User Acceptable Use Policy

Ministry of SaskBuilds and Procurement
Information Technology Division
Cyber Security and Risk Management Branch

Last revised: February 2024
Last reviewed: February 2024
Next review: January 2025

User Acceptable Use Policy

Ministry of SaskBuilds and Procurement
Information Technology Division, Cyber Security and Risk Management Branch

Contents

This document is intended for the Saskatchewan Ministry of SaskBuilds and Procurement, Information Technology Division, and partner organizations. It may contain legally privileged and/or confidential information and must not be disseminated, distributed, or copied

User Acceptable Use Policy

Ministry of SaskBuilds and Procurement
Information Technology Division, Cyber Security and Risk Management Branch

Purpose

The Government of Saskatchewan requires that GoS Assets be used in a responsible way and in compliance with all legislation and other government policies and contracts. This policy does not attempt to anticipate every situation that may arise and does not relieve anyone accessing assets of their obligation to use common sense and good judgment.

Scope

This Asset Management Policy applies to all business processes and data, information systems, components, personnel, and physical areas of the Government of Saskatchewan. Person(s) this policy applies to include but are not limited to:

- All employees, whether employed on a full-time or part-time basis by the Government of Saskatchewan
- Contractors and Service Providers that access and manage Government of Saskatchewan assets.

Governing Laws, Regulations, and Standards

Resource	Description
Privacy Act	*P-21.pdf (justice.gc.ca) Government of Canada Privacy Act*
PIPEDA	*P-8.6.pdf (justice.gc.ca)Government of Canada PIPEDA Act*
Freedom of Information and Protection of Privacy Act	Saskatchewan's provincial public sector privacy law
Local Authority Freedom of Information and Protection of Privacy Act	*Saskatchewan's municipal public sector privacy law*
Health Information Protection Act	*Saskatchewan's privacy law relating to health records*
ISO/IEC 27001:2013	8.1.3, 8.1.4
ISO/IEC 27002:2022	5.10, 5.11
NIST (National Institute of Standards and Technology) SP 800-53 v4	MP-2~7, PE-16,18,20, PL-4, SC-8, SC-28

Policy Statements

A. Acceptable Use of Assets

All assets, as defined in this document, are property of The Government of Saskatchewan and use must be in accordance with policies, standards, and guidelines. While the Government of Saskatchewan does not prohibit limited incidental use of information technology for personal reasons, users should recognize that the primary intention of providing access to information assets is to support the core work of the Government.

1. The Government of Saskatchewan allows limited incidental use of the GoS assets for personal reasons (personal correspondences, online banking, etc.), but personal use must not be abused. Personal use is acceptable if it is limited to the following considerations:

   It does not have a negative impact on overall employee productivity.

   It does not cause additional expense to the government.

   It does not compromise the government nor its assets.

   It does not disrupt the network performance.

   It does not contradict any other Government of Saskatchewan policies.
2. The GoS assets may not be used for illegal or unlawful purposes.
3. Users must only use devices, applications, or services that are authorized and approved by Information Technology Division.
4. Assets, such as laptops and mobile devices, are intended to be used only by the people to whom they have been issued. The person to whom the device was issued is ultimately responsible for any actions performed with the device.
5. Users will always protect all GoS assets, keeping them physically and logically secured and under the control of the user.

B. Electronic Communication and Internet Use

The use of The Government of Saskatchewan's communication and internet systems and services (including email, instant messaging, voicemail, forums, social media, and more) is provided to perform regular job duties. The use is a privilege, not a right, and therefore must be used with respect, common sense, and in accordance with the following requirements:

1. The email systems and other messaging services used by the Government of Saskatchewan are owned by the government and are therefore considered property of the Government of Saskatchewan.
2. Electronic communication and internet must not be used for illegal or unlawful purposes.
3. The Government of Saskatchewan's communication platforms and internet are not to be used for purposes that could be reasonably expected to strain storage or bandwidth (e.g. emailing large attachments instead of pointing to a location on a shared drive or SharePoint site).
4. Users are prohibited from using accounts that do not belong to them and are prohibited from using platforms to impersonate others.
5. Users are not to give the impression that they are representing or providing opinions on behalf of The Government of Saskatchewan unless otherwise authorized.

6. Users shall not open message attachments or click on hyperlinks sent from unknown or unsigned sources through any platform (email, instant message, social media, etc.). Attachments/links are the primary source of malware and other information security threats and should be treated with utmost caution.
7. The Government of Saskatchewan prohibits use of email or other messaging platforms for mass unsolicited mailings and chain letters.
8. Any allegations of misuse should be promptly reported to Service Desk. If you receive an offensive or suspicious email, report it to the Service Desk. Do not forward, delete, or reply to the message unless advised to do so by the Service Desk.
9. Email users are responsible for mailbox management, including organization and cleaning. If a user subscribes to a mailing list, he or she must be aware of how to unsubscribe from the list and is responsible for doing so if their current email address changes.
10. Archival and backup copies of email messages may exist despite end-user deletion, in compliance with the Records Retention Policy of the Ministry of SaskBuilds and Procurement.
11. Email access will be terminated when the employee or third party terminates their association with The Government of Saskatchewan, unless other arrangements are made.
12. Users shall not send sensitive information, electronic or physical, that is not appropriately protected. Appropriate protection is any available and reasonable administrative, technical, and physical safeguards**.**
13. Users are not permitted to automatically forward emails received by their Government account to an external email address or other messaging system unless authorized to do so.
14. Email users are expected to remember that email sent from the government email accounts reflect on the government and to comply with normal standards of professional and personal courtesy and conduct.
15. The Government of Saskatchewan may monitor any/all internet activity originating from government-owned equipment or accounts or taking place over government networks. If the Government of Saskatchewan discovers activities that do not comply with applicable law or GoS policy, records retrieved may be used to document the wrongful content.
16. Users are permitted to remotely access the government network while offsite. Users must use the approved VPN or other remote access service(s). Users will be required to authenticate using multifactor authentication (MFA). Only authorized users are permitted to access the network through VPN.

C. Mobile Device Use

The Government of Saskatchewan’s employees are permitted to use their own personal devices to access its information assets The use of personal and Government of Saskatchewan owned mobile devices must be in accordance with the following requirements:

1. It is the responsibility of any employee of the Government of Saskatchewan who uses a mobile device to access government resources to ensure that all security protocols normally used in the management of data on conventional storage infrastructure are also applied here. Access to govt networks is a privilege and not a right and it can be revoked for breach of policy or in the case of inappropriate use.
2. IT reserves the right to refuse, by physical and non-physical means, the ability to connect mobile devices to government and government-connected infrastructure. IT will engage in such action if such equipment is being used in a way that puts the organization’s systems, data, users, and clients at risk.

3. All mobile devices used for access to government assets must be protected by a strong access control (e.g., alphanumeric password or biometric authentication). Employees shall never disclose their passwords to anyone, even to family members.
4. All users of mobile devices must employ reasonable physical security measures. End users are expected to secure all such devices whether they are in use and/or being carried.
5. All mobile devices used for access to government assets must have installed up to date GoS-approved anti-malware and threat defense software.
6. All users with mobile devices used for access to government assets are prohibited from removing GoS approved anti-malware and threat defense software from the mobile device.
7. Sensitive data must not be stored on mobile devices
8. In the event of a lost or stolen mobile device that has access to Government assets, it is incumbent on the user to report the incident to Service Desk immediately.
9. All personal mobile devices attempting to connect to the government network through the internet will be assessed for appropriate, secure configurations using technology centrally managed by The Government of Saskatchewan's IT Department. Devices that do not meet assessment requirements, are not in compliance with IT's security policies, or represent any threat to the government network or data will not be allowed to connect.

D. Use of Removable Media

Removable media, as defined in this document, may be used with the following requirements:

1. Information should only be stored on removable media when required in the performance of the user's role (e.g., USB shared between two employees during a conference). Upon completion of the tasks for which the removable media was needed, all data shall be deleted.
2. Removable media should meet requirements for encryption as set by Cyber Security and Risk Management Branch.
3. The use of removable media to introduce malware or other unauthorized software into The Government of Saskatchewan's environment is strictly prohibited.
4. Mobile devices (e.g., smartphones, tablets) are not permitted to be used as removable media to transfer or store any business or customer data.
5. Any unknown removable media that is found unattended must be reported to the Service Desk and NOT inserted into any Government issued device.
6. End users are encouraged to take reasonable measures to secure removable media (e.g. storing it in a secure/locked location when not in use; not sharing with unauthorized users).
7. Use of removable media is not allowed on external or non-government-issued systems.
8. All removable media must be turned in to the Service Desk for proper disposal when no longer required for business use in accordance with the *Disposal of Electronic Storage Devices Policy*.

E. Artificial Intelligence (AI)

Utilization of AI features and applications must follow standard processes for approvals and onboarding.

1. Utilization of AI must be approved in advance. This means following our standard process for onboarding a new piece of software. Please contact ITD ServiceDesk for assistance with this process. The pre-onboarding review will include an evaluation of the AI security features, terms of service, privacy policy, reputation of the AI developer and any third-party services used by the AI.
2. As with all software, every AI must have a designated owner or responsible party within GOS who is ultimately accountable for its performance and compliance with GOS policies.

F. Clean Desk and Printing

A clean desk is important to ensure that all sensitive information is protected. This will reduce the risk of security and privacy breaches in the workplace and is part of standard basic privacy controls.

3. Employees are required to ensure that all sensitive information in hardcopy or electronic form is secure in their work area at the end of the day and when they expect to be gone for an extended period (e.g. Computer workstations must be screen locked when workspace is unoccupied).
4. Any sensitive information must be removed from view and locked in a drawer when the desk is unoccupied and at the end of the workday.
5. Passwords are not to be written down anywhere under any circumstances.
6. File cabinets containing sensitive information must be kept closed and locked when not in use or when not attended.
7. Keys/badges used for access to sensitive information must not be left unattended.
8. Printouts containing sensitive information should be immediately removed from the printer.
9. Any sensitive information that is no longer needed should be disposed of in accordance with the respective institution's/ministry's records management policy.
10. Whiteboards containing sensitive information should be erased.

G. Password Standards

Access to The Government of Saskatchewan systems and devices is controlled through individual accounts and passwords. The following requirements are in place to protect passwords and access to assets:

1. Users may not share account or password information with another person. Accounts are to be used only by the assigned user of the account and only for authorized purposes. Attempting to obtain another user's account password is strictly prohibited.
2. A user must contact the Service Desk to obtain a password reset if they have reason to believe any unauthorized person has learned their password. Users must take all necessary precautions to prevent unauthorized access to The Government of Saskatchewan's services and data.
3. Users must not use government passwords for other services. If other services are compromised, it could leave government accounts compromised as well.
4. Password complexity will be enforced by IT through system-enforced policies to ensure strong passwords and proper password hygiene.

H. Incident Response and Reporting

The Government of Saskatchewan has an incident response program for efficient remediation of information security incidents. Employees are expected to comply with the following requirements to ensure effective and efficient incident remediation:

1. Users must report any suspected security incident to the IT Service Desk including, but not limited to, lost/stolen assets, suspected malware infection, compromised credentials, and any other possible compromises of Government assets.
2. Users must cooperate with incident response processes such as forfeiting their equipment to Service Desk for investigation if it is potentially compromised.

I. Unacceptable Uses

IT will manage security policies, network, application, and data access centrally using whatever technology solutions are deemed suitable. Any attempt to contravene or bypass security will be deemed an intrusion attempt and will be subject to disciplinary action.

Supporting Internal Resources

Resource	Description
Internal Security Governance Policy	All Government of Saskatchewan Security Policies align to this Governance Policy
Information Protection Security Controls (IPSC) for Classified Data	This document defines the required access controls required to provide the proper security based on Classified Data for Government of Saskatchewan
Disposal of Electronic Storage Devices	This document defines the requirements around electronic storage devices.

Non-Compliance

In cases where it is determined that a breach or violation of Government of Saskatchewan Information Security policies has occurred, the respective Ministry under the direction of the Chief Information Officer and Information Security Branch, will initiate corrective measures including restricting access to services or initiating disciplinary action up to and including dismissal, in accordance with PS 803 Corrective Discipline policy, or in the case of contractors, vendors, or agents, the termination of a contract or agreement with the contractor, vendor, or agent

Exceptions

In certain circumstances, exceptions to this policy may be allowed based a review and acceptance of risk by the Security Governance Committee. Exceptions to this policy must be formally documented and approved by the Chief Information Security Officer, under the guidance of the Cyber Security and Risk Management Branch. Policy exceptions will be reviewed periodically for appropriateness.

Definitions

- **Assets:** Property of the government of Saskatchewan that includes Government of Saskatchewan information/data, computers, software, communication tools (email, instant messaging), access to internal networks (intranet), access to external networks (internet), as well as telephone systems, voice mail, printers, fax machines, photocopiers, multi-function devices, etc.
- **Removable media:** Any type of storage device that can be removed from a computer while the system is operational. Examples include USB flash/thumb drives, memory cards, CDs/DVDs, external hard drives, or mobile devices used for storage purposes such as MP3 players or smartphones. While there are business purposes for these devices, they are also known to be common sources of malware infections and susceptible to loss or theft, leading to breaches of sensitive information.

Revision History

Version ID	Date of Change	Author	Rationale
1.0	January 10, 2023	Kelsey Sproat	Feedback from Privacy and Legal (SBP/IJS) and Security Officers (all Ministries) incorporated.
1.1	May 10, 2023	Kelsey Sproat	Feedback from PSC incorporated. Agreed to publish this version while ownership of and collaborative finalization work continues.
1.2	January 18, 2024	Kelsey Sproat	Ownership of Acceptable Use Policy rests with ITD, Cyber Security and Risk Management Branch. Added section on Artificial Intelligence (AI). Updated link to Disposal of Electronic Storage Devices Policy.
1.3	February 6, 2024	CSRM	Transfer to new template.