IT Communications Services Governance Framework

Purpose

This document describes the IT communications governance framework for University of Saskatchewan (U of S). It identifies designated roles within the university that have specific decision-making accountabilities regarding IT communications services. This framework exists to support the university's IT Communications Services Policy and is meant to be read in conjunction with the university's data governance framework.

This framework establishes a well-aligned governance structure by delineating the business and ICT roles, and facilitating holistic and inclusive IT communications services decision-making.

Data Governance Roles and Responsibilities

The Data management Policy and the university's data classifications need to be considered when determining which IT communications services to use if transmitting university data as there may be privacy and security implications. IT communications services should not be regarded as a secure medium for the communication of confidential or restricted data and should not be depended on to retain university data.

The U of S data governance framework establishes five roles within the data governance organizational structure. The five roles are: Data Trustees, Data Stewards, Data Custodians, Data Guardians and End Users. Refer to the data governance framework for a list of the university's data trustees.

Protecting the university's data is a responsibility shared by all members of the university community.

With respect to IT communications service, the five roles data governance roles have the following accountabilities.

Data Trustees

Data Trustees have IT communications services decision-making accountabilities related to the following:

- The Data Trustee determines eligibility for IT communications services for their functional area, including decisions regarding aspects such as naming standards and provisioning or de-provisioning of accounts.
- The Data Trustee is involved when there is a need to recover evidence while investigating allegations of misconduct and managing actual or potential criminal or civil litigation in which the university is or may become a party.
- The appropriate Data Trustee or their designate must be consulted on decisions regarding unsolicited communication to large segments of the university community (e.g. all students, all faculty and staff, all employees, all alumni). See Appendix A for more information.
- The Vice-President Finance and Resources is the designated Head and Data Trustee for Freedom of Information and Protection of Privacy matters. The Head has authority for all decisions made on behalf of the university pursuant to the Freedom of Information and Protection of Privacy Policy and under the Act.
    - The Access and Privacy Office advises on and coordinates freedom of information and protection of privacy matters. See the Access and Privacy section below for more information.
- The Principal Investigator is accountable for all decisions regarding their research data.

The table below outlines which Data Trustee is responsible for decisions related to which groups of individuals at the university.

Affiliation	Description	Trustee Responsible
Faculty	Anyone in or out of scope, includes both faculty and sessional lecturers.	Associate Vice-President, People & Resources
Staff	Includes all regular employees of the U of S (e.g. full and part-time employees that work directly for the university).	Associate Vice-President, People & Resources
Student	Any individual registered or eligible to register (according to the student information system) in the current or future term.	Vice-Provost, Teaching, Learning and Student Experience
Employees (Other)	Other U of S employees, such as student markers and individuals who receive non-employment income such as scholarships from the university.	Associate Vice-President, People & Resources
Alumni and Retirees	Alumni according to the University Relations data.	Vice-President, University Relations
Professor Emeritus/Emerita	*Professor Emeritus/Emerita* as bestowed by the President.	Vice-Provost, Faculty Relations

Data Stewards

Data Stewards, as defined by Data Trustees, have IT communications services decision-making accountabilities related to the following:

- The Data Steward determines the appropriate IT communications services for use as part of their business processes.
- The Data Steward determines appropriate access to IT communications services records when required for urgent/time-sensitive business continuity reasons due to the absence of a faculty or staff member for reasons such as leaves, terminations, or attrition. This also includes decisions around:
    - Granting access to email inbox contents (existing email at time of departure, including any personal information and any pre-employment email of the individual if they are also alumni).
    - Setting autoreplies or forwarding accounts.
    - Handling new inbound email to the account following a termination (for continuity of service).
    - Limiting / restricting outbound email from account.

Data Custodians

Data Custodians, as defined by Data Stewards, have IT communications services decision-making accountabilities related to the following:

- Data Custodians will help faculty and staff make records management decisions for their business area. The content of the IT communications services records, not the delivery method, determines how the message should be treated. See the Management of University Records Policy. This includes when individuals change jobs within the university as IT communications services records continue to remain with the individual as long as they are employed by the university.
- Data Custodians will help establish and observe appropriate security measures in maintaining records containing personal or other confidential information in their possession or under their control.

Data Guardians

Data Guardians, personnel in Information and Communications Technology (ICT), have IT communications services decision-making accountabilities related to the following:

- Data Guardians determine the type and best way to deliver the correct IT communications services for the university.
- Data Guardians determine how contact information of account holders will be managed in university systems and directories.
- Data Guardians determine the best way to provide access to IT communications services. Sometimes access may be provided using the university's accounts, sometimes access may be provided indirectly (i.e. single sign on authentication to cloud services, administration of a corporate cell phone plan, etc.)
- Data Guardians determine the best way to protect the university from viruses, spam, phishing, and other security risks, including when to reject IT communications that that could compromise the university network and any systems connected to it.
- Data Guardians determine the disaster recovery mechanisms and back up processes to support the university.

ICT will only access or provide access to IT communications records that have been requested under LAFOIP (through the Access and Privacy Office), under court order, or for exigent business reasons (e.g. absence of a faculty or staff member for reasons such as leaves, terminations, or attrition or fraud investigations) following due process and in consultation with the Data Trustee as appropriate. When possible, account holders will be notified promptly when their IT communications services records have been accessed.

Individuals Who Use IT Communications Services

Members of the university community have responsibilities both as individuals and in relation to their affiliation and role with the university. Individuals may have multiple affiliations, but their primary affiliation, combined with their role, will determine their responsibilities. The affiliation hierarchy is outlined in the next section.

- Members of the community will determine how they want to identify, separate, and remove unwanted and unneeded junk mail, non-records, transitory information, and personal mail from their IT communication services.
- Members of the community will determine if they want to make personal use of IT communications services given that it is a university service and subject to access requests. Personal use must not compromise the business of the university, must not increase the university's costs, must not expose the university to additional risk, must not damage the university's reputation and must not be part of an activity that the account holder does for personal profit.
- Faculty and staff will, in consultation with their Data Custodians, determine which of their communications records are required for records retention purposes.

Affiliations, Roles, and Accounts

Affiliations are broad categories that define the different types of relationships that an individual may have with the university (e.g. faculty, staff, student, alumni, etc.). An individual may have more than one affiliation. Affiliations are used to group members of the community who have similar needs at a very high level.

Roles are tied to the duties we perform in relation to our affiliation with the university. Roles could include instructor, researcher, analyst, director, etc.

The relationship individuals have with the university changes with time. Individuals transition through different affiliations with the university, from student to alumni, employee to retiree, and even through different types of employment relationships, from student marker to intern, staff to sessional lecturer, student marker to faculty member. Members of the university community can (and do) have multiple affiliations with the university. For example, an individual can have both a student and a staff affiliation or a staff and an alumni affiliation. Individuals can also have multiple roles, for example if an individual holds jobs in two different departments simultaneously.

Affiliation Hierarchy

The members' affiliation(s) and role(s) with the university determine the type of IT communications services to which they have access, the duration for which they have access to those services, and their associated responsibilities for use of the services.

Members of the university community may have multiple affiliation(s) and role(s) with the university. These roles can change with time. However, at any given time, a member can have only one primary affiliation. The primary affiliation is assigned based on the hierarchy below.

Data about affiliations is fetched from the human resources system, the student information system, and the alumni database. The hierarchy ranking is as follows:

1. Faculty — Anyone in or out of scope, includes both faculty and sessional lecturers.
2. Staff — Includes all regular employees of the U of S (e.g. full and part-time employees that work directly for the university).
3. Student — Any individual registered or eligible to register (according to the student information system) in the current or future term.
4. Employees (Other) — Other U of S employees, such as student markers and individuals who receive non-employment income such as scholarships from the university.
5. Alum — Alumni according to the University Relations data.
6. Affiliate — Works for an organization to which the U of S provides services, such as STM, CLS, and Prairie Swine Center. Currently, retirees and *professors emeriti* are included in affiliate, but there are plans to have a separate affiliation for retirees and *professors emeriti*.
7. Guest — Individuals that have registered for temporary guest accounts. These accounts do not have an NSID.
8. Applicant — A person who has applied for admission but has not yet been accepted as a student.

Therefore, if an individual has both the Faculty and Staff affiliation, Faculty is their primary affiliation. If an individual has both a Staff and Alum affiliation, Staff is their primary affiliation. The Data Trustee for an individual's primary affiliation makes the final decisions related to their IT communication services.

University Accounts

As stated in the university's Computer Use Policy, "Access to the University's computing facilities and services is provided through an account issued to each individual. No one is authorized to use any University computing facility or service without such an account. Computer accounts and authorization are not transferable. The person to whom authorization is granted is responsible for all use of that account and is expected to take reasonable steps to ensure the security of the account."

Network Services ID (NSID)
The university provides members of the community with a Network Services ID (NSID) that is used as a username to access university computer and network services such as PAWS, email, computer labs and password-protected webpages. The services that you are eligible for depend on your affiliation and role at the university.

The university provides individuals with ***a single NSID account***, even when they have multiple affiliations (e.g. faculty, staff, student, alumni). Individuals might also be provided with functional/role-based accounts, depending on their role with the university.

Role-based or Departmental Accounts
Special purpose NSIDs may be created to address the needs for a particular role (e.g. President, Vice-President), function, organization, or IT system to access university computer and network services. These NSIDs may be shared by storing data in a central location that can be accessed by multiple individuals if necessary. They can provide joint access to voicemail and file storage and are an alternative to mailing lists. Role-based accounts can help with records management for senior leadership roles or roles that experience regular turnover. Records management responsibilities may be different for role-based or departmental accounts depending on their purpose.

Access and Privacy

The Access and Privacy Office advises on and coordinates freedom of information and protection of privacy matters. The Access and Privacy Officer, in consultation with the appropriate colleges, departments, and administrative units, the Head and others as required, is responsible for responding on behalf of the university to all requests for information. The Access and Privacy Officer will also provide advice to colleges, departments, and administrative units relating to freedom of information and protection of privacy issues, including how they pertain to IT communications services records.

- Access to IT communications services records can be requested under the Local Authority Freedom of Information and Protection of Privacy Act, or by court order.
- Access to IT communications services records may be required to recover evidence while investigating matters concerning appropriate use (e.g. harassment, fraud) and managing actual or potential criminal or civil litigation in which the university is or may become a party.
- Access to IT communications services records may also be required for urgent/time-sensitive business continuity reasons due to the absence of a faculty or staff member for reasons such as leaves, terminations, or attrition.

All information about an identifiable individual is personal information, and must be dealt with in accordance with the Act. This includes personal information contained within IT communications services records. Personal information does have degrees of sensitivity associated with it. Some personal information, such as phone

numbers, has lower sensitivity than other personal information, such as social insurance numbers, which have higher sensitivity.

The Access and Privacy Officer can provide assistance regarding IT communications services records and decisions regarding:

- Identifying who should have access to a user's account.
- How often the university reviews who has access.
- Identifying who can approve a request for access.
- Developing the process used to approve and provide access.
- Providing guidance on identifying who must be consulted before account access (i.e. content) is granted and determining the appropriate access to email inbox contents.
- Providing guidance on identifying who must be consulted before message forwarding and/or message auto-replies can be provided.

Canada's Anti-Spam Legislation (CASL)

Each college, department, and unit at the U of S is responsible for ensuring that its outgoing electronic messages (including email, text message, automated telephone message or social media message) comply with CASL. Compliance is overseen by University Communications. It is important to have a proper records management or customer relationship management program in order to record consent; if challenged under CASL, the onus is on the university to establish proof of consent.

Appendix A – Approvals for Unsolicited Communications to Large Groups

Electronic mailing lists hosted on university systems are subject to the IT Communications Services Policy.

The university uses many email lists that are automatically created and maintained based on individuals' affiliation or role with the University of Saskatchewan. These lists comprise specific identifiable groups, such as all faculty and staff, all students, all faculty, department or division staff or class lists of students. Individuals may not request exemption from these lists and for that reason all e-mail sent to these types of lists will be considered unsolicited, in that the recipient(s) has not requested the communication.

The appropriate Data Trustee or their designate must be consulted on decisions regarding unsolicited communication to large segments of the university community (e.g. all students, all faculty and staff, all employees, all alumni).

Approvals for Unsolicited E-Mail Communications (Examples)

The following levels are established for the creation and use of involuntary e-mail lists. These are very broad categories and are intended as a guideline in making decisions regarding appropriate units and Data Trustees for approving unsolicited e-mail.

Audience Type	Approval	Usage Examples
All U of S faculty, staff, students, researchers	Vice-President, University Relations	University-wide, general announcements
	Crisis Management Team	Emergency announcements
	Data Trustee for the service impacted	Service outages
Students	Vice-Provost, Teaching, Learning and Student Experience	Information specific to students.
Alumni	Vice-President, University Relations	Notification of events. Notification of programs and services for alumni.
Faculty and staff	Associate Vice-President, People and Resources	Information specific to faculty and staff or retired faculty and staff.
All students of a college	The Dean of the college	Notification of events, programs, or services for students in the college.
All students of a class	The instructor of the class	Class notes. Notifications of class events.
Employees of a college or department	The Dean or Department Head	Notifications of special events.

Operationally, approval within a business unit may be delegated.