User Acceptable Use Policy

Last revised: April 2021
Last reviewed: April 2021
Next review: April 2022

Ministry of SaskBuilds and Procurement
Information Technology Division, Information Security Branch

Purpose

The Government of Saskatchewan provides many business tools to its employees and contractors to enhance their productivity and jobs. These tools include computers, software, communication tools (email, chat), access to internal networks (intranet), access to external networks (internet), as well as telephone systems, voice mail, fax, photocopiers, multi-function devices, etc. The Government of Saskatchewan requires that these work tools be used in a responsible way, ethically, and in compliance with all legislation and other Government policies and contracts. Noncompliance could have a severe, negative impact on the company, its employees, and its clients. This policy does not attempt to anticipate every situation that may arise and does not relieve anyone accessing the system of their obligation to use common sense and good judgment.

Individuals at The Government of Saskatchewan are encouraged to use the corporate systems and resources to further the business goals and objectives of the organization. The types of activities that are encouraged include:

- Communicating with fellow employees, Government business partners, and Government clients within the context of an individual's assigned responsibilities.
- Acquiring or sharing information necessary or related to the performance of an individual's assigned responsibilities.
- Participating in educational or professional development activities.

Scope

This policy is applicable to all employees of The Government of Saskatchewan, including full-time, part-time, and temporary employees; contractors; students; and interns. The requirements defined in this policy are applicable to all data, systems, and services owned and/or managed by The Government of Saskatchewan.

Definitions

- **Shadow IT:** The acquisition and use of information technology systems and/or services within the organization that have not been approved by the IT Department. Oftentimes, the IT Department is not even aware of these solutions being implemented.
- **Malware:** A program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system, or of otherwise annoying or disrupting the victim.
- **Social engineering:** The "con game"; the art of manipulating end users into providing confidential or personal information. One example is "phishing," where hackers pretend to be trusted organizations such as banks, company suppliers, IT staff, or mobile carriers to get your personal information such as credit card details or confidential corporate information.
- **Removable media:** Any type of storage device that can be removed from a computer while the system is running. 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.
- **Service Desk:** The Government of Saskatchewan's internal service desk support team, which can be reached through email at itoservicedesk@gov.sk.ca or by phone at 306-787-5000 or by logging a request on Service Now.

Policy

A. Acceptable Use of Assets

Assets include, but are not limited to, physical equipment, such as desktop computers, servers, printers, laptops, telephones, mobile devices, and removable media (such as USB flash drives), as well as systems and services, such as the organizational network, internet, voicemail, and more. Organizational data is also considered to be an asset. All devices and systems are property of The Government of Saskatchewan and all use must be in accordance with policies, standards, and guidelines.

1. The Government of Saskatchewan allows limited use of the network, systems, and devices 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:
   a) It does not have a negative impact on overall employee productivity.
   b) It does not cause additional expense to the company.
   c) It does not compromise the company is any way.
   d) It does not disrupt the network performance in any way.
   e) It does not contradict any other Government of Saskatchewan policies in any way.
2. The Government of Saskatchewan assets and systems may not be used for illegal or unlawful purposes, including copyright infringement, obscenity, personal gain, libel, slander, fraud, defamation, plagiarism, intimidation, forgery, impersonation, illegal gambling, soliciting for pyramid schemes, and computer tampering (e.g. spreading computer viruses).
3. Users should not access and/or purchase technology, devices, applications, or services that are not formally authorized and approved by IT. (This circumvention of the IT Department is known as Shadow IT.)
4. IT assets, such as laptops and mobile devices, are intended to be used only by the people to whom they have been issued. If another employee or non-employee (e.g. family member) is using the device, the use should be monitored to ensure that no sensitive data is accessed by the unauthorized party. The person to whom the device was issued is ultimately responsible for any actions performed with the device.
5. Users will always protect all corporate-managed IT assets, keeping them physically and logically secured and under the control of the user, including but not limited to:
   a) Locking down laptops with a locking cable or storing them in a locked drawer or cabinet when leaving them in the office.
   b) Ensuring the workstation is locked (screen/keyboard) whenever walking away from it.
6. Access to The Government of Saskatchewan's systems and devices is controlled through individual accounts and passwords, as outlined in the Password Standard section of this document and in the Access Control Policy.
7. All voicemail boxes will be protected with a PIN (personal identification number).. Easy-to-guess or previously used PINs will be blocked by the system. PINs must not be shared with others.
8. Removable media, such as USB flash drives, CDs, etc., may be used with the following requirements:
   a) 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).
   b) Removable media should meet requirements for encryption as set by Information Security Branch.
   c) The use of removable media to introduce malware or other unauthorized software into The Government of Saskatchewan's environment is strictly prohibited.

d) Mobile devices (e.g., smartphones, tablets) are not permitted to be used as removable media to transfer or store any business or customer data.

e) Any unknown removable media that is found unattended must be reported to the Service Desk and NOT inserted into any Government issued device.

f) 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).

g) Use of removable media is not allowed on external or non-company-issued systems.

h) Upon completion of the assigned duties, all data shall be deleted, in accordance with NIST SP 800-88 Rev. 1, from the removable media.

i) All removable media must be turned in to the Service Desk for proper disposal (in accordance with NIST SP 800-88 Rev. 1) when no longer required for business use.

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 company and are therefore its property. This gives The Government of Saskatchewan the right to monitor all email traffic passing through its email system. This monitoring may include, but is not limited to, inadvertent reading by IT staff during the normal course of managing the email system, review by the HR and legal team during the email discovery phase of litigation, and observation by management in cases of suspected abuse or employee inefficiency.

2. The Government of Saskatchewan often delivers official communications via email. As a result, employees of The Government of Saskatchewan with email accounts are expected to check their email in a consistent and timely manner so that they are aware of important company announcements and updates, as well as for fulfilling business and role-oriented tasks.

3. Electronic communication and internet must not be used for illegal or unlawful purposes, including, but not limited to, copyright infringement, obscenity, libel, slander, fraud, defamation, plagiarism, harassment (including offensive and/or insulting content), discrimination, intimidation, forgery, impersonation, illegal gambling, soliciting for illegal pyramid schemes, and computer tampering (e.g., spreading computer viruses).

4. 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). Individual use of resources will not interfere with others' use of The Government of Saskatchewan's email system and services.

5. Users are prohibited from using accounts that do not belong to them and are prohibited from using platforms to impersonate others.

    a) 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 social engineering and should be treated with utmost caution.

7. The Government of Saskatchewan prohibits use of email or other messaging platforms for mass unsolicited mailings, chain letters, and competitive commercial activity unless preapproved by The Government of Saskatchewan.

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 Government of Saskatchewan's Records Retention Policy.

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. The Government of Saskatchewan is under no obligation to store or forward the contents of an individual's email inbox/outbox after the term of their employment has ceased.

12. Users shall not send sensitive information that is not appropriately protected (encrypted). Appropriate means of protection include but are not limited to [OneDrive or encrypted attachments through email].)

    a) Users shall take extra precautions when transmitting company, client, and/or other regulated information via electronic communications. Sensitive material should be marked and encrypted appropriately. Keep in mind that all email messages sent outside of The Government of Saskatchewan become the property of the receiver.

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 by way of an approved Risk Management Decision Item (RMDI).

14. The Government of Saskatchewan assumes no liability for direct and/or indirect damages arising from the user's use of The Government of Saskatchewan's email system and services. Users are solely responsible for the content they disseminate. The Government of Saskatchewan is not responsible for any third-party claim, demand, or damage arising out of use The Government of Saskatchewan's email systems or services.

    a) However, email users are expected to remember that email sent from the company's email accounts reflects on the company. Please comply with normal standards of professional and personal courtesy and conduct.

15. The Government of Saskatchewan may monitor any/all internet activity originating from company-owned equipment or accounts or taking place over company networks. If the Government of Saskatchewan discovers activities that do not comply with applicable law or corporate/departmental policy, records retrieved may be used to document the wrongful content in accordance with due process.

16. Users are permitted to remotely access the corporate network while offsite. Users must use the approved VPN service(s). Users will be required to authenticate using multifactor authentication (MFA). Only authorized users are permitted to access the network through VPN.

17. The Government of Saskatchewan's social media accounts are permitted to be used for business purposes only. These purposes include building positive brand image, providing customer support, monitoring public opinion, professional networking, and more. The following requirements are imposed for appropriate use of social media:

    a) All new social media accounts must be approved by senior Executive council staff prior to launch All actions and communications through social media must adhere to Social Media Policy.

    b) All GoS social media accounts must be tied to a GoS email address. The use of personal social media accounts and user IDs for company use is prohibited.

    c) The use of Government of Saskatchewan social media user IDs for personal use is prohibited.

C. Data Security

Maintaining the confidentiality, integrity, and availability of organizational data is paramount to the security and success of the organization. The following requirements are defined to keep data secure and handled appropriately.

1. All organizational data is owned by The Government of Saskatchewan and, as such, all users are responsible for appropriately respecting and protecting all data assets.
2. Users must keep all data secure by taking sensible precautions and following requirements defined in this policy, Asset Management Policy, and the data-handling requirements defined in the Guide for Information Protection Classification. This standard outlines the requirements for creating, using, storing, transmitting, archiving, and destroying data.
3. Data must be classified based on sensitivity, as defined in the Asset Management Policy. Data must be classified as Class A, Class B, Class C, or Public. Data at each classification level must be safeguarded and handled appropriately in accordance with the Guide for Information Protection Classification.
4. Users may not view, copy, alter, or destroy data, software, documentation, or data communications belonging to The Government of Saskatchewan or another individual without authorized permission.
5. Users will only access data provided to them for duties in connection with their employment or engagement and in accordance with their terms and conditions of employment or equivalent. Access to some applications and information sources will be routinely recorded and/or monitored for this purpose.
6. Extraction, manipulation, and reporting of the Government of Saskatchewan data must be done for business purposes only.
    a) Personal use of organizational data, including derived data, in any format and at any location, is prohibited.
7. Users will follow all company-sanctioned data removal procedures to permanently erase data from devices once its use is no longer required, as defined in the Asset Management Procedure. Data must be retained for the length of time defined in the Data Retention Policy.

D. Mobile Device Use

The Government of Saskatchewan's employees are permitted to use their own personal devices to access the internet over the corporate guest wireless network and to send/receive email. The use of personal mobile devices is a privilege, not a right, and therefore must be used with respect, common sense, and 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 corporate resources to ensure that all security protocols normally used in the management of data on conventional storage infrastructure are also applied here. It is imperative that any mobile device that is used to conduct Government business be used appropriately, responsibly, and ethically. Failure to do so will result in immediate suspension of that user's account.
2. IT reserves the right to refuse, by physical and non-physical means, the ability to connect mobile devices to corporate and corporate-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 company systems and/or data (such as email) must be protected by a strong access control (e.g. alphanumeric password or biometric authentication). Employees are encouraged to never disclose their passwords to anyone, even to family members, if business work is conducted from the mobile device.
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 company systems and/or data (such as email) must have installed up to date GoS-approved anti-malware and threat defense software.
6. All users with mobile devices used for access to company systems and/or data are prohibited from removing GoS approved anti-malware and threat defense software from the mobile device.
7. Sensitive data (e.g. client data) and passwords must not be stored on mobile devices.
8. In the event of a lost or stolen mobile device that has access to Government resources (e.g. email, OneDrive, Authenticator), it is incumbent on the user to report the incident to Service Desk immediately.
9. All personal mobile devices attempting to connect to the corporate 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 are not approved by IT, are not in compliance with IT's security policies, or represent any threat to the corporate network or data will not be allowed to connect.

E. Clean Desk and Printing

A clean desk policy is an important tool to ensure that all sensitive materials, such as information about an employee, a customer, or intellectual property, are removed from an end-user workspace and locked away when the items are not in use or an employee leaves his/her workstation. This will reduce the risk of security breaches in the workplace and is part of standard basic privacy controls.

1. 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.
   a) Computer workstations must be locked (screen/keyboard) when workspace is unoccupied.
   b) Laptops must be either locked with a locking cable or locked away in a drawer if not taken home at the end of the workday.
2. Any sensitive information (e.g., client data) must be removed from the desk and locked in a drawer when the desk is unoccupied and at the end of the workday.
3. Passwords are not to be written down anywhere or under any circumstances.
4. File cabinets containing sensitive information must be kept closed and locked when not in use or when not attended.
5. Keys/badges used for access to sensitive information must not be left at an unattended desk.
6. Printouts containing sensitive information should be immediately removed from the printer.
7. Upon disposal, sensitive documents should be shredded.
8. Whiteboards containing sensitive information should be erased.

F. 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 those passwords and access to sensitive data and systems:

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 corporate passwords for other services. If other services are compromised, it could leave corporate accounts compromised as well.

4. Password complexity will be enforced by IT through system-enforced policies to ensure strong passwords and proper password hygiene:

    a) Passwords will expire every [90 days] and users will be forced to change them. Users are encouraged to reset their passwords prior to the expiry date to minimize any interruption to network access.

    b) A minimum lifespan of [1 day] is enforced to prevent too frequent password changes.

    c) The previous [7] passwords cannot be reused.

    d) Password complexity requirements enforce the use of a minimum of [3] categories (Uppercase, lowercase, numbers, non-alphanumeric symbols, and Unicode characters.)

    e) Upon [5] failed login attempts, accounts will be locked]. Accounts can be unlocked by contacting Service Desk.

G. 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 equipment, suspected malware infection, compromised credentials, and any other possible compromises of Government systems and/or data.

2. Users must cooperate with incident response processes such as forfeiting their equipment to Service Desk for investigation if it is potentially compromised.

H. Security Awareness and Training

Human error and negligence are common sources of security issues. The Government of Saskatchewan takes a proactive approach by requiring security awareness and training:

1. During onboarding, all users will be required to undergo information security awareness and training. Upon completion, users will be required to sign a declaration that they have completed training, understand the requirements and specific procedures taught, and intend to abide by the policies and procedures provided.

2. Users must complete ongoing security awareness and training as scheduled by the IT Department. Employees will be kept up to date on new improvements and emerging threats.

I. Security 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. The following restrictions and requirements are enforced at The Government of Saskatchewan to establish and maintain the confidentiality, integrity, and availability of systems and data:

1. Users must not introduce malicious programs into the network or a system (e.g. viruses, worms, Trojan horses, email bombs, etc.).

2. Users must not introduce or contribute to security breaches or disruptions of network communication.

    a) Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a system or account that the employee is not expressly authorized to access, unless these actions are within the scope of regular duties. For the purposes of this section, “disruption” includes, but is not limited to, network sniffing, ping floods, packet spoofing, denial of service, and forged routing information for malicious purposes.

3. Port scanning or security scanning is expressly prohibited unless prior authorization is granted in writing by the Chief Information Security Officer.

4. Users must not execute any form of network monitoring that will intercept data not intended for the employee's host unless this activity is a part of the employee's normal job/duty.
5. Users must not circumvent user authentication or security of any host, network, or account.
6. Users must not introduce honeypots, honeynets, or similar technology on the corporate network.
7. No servers (i.e., running web or FTP services from user workstations) or devices that actively listen for network traffic can be put on the corporate network without prior written authorization by the Chief Information Officer.
8. Users must not interfere with or deny service to any user (for example, denial of service attack).

J. Ownership and Privacy Issues

The systems are the Corporation's property as well as, for access and security purposes, the information they contain. We respect our employees' right to privacy; however, we grant access to our systems for business use. Employees must not expect that information contained in these systems is private. The Company reserves the right, from time to time, for commercial, legal, or otherwise valid reasons, to read, monitor, control, and access user files and messages created, saved, transmitted, or received. In the event of intercepted illegal activity, we will bring them to the attention of the appropriate authority without prior notification to the sender or receiver.

Non-Compliance

In cases where it is determined that a breach or violation of Government of Saskatchewan policies has occurred, the Information Security Branch, under the direction of the Chief Information Officer and the respective Ministry, will initiate corrective measures including restricting access to services or initiating disciplinary action up to and including dismissal, 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 Officer, under the guidance of the Information Security Branch. Policy exceptions will be reviewed periodically for appropriateness.

Agreement

I have read and understand the Human Resources Security Policy. I understand that if I violate the rules explained herein, I may face legal or disciplinary action according to applicable laws or company policy.

____
Employee Name

____ ______________________________________
Employee Signature Date

Revision History

Version ID	Date of Change	Author	Rationale