PRIVACY POLICY

SaskPower
Powering our future®

Division	Corporate & Regulatory Affairs
Policy Title	Corporate Privacy Policy
Issue Date	03/22/2022
Revision Frequency	5 years

POLICY STATEMENT

Purpose:

SaskPower is committed to protecting personal information in its possession or control in accordance with *The Freedom of Information and Protection of Privacy Act*. Personal health information in SaskPower's custody or control shall be protected in accordance with *The Health Information Protection Act*.

This policy establishes appropriate controls for the collection, use and disclosure of personal information and personal health information required to carry out SaskPower business.

Principles:

Personal information as used in this Policy is defined in section 24 of *The Freedom of Information and Protection of Privacy Act* (Saskatchewan) (the "Act").

Personal health information is defined in section 2(m) of *The Health Information Protection Act*.

There are specific items excepted from the definition of personal information and reference should always be made to the Act. If Personnel are uncertain what is or is not personal information, contact SaskPower's Law/RIM Department.

SaskPower's Privacy Policy is based on compliance with these Acts.

If there is any inconsistency between the Acts and this Policy, the Acts shall supersede this policy.

APPLICABILITY

Applies to:	The Board of Directors of SaskPower, SaskPower officers, employees, and contractors, as well as directors, officers and employees of SaskPower subsidiaries (collectively "Personnel").

REQUIREMENTS

Responsibilities:

Personnel shall handle personal information in compliance with *The Freedom of Information and Protection of Privacy Act* and other legislative authorities.

Personnel shall handle personal health information in compliance with *The Health Information Protection Act* and other legislative authorities. Personal health information shall be treated in a manner similar to personal information as set out in this policy. Where requirements under *The Health Information Protection Act* vary from the requirements in this policy, *The Health Information Protection Act* shall prevail.

Personnel are responsible for safeguarding the privacy, confidentiality and security of information in the workplace and when working remotely. Personal information shall only be shared on a strict need to know basis.

Personnel shall proactively incorporate privacy protection into all corporate initiatives. All modifications to existing business systems and processes and all new business process initiatives must have a Privacy Impact Assessment performed. All initiatives must have this step undertaken as part of the initial planning for the initiative.

- The Privacy Impact Assessment shall be in a form approved by the Chief Privacy Officer.
- If the Privacy Impact Assessment identifies area(s) of non-compliance with the principles contained in this policy which cannot be remedied, then the Divisional Compliance Officers shall consider the risks involved and make a recommendation to the Chief Privacy Officer whether the project will be allowed to proceed.
- Non-compliance will require approval from the Chief Privacy Officer and an approved work plan to attain compliance within such period of time as specified by the Chief

Privacy Officer. At the expiry of the time allotted for achieving compliance, another Privacy Impact Assessment shall be performed. If a passing grade is not attained, the Chief Privacy Officer may specify a further period of time for compliance to be achieved or sign off on the initiative as is.

Personnel who collect, access, use, process, store, modify, share, disclose and/or destroy personal information must comply with the following:

- **Consent:** The knowledge and consent of the individual are required for the collection, use or disclosure of personal information except where inappropriate or permitted by law. Informed consent must be obtained directly from the individual to whom the information relates or by legislative authority.
- **Collect only what is needed:** Personnel must only collect personal information for an identified business purpose that is necessary to the proper functioning of its business.
- **Use of personal information:** Personal information must only be used or disclosed for the purposes for which it was collected, for a use that is consistent with that purpose, with the consent of the individual or when collection, use or disclosure is authorized by legislation.
- **Disclosure:** Personal information shall not be used or disclosed by SaskPower for purposes other than those for which it was collected, except with the consent of the individual or as required by law.
- **Retention and disposal:** Personal information must be retained only as long as necessary for the fulfillment of its stated collection purpose or as specified by law. When the retention requirements have been met, appropriate steps must be taken to safely and securely dispose of the records.
- **Removal of personal information:** In general, personal information must not be removed from SaskPower's business premises. Permission to take such information off site may be granted by an out of scope supervisor, provided that the involved worker has successfully completed the mandatory Privacy Awareness Training Course offered by SaskPower. A signed confidentiality agreement may also be required.
- **Confidentiality:** Personnel must keep personal information confidential.
    - Display screens for all computer equipment used to process personal information must be positioned such that they cannot be readily viewed through a window, by persons walking past or by persons waiting in reception areas.
    - Whenever a person not authorized to view information enters the immediate area, precautions to conceal personal information must promptly be taken.

- Whenever personal information is contained on laptops, the devices must have an encryption scheme in place as approved by the Chief Privacy Officer and/or Enterprise Security.

- **Personal information privacy awareness training:** As part of the ongoing Privacy Management Process, all Personnel for whom training is deemed necessary will be required to successfully complete a training course on privacy on SaskPower's time and at SaskPower's expense.
  - Completion of the training shall be mandatory and there shall be no exceptions. Records will be kept respecting completion of this course.
  - All new hires shall successfully complete this course within 90 days of their hire or sooner if they handle personal information in the course of their employment.
  - Course materials shall be approved by the Chief Privacy Officer.
- **Personal information security awareness:** All new hires shall be required as a condition of their employment to complete security training regarding their obligations with respect to personal information. The training shall be in a form approved by the Chief Privacy Officer.
- **Security:** SaskPower will ensure that appropriate safeguards are in place to protect personal information. These safeguards are intended to address such concerns as appropriate access to information, breach prevention, recovery, information integrity and other potential security issues. Safeguards include technical, procedural and organizational measures. Personnel shall assign appropriate sensitivity levels to all personal information in accordance with the Data Classification Standard.
- **Privacy breach of personal information:** A privacy breach occurs when there is unauthorized access to, collection, use, disclosure or disposal of personal information either internally or externally, in contravention of the Act. In the event of any loss, suspected security breach or theft of personal information, Personnel must advise the Chief Privacy Officer who will evaluate the incident and refer the matter to Internal Audit where appropriate.
- **Information Management Service Provider:** Before disclosing personal information to an Information Management Service Provider, SaskPower is required to enter into a written agreement that contains wording appropriate to the security of the information.

Individual's rights

An individual, whether a customer or employee, has the following rights:

- **Openness:** SaskPower shall make specific information about its policies and practices relating to the management of personal information readily available to individuals.
- **Individual's access to their personal information:** Upon request to SaskPower, an individual shall be informed of the existence, use and disclosure of his or her personal information and shall be given access to that information. An individual shall have the right to challenge SaskPower as to the accuracy and completeness of the information and to have it amended as appropriate.
- **Accuracy:** Personal information shall be accurate and kept as up to date as necessary for the purposes for which SaskPower has collected it.
- **Correction:** An individual has the right to request correction of personal information. If correction is requested, but not made, the individual has the right to have a notation made and to be advised as to the reason a request was disregarded.
- **Challenging compliance:** An individual shall be able to challenge compliance with any of these requirements. Challenges shall be forwarded to the Chief Privacy Officer.

Employees have limited privacy when they are using SaskPower assets or representing SaskPower. Random surveillance is not allowed. Any investigation will only be allowed when there is cause to believe that resources are being misused or unethical conduct has occurred and the Executive has authorized the investigation in accordance with the Code of Conduct.

Employee information will be shared on a strict need to know basis and in accordance with the Acts.

Conditions:

SaskPower considers all personal information pertaining to its employees, superannuates, customers, contractors, subsidiaries and business activities to be private and confidential. The highest standards of confidentiality and privacy management shall be implemented and maintained.

Employees are required to use SaskPower assets in accordance with the Enterprise Security Information Technology Acceptable Use Policy. Cyber Operational Technology Assets are to be used exclusively for its designated purpose and personal use is prohibited.

Governance:

SaskPower's Chief Privacy Officer is responsible for:

- recommending protection of personal information in accordance with legislative requirements, and

- receiving, reviewing and/or investigating all privacy complaints or breaches in relation to the application of this policy.

Records and Information Management is responsible for:

- Corporate Information Governance and Records Management
- assisting the Chief Privacy Officer in carrying out assigned duties
- providing guidance with respect to this policy
- ensuring this policy is maintained
- leading the privacy impact assessment process on initiatives where personal information is collected, used or disclosed.

Personnel are responsible for compliance with this policy and related procedures and guidelines.

RESOURCES

Related Policies:

Enterprise Security Policy
Code of Conduct Policy
Records and Information Management Policy

Ownership & Inquiries

Position Owner	Director
Business Department	Corporate and Regulatory Affairs
Contact Person	Chief Privacy Officer
Approved by	Board of Directors
Date	6/24/2004
Contact Information	306-566-5820

Document History

Revised by	Revision Purpose	Date
RIM	Update to 2004 Policy	3/22/2022