and employee emergency contact information".
Recommendation was implemented

Commented [JA5]: New Comment:- Privacy office had recommended to add language defining the role of operational leader "responsible for the overall procurement, development, integration, modification, operation, maintenance and retirement of Electronic Systems".
Recommendation was implemented

Commented [JA6]: New Comment:- Privacy office had recommended to simplify the definition of "Principle of Least Privilege".
Recommendation was implemented

2.9 **Regulated Information** means a class of Digital Information ~~which means information~~ of a ~~n extremely~~ sensitive or confidential nature that is protected from general distribution and is stored within a controlled access system. This information ~~is~~ may be protected by legal contract, legislation, or regulation. ~~Special authorization must be obtained before regulated information is made available. The level of access will be determined based on the end-user's role requirements.~~ Examples ~~of limited access information~~ include, but are not limited to, employment and education equity declarations, and records pertaining to disciplinary actions. ~~The authorization and requirements will be tracked by ITS.~~

~~2.5~~2.10 **Role Based Access** means a model to restrict a User's access to certain Digital Information and Electronic Systems based on their role (e.g., prospect, student, alumni, staff, faculty member, retiree). ~~Role Based Access is based on the concept that a User should only have access to the information and systems that they absolutely need to perform their responsibilities, and no more.~~

~~2.6~~ **Service Provider** means a person or company retained under contract to perform services for the University. ~~include technical staff, work units or external service providers/vendors who design, manage, and operate electronic information systems (e.g. project managers, system designers, software developers, business analysts, application administrators, cloud tenant administrators, cloud service providers, or network and system administrators).~~

~~2.11~~

~~**SFU's Digital Information** is means the digital information University Information needed to conduct University Business.~~

~~**2.7** **SFU's Digital Information and Electronic Systems** means all digital University Information and all computers, applications, storage, networking, infrastructure, or processes used to create, store, secure, exchange or dispose of all forms of that Ddigital Iinformation. The systems may reside on premise at an SFU campus, at provincial or federal government site, or at an external vendor site. Either Local IT Staff or ITS teams may manage these systems.~~

~~**2.7** **SFU's Electronic Systems** are means all electronic devices, computers, applications, storage, networking, infrastructure, or processes used to create, store, transfer, secure, exchange or dispose of all forms of Digital Information, within the the services, devices and facilities that are owned, leased, or provided by SFUthe University, and that are used to store, process, or transmit SFU's Digital Information. This includes, but is not limited to:~~

- ~~computers and computing facilities;~~
- ~~computing hardware and equipment;~~
- ~~mobile computing devices;~~
- ~~digital storage media;~~
- ~~communication gateways and networks;~~
- ~~email systems;~~
- ~~telephones or other communication systems; and~~
- ~~software.~~

~~2.8~~2.12 **University** means Simon Fraser University ("SFU").

~~2.9~~2.13 **University Business** means activities in support of the administrative, academic, research, or other mandates of the University.

Commented [JA7]: New Comment:- Privacy office had recommended to simplify the definition of "Regulated Information".
Recommendation was implemented

Commented [JA8]: New Comment:- Privacy office had recommended to simplify the definition of "Role Based Access".
Recommendation was implemented

Commented [JA9]: New Comment:- Privacy office had recommended to simplify the definition of "Service Provider".
Recommendation was implemented

~~2.10~~2.14 **University Community** means all ~~s~~Students and employees of the University, and all people who have a status at the University mandated by legislation or other University policies, including research assistants, post-doctoral fellows, members of Senate and the Board of Governors, volunteers, visiting and emeritus faculty, and visiting researchers.

2.15 **User** means any individual who uses or accesses Digital Information and Electronic Systems ~~working for the University in any capacity, whether paid or unpaid,~~ including University employees, Service Providers, ~~student employees,~~ volunteers, visitors and ~~, as well as~~ students ~~who use or access SFU Digital Information and Electronic Systems~~.

2.16 **Unit** means a group of Users linked by a common interest or purpose, including, but not limited to, faculties, departments, divisions, schools, offices, or centres.

Commented [JA10]: New Comment:- Privacy office had recommended to simplify the definition of "Users". Recommendation was implemented

Commented [JA11]: New Comment:- Privacy office had recommended to add the definition of "Unit". Recommendation was implemented

SFU SIMON FRASER UNIVERSITY
ENGAGING THE WORLD

Policies and Procedures

Fair Use of Information and Communications Technology

SIMON FRASER UNIVERSITY
POLICIES AND PROCEDURES

Date	**Number**
March 23, 1993	GP 24
Revision Date	**Revision No.**
January 29, 2009	A

Preamble

This policy allows those who administer the University's Information and Communications Technology (ICT) resources to do so as transparently as possible, while providing users with essential guidance on their rights and responsibilities.

ICT resources (see section 6) include business tools that facilitate University processes and activities related to its research, teaching and community service mandates. The University recognizes those resources may be the pathway by which controversial points of view and new ideas are disseminated and tested by members of the community.

The University continuously strives to create an environment that provides members of the community with the resources needed to meet the objectives of their work and/or studies, and to create a working and learning environment that promotes full, free and responsible participation by all members.

1.0 Purpose:

1.1 The Purpose of this policy is to:

a) establish the University's right to control and manage its Information and Communications Technology (ICT) resources;

b) inform administrators and users of SFU's ICT resources of their rights and responsibilities regarding the management and use of these

fundamental resources; and

c) make users accountable for their use of the University's ICT resources.

2.0 Policy

2.1 Right of Access

2.1.1 Authorized users of the University's ICT resources have the right to access them without interference by others.

2.1.2 Where users misuse the University's ICT resources, their right of access may be restricted or removed. (See section 2.6.)

2.2 Confidentiality and Privacy Protection

2.2.1 General

The University respects the privacy of those who use the University's ICT resources and protects users' information by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or disposal. The University's ICT staff will comply with the FOIPOP Act and the University's information and privacy policies (I10 series) and will disclose a user's activities and personal information only as permitted or required by law.

2.2.2 Logging of Information

Most activities performed using the University's ICT resources are logged. Information in log files is owned by the University and is routinely examined by ICT support staff to monitor the performance, reliability and security of ICT resources. ICT support must not disclose information learned from or contained within these log files except when authorized in writing to do so by their Director in order to:

a) investigate an alleged violation of this Policy or other related University Policy using the procedure outlined in Appendix II; or to

b) respond to a request for information pursuant to proceedings under the auspices of another University Policy using the procedure outlined in Appendix II; or to

c) ensure administrative continuity (see sections 2.2.3 and 2.2.4).

2.2.3 Disclosure of Information - Administrative Continuity

In cases of the absence, retirement or termination of an employee engaged in administrative duties, there may be occasions where departments need access to that individual's emails or files to conduct business as permitted under section 33.2(c) FOIPOP Act. In such cases the Chair or unit head can obtain access by making a request to the Director, Client and Research Services (CaRS). Any information released under this provision may not be used for any employee discipline or other purpose except administrative continuity and any personal information shall be kept confidential.

2.2.4 Role Accounts

Role accounts (i.e., those granted to a role or organizational position rather than to an individual for business purposes) may be shared amongst authorized users as determined by the appropriate Department Chair/unit head. Information contained in these accounts may be

accessed and disseminated upon the request of the Chair/unit head to the Director, Client and Research Services (CaRS). Users are advised that role accounts should not be used to store personal information as they are subject to access should the University need to do so to conduct its operations.

2.3 Personal Use

2.3.1 Accounts to access ICT resources are issued for the sole use of the person to whom they are issued. Accounts are not to be shared, given, rented, sold or reassigned to any other individual or organization. Role accounts are exceptions to this provision

2.3.2 Incidental personal use of ICT resources is allowed provided that it does not: contravene the law and provisions of this or other University policies; interfere with access to ICT resources by authorized users; or cause the University to incur additional costs (e.g., excessive use of internet bandwidth).

2.4 Commercial Use

2.4.1 The University's ICT resources shall not be used for commercial purposes, for profit-making, or for the benefit of non-SFU organizations unless these purposes are authorized under, and consistent with, the appropriate University policies and procedures. This provision shall not restrict SFU researchers from pursuing their research activities and freely exchanging information.

2.5 Misuse

2.5.1 Misuse of the University's ICT Resources is explicitly prohibited. Activities included under the definition of "misuse" are set out in Section 6.0 Definitions below.

2.6 Protective Measures

2.6.1 The University reserves the right to limit, restrict or terminate user access, and to inspect, copy, remove or otherwise alter any data, files or other ICT resources covered by this policy.

2.6.2 At the direction of the Director, CaRS or designate, interim measures may be taken by duly authorized ICT staff in immediate response to allegations or awareness of misuse. These measures shall remain in force until the matter is resolved by the appropriate University Officer.

3.0 Scope:

3.1 This Policy applies to anyone using the University's ICT resources or using their SFU authorization credentials to access ICT resources provided by other organizations. In the latter case, users are responsible for making themselves aware of, and to comply with, the other organization's "acceptable use" policies.

3.2 This Policy covers all University-owned or -leased ICT resources, whether individually controlled or shared, standalone or networked, and to all activities of individuals accessing University-owned ICT resources from non-University-owned ICT resources (e.g., personal computer, PDA, or other devices).

3.3 From time to time the University may grant access to ICT resources to persons from other organizations through reciprocal sharing agreements with individual organizations or through participation in a federation of organizations. This privilege may be revoked solely at the discretion of the University.

4.0 Roles and Responsibilities:

4.1 The University's ICT resources will be provided and protected by the University to a degree that is reasonable and technically feasible under the guidelines set out by this policy, its associated procedures, section 30 of the FOIPOP Act and any other relevant University policy or procedure (see Appendix 1 for a partial list of such documents).

4.2 The University warrants that it makes reasonable security arrangements for the ICT resources offered; however, SFU stipulates that there are no guarantees regarding the accessibility, reliability or security of said resources.

4.3 The responsibilities of the ICT staff, in priority order, are to maintain the security of the information in the ICT environment, maintain the ICT environment in an operationally available state, and ensure that the ICT resources are accessible to the members of the user community. Where the security of information within the ICT environment is threatened, access to the environment may be restricted until the threat is resolved.

5.0 Authority:

5.1 This policy is administered under the authority of the Chief Information Officer.

6.0 Definitions

Authorization for File Access is the Form required to view information either owned by an Authorized User or pertaining to an Authorized User for which the User has not given permission, except for role accounts (section 2.2.4) or in situations dealing with Administrative continuity (section 2.2.3). An Authorization is normally required to support an investigation or process associated with the application of this or another University Policy.

Authorized Users are those who have current ICT identity credentials granted by an authorized 0fficer of the University.

Confidentiality means keeping personal information private or secret, safe from access, use or disclosure by people who are not authorized to handle that information. (BC Govt. FOIPOP Policy and Procedures Manual.)

FOIPOP Act refers to the Freedom of Information and Protection of Privacy Act and associated Regulations enacted by the Province of British Columbia. Also known as FOIPOP.

ICT Resources Information resources in this document are meant to include any information in digital format, or any hardware or software that make possible the electronic storage and use of such information. This includes, but is not limited to, electronic mail, local databases, externally accessed databases, CD-ROM, motion picture film, recorded magnetic media, photographs, and digitized information. For purposes of this Policy, the "appropriate use of ICT resources" does not refer to managing digital information in terms of its classification, organization, retention or disposal; this is not a records management policy.

Interim measures may include, but are not limited to:

- contact with respondents to establish the veracity of allegations;
- discussions with respondents to informally resolve problems;
- instruction to respondents to cease and desist alleged misuse within a time limit; or
- temporary disabling of respondents' computer accounts or other access.

It is understood that interim measures are to be preemptive and remedial rather than punitive, and will remain in force until the matter is resolved by the appropriate University Officer.

Misuse under this policy encompasses, but is not limited to:

Unlawful Activities:

- Any activity that contravenes federal or provincial legislation, whether or not the activity is reported to the police
- The evidence supporting a suspicion or allegation of unlawful activity will be assessed and misuse will be determined based on a 'Balance of Probabilities' standard
- Knowledge of and compliance with the law is the responsibility of the user

Threats to System Security or Integrity:

- Seeking to gain, or gaining, unauthorized access to ICT resources
- Possessing, creating, transmitting or storing tools, programs, attachments or other materials for the purpose of gaining unauthorized access
- Examining or using without authorization another user's files or programs in transit or in storage
- Unauthorized scanning of other computers on the network
- Preventing rightful access to computer-based information and ICT resources
- Altering, disrupting or otherwise interfering with the integrity of computer-based information and ICT resources, including the passing on of viruses, worms, "trojans" or other "malware"
- Endangering the finite capacity of any system through "chain mail," "flame wars," "bombing," "spamming" or using any method system administrators consider may endanger and/or restrict the access to their accounts by other authorized users
- Impersonating another user (regardless of whether the other user is real or fictitious) by altering individual system identity

Excessive Use of ICT Resources:

- Use of ICT resources in a manner that may result in additional cost to the University
- Use of ICT resources in a manner that consumes resources that would rightfully be available to others.

Contravention of University Policy

- Use of ICT Resources contrary to another University policy will be addressed as applicable under the relevant policy.

Personal is defined as relating to, concerning, or affecting a person as a private individual (rather than as a member of a group or the public, or in a public or professional capacity); individual, private; one's own.

Personal Information means recorded information about an identifiable individual other than contact information (FOIPOP Act).

Privacy means the state or condition of being alone, undisturbed, or free from public attention, as a matter of choice or right; seclusion, freedom from interference or intrusion. (BC Govt. FOIPOP Policy and Procedures Manual)

Record includes books, documents, maps, drawings, photographs, letters, vouchers, papers and any other thing on which information is

recorded or stored by graphic, electronic, mechanical or other means, but does not include a computer program or any other mechanism that produces records (FOIPOP Act). Note that this definition of "record" specifically excludes ICT resources (i.e., a computer program or any other mechanism that produces records).

APPENDIX I

This Policy should be read and understood in conjunction with the following University Policies and documents, and with the University's Statement on Values and Commitments:

A 30.01 Faculty Code of Ethics
AD 1.06 Commercial Activities and Advertising
AD 1.12 Selling, Serving and Advertising Liquor
GP 18 Human Rights
GP 25 Response to Violence and Threatening Behaviour
GP 30 Interpretation Policy
I 10.04 Access to Information and Protection of Privacy
R 30.03 Intellectual Property Policy
T 10.01 Code of Student Conduct
T 10.02 Code of Academic Honesty
Applicable Residence and Housing agreements/contracts

APPENDIX II – Procedure to Authorize File Access

An Authorization for File Access is required to view information either owned by an Authorized User or pertaining to an Authorized User for which the User has not given permission, except for role accounts (section 2.2.4) or in situations dealing with Administrative continuity (section 2.2.3). An Authorization is normally required to support an investigation or process associated with the application of this or another University Policy.

Log files and file directories are system resources and are routinely monitored by duly authorized system support staff to maintain the security, reliability, accessibility, and performance of the University's ICT resources. Notwithstanding these, systems staff must not divulge any information pertaining to the activities of an Authorized User to anyone other than other duly authorized system support staff.

Neither the Authorization forms nor the information arising from their use may be transmitted via any insecure communications media. E.g., email is neither acceptable nor sufficient.

1. If the Authorization for File Access is sought to support an allegation or suspicion of misuse under this policy, an Authorization for File Access Form must be completed by the person making the claim.

2. If the Authorization for File Access is sought to support the application of another University Policy, the Authorization for File Access Form shall be completed by the person duly appointed to investigate under the auspices of the applicable University Policy.

3. The Authorization for File Access must contain the following information:

The name of the applicant
The date of the application to access the files

The ID of the Authorized User for which the application is requested

The date that the file access must cease/end

The Name of the Authorized User for which the application is requested

The University Policy under which the application is requested

A description containing the reason for the request and the information requested

The names of staff/faculty who are authorized to access this information when it is produced

The name, phone number, and signature of the person requesting the information

4. The completed Authorization for File Access form should be taken to the Director, CaRS. The request will be reviewed to ensure that the information requested is possible to produce, that it is sufficient to meet the objective of the request, and that the resources required to produce the information are available. (Note: Requests for information from backup tapes or log files can take several days to produce.) If the Director, CaRS agrees with the technical aspects of the requests and has the resources available to produce the information the Director, CaRS will approve the form.

5. The Director, CaRS will then take the form to seek the approval of two University Vice-Presidents. The requestor may or may not accompany the Director when seeking the Vice-Presidents' approval.

6. The information will be assembled and two copies prepared on an appropriate storage media (usually a write once CD or DVD). The information will be assembled by the appropriate systems support person, who will initial the media in order to identify it later if necessary. One copy will be stored in a confidential file with the original of the approved Authorization for File Access form, and the second will be given to the requestor.

APPENDIX III – Authorization for File Access

Sample Form Attached

GP24_Request_for_Access_to_Personal_Information_Contained_In_ICT_Resources.pdf

Request for Access to Personal Information Contained in ICT Resources

SFU SIMON FRASER UNIVERSITY

POLICY AND PROCEDURES

ACCEPTABLE USE AND SECURITY OF DIGITAL AND ELECTRONIC SYSTEMS

Date	**Number**
March 23, 1993	GP-24 [NEW]
Date of Last Review/Revision	**Mandated Review**
January 29, 2002	[TBA]

Updated Discussion Draft: September 09, 2022

Policy Authority: Vice President Finance and Administration

Associated Procedure(s): See section 14 of this Policy

EXECUTIVE SUMMARY

Simon Fraser University (the "University~~"SFU~~") is committed to protecting the Digital Information and Electronic Systems that are critical to teaching, research, business operations, and other University activities and that are vital ~~critical~~ to the communities we support. This policy establishes standards and guidelines to:

- secure the Regulated ~~personally identifiable~~ Digital Information that our Electronic Systems contain;
- maintain the integrity of those Electronic Systems, and
- safeguard the financial assets of the University.

Access to, and use of, Digital Information and Electronic Systems will be granted using Role-Based Access principles. This enables Users to access Digital Information and Electronic Systems only as required for their role at the University, and only at the level required to perform their role. Everyone who accesses or uses Digital Information and Electronic Systems must do so ethically, responsibly, lawfully, and in a manner consistent with the Procedures, Standards, Guidelines, Controls, and Processes associated with this and any other relevant University p~~P~~olicypolicy or procedure.

Commented [JA1]: New Comment: - Privacy office had recommended that we mention University rather than SFU. Recommendation was incorporated

Commented [JA2]: New Comment:- Privacy office recommended to change the word Critical as it was used twice in the same sentence. Recommendation was implemented with the change of "Critical" to "Vital"

Commented [JA3]: New Comment:- Privacy office recommended to add the term sensitive information as the security of both sensitive and personally identified information must be addressed.
Recommendation was incorporated by adding the word Regulated this in in compliance with the definition provided in Appendix A

Commented [JA4]: New Comment:- Privacy office had recommended that we add "any other relevant University policy or procedure".
Recommendation was incorporated

TABLE OF CONTENTS

Contents

1.0 PREAMBLE

1.1 The University will strive to balance the need for security with the open pursuit of academic activities. Security concerns may place limits on the way in which work is done, but not on the research or inquiry that is pursued. When limitations are needed, the University will make reasonable efforts to consult with person(s) impacted to attempt to find appropriate and workable solutions.

1.2 Proper management of the security risks associated with access to and use of Digital Information and Electronic Systems is imperative to support the University's academic, research, and administrative activities.

1.3 To ensure Digital Information and Electronic Systems remain secure, to a degree that is reasonable and technically feasible and in accordance with FIPPA, the University will grant access to Users by utilizing Role-Based Access principles and security controls.

1.4 Each User of Digital Information and Electronic Systems is responsible for abiding by the University's Role-Based Access principles and security controls.

2.0 PURPOSE

2.1 This policy, together with its associated Procedures, Standards, Guidelines, Controls, and Processes referenced in section 14, establishes the University's expectations for access to, and use of, Digital Information and Electronic Systems.

3.0 SCOPE AND JURISDICTION

3.1 This policy applies to all Digital Information and Electronic Systems

3.2 This policy applies to all Service Providers and members of the University Community who are authorized to access and use Digital Information and Electronic Systems. ~~for the purpose of creating, storing, transmitting, using, or disposing of SFU Digital Information.~~

~~This policy only applies to Ddigital Iinformation and, Electronic Systems and the University's digital record-keeping processes.~~

3.3 A breach of this policy may result in the University restricting or withdrawing a User's access to Digital Information and Electronic Systems, including computing privileges and network access.

4.0 DEFINITIONS

4.1 See Appendix A for the definitions of words used in this policy and its associated Procedures, Standards, Guidelines, Controls, and Processes.

5.0 POLICY

Commented [JA5]: New Comment:- Privacy office had recommended to add wording "to a degree that is reasonable and technically feasible and in accordance with FIPPA". Recommendation was incorporated

Commented [JA6]: New Comment:- Privacy office had recommended to remove wording "both administrative and academic" from 3.1 and 3.2, as this was covered in the definition of Digital Information and Electronic Systems. Recommendations were implemented

Commented [JA7]: New Comment:- Privacy office had recommended to remove wording "for the purpose of creating , storing, transmitting, using, or disposing SFU Digital Information" from 3.2, as this was covered in the definition of Digital Information and Electronic Systems. Privacy office also recommended to add "Service Providers" in the sentence.
Recommendations were implemented

Commented [JA8]: New Comment:- Privacy office had recommended to remove wording "for the purpose of creating , storing, transmitting, using, or disposing SFU Digital Information" from 3.2, as this was covered in the definition of Digital Information and Electronic Systems. Privacy office also recommended to add "Service Providers" in the sentence.
Recommendations were implemented

Commented [JA9]: New Comment:- Privacy office had recommended to remove wording "This policy only applies to Digital Information and Electronic Systems and the University's digital record-keeping security processes." As this was covered in 3.1. and 3.2
Recommendation was implemented

Commented [JA10]: New Comment:- Privacy office had recommended to move this section from 5.2.2 to 3.3. As this section would impact the entire user community.
Recommendation was incorporated

5.1 Role-Based Access to Digital Information and Electronic Systems

5.1.1 The University will utilize Role-Based Access principles to grant Users access to Digital Information and Electronic Systems. Role-Based Access enables Users to access information and systems only as required for their role at the University, and only at the level required to perform their role.

5.2 Use of Digital Information and Electronic Systems

5.2.1 All Users must:

a. use Digital Information and Electronic Systems responsibly, lawfully, ethically, in accordance with the User's Role-Based Access, and in adherence to license agreements.

~~b. ensure the security of the SFU's Digital Information and Electronic Systems by:~~

~~i. applying the Digital Information Classification Standard to determine which class of SFU's Digital Information is appropriate: Internal Information, Public Access Information or Regulated Information; and~~

~~ii. applying the Minimum Digital Information Security Standards for SFU's Digital Information and the Digital Information Domain Standards applicable to each classification of SFU's \ Digital Information.~~

~~5.2.2 A breach of this policy may result in the University restricting or withdrawing a User's access to SFU's Digital Information and Electronic Systems, including computing privileges and network access.~~

5.3 Security of Digital Information and Electronic Systems

5.3.1 All Users of Digital Information and Electronic Systems must take appropriate steps to ensure security by ~~(see section 5.2.1, above):~~

i. applying the Digital Information Classification Standard to determine which class of Digital Information is appropriate: Internal Information, Public Access Information or Regulated Information; and

ii. applying the digital information security and domain Standards applicable to each classification of Digital Information.

~~5.3.1~~5.3.2 All Operational Leaders ~~owners~~ and Service Providers of Digital Information and Electronic Systems, and those who are responsible for maintaining and administering them, must

Commented [JA11]: New Comment:- Digital Library Services had recommended to add "and in adherence to license agreement". Digital Library Services invoke GP 24 when end users contravene library policies or license agreements.
Recommendation was incorporated

Commented [JA12]: New Comment:- Privacy office had recommended to move this section from 5.2.1 b to 5.3.1. This section was referred from 5.3, this section is more suitable under the "Security of Digital Information and Electronic Systems".
Recommendation was implemented

Commented [JA13]: New Comment:- The term owner was overlapping with the Operational Leader. Privacy office recommended to remove owner and state Operational Leader. Operational Leader is also defined in Appendix
Recommendation was implemented

protect the systems from cybersecurity or other threats by managing and remediating any vulnerabilities throughout the Electronic System's lifecycle.

5.3.3 Disclosure of Information - Administrative Continuity

In cases of the absence, retirement or termination of an employee engaged in administrative duties, there may be occasions where Units need access to that individual's emails or files to conduct business as permitted under section FIPP Act (RSBC 1996, c. 165). In such cases the Unit head can obtain access by making a request to the Chief Privacy Officer. Any information released under this provision may not be used for any employee discipline or other purpose except administrative continuity and any personal information shall be kept confidential.

5.3.4 Role Accounts

Role accounts (that is, those accounts granted to a role or organizational position rather than to an individual for business purposes) may be shared amongst Users as determined by the appropriate Operational Leader. Role accounts must have one responsible owner as appointed by the Operational Leader but may be shared amongst Users as determined by the appropriate Operational Leader. Role accounts cannot be used to store Personal Information as they are subject to access by the University to conduct its operations. The Chief Information Security Officer has the authority to permit an Operational Leader to access and disseminate the information contained in a Role account. Role accounts cannot be used to share licensed software in a manner that may violate the license. Use of Role accounts may be prohibited in specific systems and processes if the use of Role accounts fails to meet regulatory or legislative requirements.

5.4 Use of Non-University Systems for University Business

5.4.1 To optimize the security of Digital Information and Electronic Systems and to ensure administrative effectiveness and the best use of University resources, Units ~~should choose to~~must use approved Electronic Systems~~, when available~~.

5.4.2 When approved Electronic Systems are not available Users or Units who wish to store, transmit, use, or dispose of Regulated Information or Internal Information using systems other than Electronic Systems must be pre-authorized by the Chief Information Security Officer ("CISO") to do so. Once approved, adherence to the Procedures, Standards, Guidelines, Controls, and Processes associated with this policy is required.

5.5 CISO - Emergency Authority

Commented [JA14]: New Comment:- "Disclosure of Information -Administrative Continuity" section was part of the old GP 24 policy. It was removed from the policy this time and would have been added into the security standard's that will follow the policy. Privacy office refers to this particular section on a regular basis. There was a risk that the standard might not be made in time when the policy goes live could cause operational issues for the Privacy team. Recommendation was made to add this section back to the policy.
Recommendation was incorporated

Commented [JA15]: New Comment:- "Role Account" section was part of the old GP 24 policy. It was removed from the policy this time and would have been added into the security standard's that will follow the policy. Privacy office refers to this particular section on a regular basis. There was a risk that the standard might not be made in time when the policy goes live could cause operational issues for the Privacy team. Recommendation was made to add this section back to the policy.
Recommendation was incorporated

Commented [JA16]: New Comment:- Privacy office recommended to
replace the word "must" rather than "should choose to" for use of approved software.
Recommendation was incorporated

Commented [JA17]: New Comment:- Privacy office recommended to
the remove the wording "when available" from section 5.4.1 and replace it with "When approved Electronic Systems are not available" in section 5.4.2. This was recommended to provide clarity to the readers.
Recommendation was incorporated

5.5.1 If an emergency arises that threatens the security of Digital Information or Electronic Systems, the CISO has the authority and responsibility to implement emergency response measures to shut down the risk and to mitigate further damage. Those affected by such actions shall be notified as soon as practicable.

5.5.2 The CISO will immediately report any such emergency response measures to the Executive Team. The Executive Team will work with the CISO to evaluate the risk and review next steps.

6.0 ROLES AND RESPONSIBILITIES

6.1 Chief Information Security Officer

6.1.1 The CISO (or delegate) shall perform a coordinating role in the implementation, administration, and support of this policy by:

a. developing, issuing, and regularly reviewing the Procedures, Standards, Guidelines, Controls, and Processes;

b. providing guidance on compliance with the policy;

c. providing an ongoing security awareness training program;

d. assisting in the investigation of breaches and potential breaches of the policy; and

e. consulting with the Access and Privacy Program at the Archives and Records Management Department to determine the potential privacy impact associated with any information security incident or breach.

Commented [JA18]: New Comment:- Privacy office recommended to
the add the word "Department" to the Archives and Records Management. This was to standardize the language
Recommendation was incorporated

6.2 Operational Leaders

6.2.1 Operational Leaders of Academic or Administrative Units are responsible for maintaining the security of their local Digital Information and Electronic Systems. Their responsibilities include:

a. assigning access, renewing, retiring, or revoking User authorizations within their area of responsibility based upon the User's role within the Unit (Role-Based Access) following the Principle of Least Privilege

b. ensuring that Digital Information and Electronic Systems are secured, with particular care concerning User identification and validation measures;

c. ensuring that Digital Information, within their area of responsibility, is maintained, transmitted, stored, retained and disposed in a secure and consistent manner that adheres to all relevant University policies including Procedures, Standards, Guidelines, Controls, and Processes, record retention schedules and disposal authorities and the *Freedom of Information and Protection of Privacy Act*;

Commented [JA19]:
New Comment:- Privacy office recommended to add retention and disposition to this section. Digital information should be retained and disposed of according to an approved Records Retention Schedule and Disposition Authority. This was to ensure the entire lifecycle of digital information is addressed.
Recommendation was Incorporated

d. ensuring that breaches and potential breaches of this policy occurring within their Unit are reported to the CISO, then continuing to assist in the investigation, while preserving evidence where required;

e. ensuring that technical staff within their Unit are aware of and adhere to this policy and its associated Procedures, Standards, Guidelines, Controls, and Processes;

f. ensuring their technical staff support University security standards in the design, installation, maintenance, training, and use of Digital Information and Electronic Systems; and

g. working with Chief Information Officer ("CIO") and CISO to make training, other information, and resources necessary to support this policy available to their Unit.

7.0 REPORTING

7.1 The CISO will report to the Audit, Risk, and Compliance Committee of the Board of Governors on matters related to the security and use of Digital Information and Electronic Systems.

8.0 RELATED LEGAL, POLICY AUTHORITIES AND AGREEMENTS

8.1 The legal and other University Policy authorities and agreements that may bear on the administration of this policy and may be consulted as needed include but are not limited to:

8.1.1 *University Act*, RSBC 1996, c 468

8.1.2 *Freedom of Information and Protection of Privacy Act*, RSBC 1996, c 165

8.1.3 Enterprise Risk Management (GP 42)

8.1.4 The University's Information Policy Series, including Protection of Privacy (I 10.11)

9.0 ACCESS TO INFORMATION AND PROTECTION OF PRIVACY

9.1 The information and records made and received to administer this policy are subject to the access to information and protection of privacy provisions of British Columbia's *Freedom of Information and Protection of Privacy Act* and the University's Information Policy series.

10.0 RETENTION AND DISPOSAL OF DIGITAL INFORMATION

10.1 Information and records made and received to administer this policy are evidence of the University's actions to guide access to, and the use and security of, Digital Information and Electronic Systems. Digital Information and records must be retained and disposed of in accordance with a records retention schedule approved by the University Archivist.

11.0 POLICY REVIEW

11.1 This policy must be reviewed every five years but may be reviewed as needed.

12.0 POLICY AUTHORITY

12.1 This policy is administered under the authority ~~of the policy is administered under the authority~~ of the Vice-President Finance and Administration.

Commented [JA20]: New Comment:- This sentence was repeated twice. Removed the repeating sentence

13.0 INTERPRETATION

13.1 ~~Nothing in~~ T~~t~~his policy should be interpreted in a manner that is ~~in~~consistent with the University's legal obligations, including its obligations under any relevant collective agreement or employment policy with non-unionized employees.

13.2 Questions of interpretation or application of this policy shall be referred to the Vice-President Finance and Administration ~~who will decide~~for determination, and whose decision shall be final.

14.0 PROCEDURES AND OTHER ASSOCIATED DOCUMENTS

14.1 Appendix A contains the definitions applicable to this policy and its associated Procedures, Standards, Guidelines, Controls, and Processes.

14.2 The Procedures, Standards, Guidelines, Controls, and Processes associated with this policy include but are not limited to:

14.2.1 Digital Information Classification Standard;

14.2.2 Acceptable Use of Electronic Systems Standard;

14.3 The associated Procedures, Standards, Guidelines, Controls, and Processes listed above will be published on the [Web Site TBD].

APPENDIX A – DEFINITIONS - Acceptable Use and Security of Digital Information and Electronic Systems

Date [TBA]	**Number** GP-24 [NEW]
Date of Last Review/Revision [TBA]	**Mandated Review** [TBA]

Updated Discussion Draft – September09, 2022

Policy Authority: Vice President Finance and Administration

Parent Policy: Acceptable Use and Security of Digital Information and Electronic Systems (GP-NEW)

1.0 PURPOSE

1.1 The purpose of this Appendix is to define the words used in the Acceptable Use and Security of Digital Information and Electronic Systems Policy [GP-NEW] and its associated procedures, standards, guidelines, controls, and processes.

2.0 DEFINITIONS

2.1 **Chief Information Security Officer ("CISO")** means the position at SFU responsible for Digital Information and Electronic Systems in relation to risk, security, ~~privacy,~~ security technology standards, compliance, and enterprise security architecture.

2.2 **Digital Information** means information that is stored or processed by Electronic Systems to conduct University Business.

2.3 **Electronic Systems** means all electronic devices, computers, applications, storage, networking, infrastructure, or processes used to create, store, transfer, secure, exchange or dispose of all forms of Digital Information, within the services, devices and facilities that are owned, leased, or provided by the University, and that are used to store, process, or transmit Digital Information.

Commented [JA1]: New Comment:- Privacy office had recommended to remove the word "privacy" as there is a Privacy Office and they are responsible for the Privacy regulation. Recommendation was implemented

Commented [JA2]: New Comment:- Privacy office had recommended to remove the definition of "Digital Information and Electronic Systems", since there were separate definitions for "Digital information" and "Electronics Systems". This was causing confusion for the readers.
Recommendation was incorporated

This includes, but is not limited to:

- computers and computing facilities;
- computing hardware and equipment;
- mobile computing devices;
- digital storage media;
- communication gateways and networks;
- email systems;
- telephones or other communication systems; and
- software.

Executive Team is the senior management team of SFU chaired by the President.

2.4

2.5 **Internal Information** means a class of Digital Information that access is limited to employees and other authorized Users and is stored within a controlled access system. This is the default category, used for information that is not Public Access Information or Regulated Information. Internal Information is available to those employees with a need for access as part of their job duties. Examples of Internal Information include student transcripts, employee emails in their Computing-ID and role-based University email accounts, and employee emergency contact information.

~~Internal Information is means a class of SFU Digital Information that access is limited to employees and other authorized Users and is stored within a controlled access system. This is the default category, used for information that is not Public Access Information or Regulated Information. Internal Information is available to those employees with a need for access as part of their job duties. Restrictions are applied based on a need-to-know basis. Access is assigned by the employee's job responsibilities. Examples of Internal Information include student grades transcripts, employee emails in their Computing-ID and role-based University email accounts, and personal employee emergency contact information.~~

~~2.1~~2.6 **Operational Leader of an Academic or Administrative Unit** means a person who oversees the day- to-day use of Digital Information and Electronic Systems within their faculty or Unit ~~department~~ of the U~~u~~niversity responsible for the overall procurement, development, integration, modification, operation, maintenance and retirement of Electronic Systems. The responsibilities of an Operational Leader may be ~~assigned~~ delegated to a system administrator, a service owner, an academic or non-academic Director or to another position within a specific area of the University.

~~2.2~~2.7 **Principle of Least Privilege** means the concept that a User should only have access rights to information as needed to perform their responsibilities, and no more.

~~2.3~~2.8 **Public Access Information** means a class of Digital Information that is information that is generally available to the public. This information is deemed to be public by legislation or policy. Examples include information contained in the University's annual report, published convocation lists, statistical reports on enrolment and information about an employee's position, function, or remuneration.

Commented [JA3]: New Comment:- The definition for "Executive team" was missing. "Executive Team" is mentioned in the GP 24 section 5.5.2.
Recommendation was implemented

Commented [JA4]: New Comment:- Privacy office had recommended to add more examples i.e. "transcripts, employee emails in their Computing-ID and role-based University email accounts, and employee emergency contact information".
Recommendation was implemented

Commented [JA5]: New Comment:- Privacy office had recommended to add language defining the role of operational leader "responsible for the overall procurement, development, integration, modification, operation, maintenance and retirement of Electronic Systems".
Recommendation was implemented

Commented [JA6]: New Comment:- Privacy office had recommended to simplify the definition of "Principle of Least Privilege".
Recommendation was implemented

2.9 **Regulated Information** means a class of Digital Information ~~which means information~~ of a ~~n extremely~~ sensitive or confidential nature that is protected from general distribution and is stored within a controlled access system. This information ~~is~~ may be protected by legal contract, legislation, or regulation. ~~Special authorization must be obtained before regulated information is made available. The level of access will be determined based on the end-user's role requirements.~~ Examples ~~of limited access information~~ include, but are not limited to, employment and education equity declarations, and records pertaining to disciplinary actions. ~~The authorization and requirements will be tracked by ITS.~~

~~2.4~~2.10 **Role Based Access** means a model to restrict a User's access to certain Digital Information and Electronic Systems based on their role (e.g., prospect, student, alumni, staff, faculty member, retiree). ~~Role Based Access is based on the concept that a User should only have access to the information and systems that they absolutely need to perform their responsibilities, and no more.~~

~~2.5~~ **Service Provider** means a person or company retained under contract to perform services for the University. ~~include technical staff, work units or external service providers/vendors who design, manage, and operate electronic information systems (e.g. project managers, system designers, software developers, business analysts, application administrators, cloud tenant administrators, cloud service providers, or network and system administrators).~~

~~2.11~~

~~2.6 **SFU's Digital Information** is means the digital information University Information needed to conduct University Business.~~

~~2.7 **SFU's Digital Information and Electronic Systems** means all digital University Information and all computers, applications, storage, networking, infrastructure, or processes used to create, store, secure, exchange or dispose of all forms of that Ddigital Iinformation. The systems may reside on premise at an SFU campus, at provincial or federal government site, or at an external vendor site. Either Local IT Staff or ITS teams may manage these systems.~~

~~2.8 **SFU's Electronic Systems** are means all electronic devices, computers, applications, storage, networking, infrastructure, or processes used to create, store, transfer, secure, exchange or dispose of all forms of Digital Information, within the the services, devices and facilities that are owned, leased, or provided by SFUthe University, and that are used to store, process, or transmit SFU's Digital Information. This includes, but is not limited to:~~

- ~~computers and computing facilities;~~
- ~~computing hardware and equipment;~~
- ~~mobile computing devices;~~
- ~~digital storage media;~~
- ~~communication gateways and networks;~~
- ~~email systems;~~
- ~~telephones or other communication systems; and~~
- ~~software.~~

~~2.9~~2.12 **University** means Simon Fraser University ("SFU").

~~2.10~~2.13 **University Business** means activities in support of the administrative, academic, research, or other mandates of the University.

Commented [JA7]: New Comment:- Privacy office had recommended to simplify the definition of "Regulated Information".
Recommendation was implemented

Commented [JA8]: New Comment:- Privacy office had recommended to simplify the definition of "Role Based Access".
Recommendation was implemented

Commented [JA9]: New Comment:- Privacy office had recommended to simplify the definition of "Service Provider".
Recommendation was implemented

~~2.11~~2.14 **University Community** means all ~~s~~Students and employees of the University, and all people who have a status at the University mandated by legislation or other University policies, including research assistants, post-doctoral fellows, members of Senate and the Board of Governors, volunteers, visiting and emeritus faculty, and visiting researchers.

2.15 **User** means any individual who uses or accesses Digital Information and Electronic Systems ~~working for the University in any capacity, whether paid or unpaid,~~ including University employees, Service Providers, ~~student employees,~~ volunteers, visitors and ~~, as well as~~ students ~~who use or access SFU Digital Information and Electronic Systems~~.

2.16 **Unit** means a group of Users linked by a common interest or purpose, including, but not limited to, faculties, departments, divisions, schools, offices, or centres.

Commented [JA10]: New Comment:- Privacy office had recommended to simplify the definition of "Users". Recommendation was implemented

Commented [JA11]: New Comment:- Privacy office had recommended to add the definition of "Unit". Recommendation was implemented