



# User Handbook on IT Security



Government  
of  
Saskatchewan  
Ministry of Central Services

# Cyber Criminal Moves



## Consider IT Security

As Government of Saskatchewan employees, we are often entrusted with sensitive data in a variety of capacities.

It is our responsibility to handle this sensitive information with the greatest possible care and to help prevent an IT security incident from taking place.

An IT security incident can affect anywhere from one computer to an entire network, and impact our ability to deliver services to citizens. In some cases it could even cause unauthorized disclosure of citizen and resident information.

Part of our responsibility is to educate ourselves on approved government IT security practices and the policies that exist.

It also involves always being aware of potential threats in our day-to-day work, and taking the right measures to safeguard sensitive information against those threats.

This guide will walk you through a number of common IT security threats, and explain what you can do as a Government of Saskatchewan employee to protect the sensitive data in our trust.

If you need assistance with matters of information security that are not addressed in this guide, Ministry Security Officers exist across government. They have a responsibility to promote security awareness and compliance with information security policies within their ministry. A list of Ministry Security Officers is available at [www.employeeservices.gov.sk.ca/ITSecurity](http://www.employeeservices.gov.sk.ca/ITSecurity).



# Social Engineering

## How to save face in the company of a social engineer

Social engineers are hackers who trick their victims into breaking normal security procedures by impersonating someone in a position of authority. For example, a social engineer may pose as tech support or a researcher.


Regardless of the scenario they invent, they will ultimately request the same thing of their victims — their sensitive information. Once they have the information they need, there's no saying how much damage they can do.

They sometimes piece together bits of information, like that left online through social media, to eventually collect a large amount of information that can be used against their victims.

### To protect your information against social engineers:

- If someone calls claiming to be a Government of Saskatchewan employee or other authority figure and asks you for government information, verify their identity first. One way you can do this is by telling them you'll call them back. Look them up in the Government Directory or other trusted source, and initiate a new call at their phone number.

### To avoid leaving an information trail:

- Lock your computer each time you step away by holding the  and L keys.
- Clean up your work area of any government information.
- Always shred sensitive information.
- Use separate passwords for everything, and keep them to yourself.
- Keep sensitive government information off social media.
- Use caution when accessing email in a public place — someone could be reading over your shoulder.



# Phishing

## Don't take the bait!

Anyone can be a target of a phishing attack.

Phishing is a scam where a criminal sends an email to a victim, masquerading as a trusted organization like a bank, credit card company or e-commerce site.

This email is often meant to scare or excite the recipient into clicking a link to a cloned website that looks just like the real thing, and even has a very similar web address.

The web page may have a fake login box, meant to trick the victim into entering their information.

This is one way cyber criminals can carry out identity theft.

### Here are some tips you can use to avoid getting phished:

- Before you click any links, check the real site address by holding your cursor over the link. If it looks suspicious, don't click it.
- Know who is sending you emails before you click any links.
- Watch out for poorly written emails and attachments. These can contain malware like viruses or spyware.
- Beware of emails that ask you to provide sensitive information.
- Be leery if the topic of an email creates a feeling of urgency.
- If you need to access a site, enter the URL into the web browser yourself—don't click on any hyperlinks, open any attachments or copy and paste the URL from the email.

If you think an email in your government account could be a phishing attack, don't open it or click on any links. Clicking a malicious link could infect your computer. It can then spread to other users.

Instead, call the IT Service Desk immediately at 306-787-5000.



# Passwords

## Password best practices:

Just like how good home security is key to preventing a robbery, strong and secure passwords are key to keeping our information safe.

A good password is equally about the quality of password you choose, as it is about keeping it safe and secure.

Read on to learn how you can safeguard your passwords.

### Tips to protect your passwords

- Do not share your passwords with anyone.
- Change your password immediately if you suspect someone might know it.
- Do not write passwords down or save them in a file.
- If you lose your password, call the IT Service Desk at 306-787-5000. You can also retrieve your password yourself if you have registered in the Quest password self-service tool. You can register by clicking the Quest One Password Self Service shortcut on your desktop.
- Use different passwords for business and personal use.
- Longer passwords are better.
- Strong passwords are difficult to guess. A strong password could be made up of the first letter of each word in a phrase (i.e. "I'm a little teapot, short and stout" would be ialtsas. Adding numbers, special characters and upper case letters adds complexity. This password could be made better by changing it to 1@ltSa\$.



# Applications

## Use applications safely

Freeware, mobile applications and cloud-based storage applications like Google Drive can seem like attractive options for their unique service offerings or affordability. Unfortunately, if any of these applications are unapproved for work use, these benefits might come at an unforeseen cost.

When we open our systems up to unapproved applications, we also potentially open our systems to many hidden sets of eyes.

### Tips for safe application use

- As long as the software is IT division-approved, installed and managed, it is safe to use. Nothing unapproved should exist on your work desktop or laptop. Any updates to your desktop or laptop applications should be done by submitting an IT Service Request.
- Some applications live in the cloud, and don't need to be downloaded to use them. If these applications are used on work machines, users should keep sensitive government information out of these applications.
- Applications for mobile devices, like phones and tablets, should only be downloaded from recognized app stores. Examples of recognized app stores include the Apple store, Google store and BlackBerry app store.
- Users should not use government email addresses to sign up for non-work related services like games or social media.
- The installation of Bluetooth devices, like a Bluetooth mouse or speaker, must be approved and carried out by the IT division of Central Services. This can be done by submitting an IT Service Request.

### Use of Lync instant messenger and text messaging

- Lync and text messaging are convenient for quick discussions with other employees, like to tell a colleague that you're on your way. However, users should be aware that email is required for any business related to the Government of Saskatchewan that would in turn become an official government record.



# Social Media

## Know who's dropping by on social media

With social media reshaping the way we interact with each other, and even sometimes the way we work, it's important to distinguish between personal and professional use.

This is why separate accounts are a must for your personal and work-related government social media use. These accounts should also use different passwords from each other.

Most importantly, sensitive work information should never make its way onto social media.

Government of Saskatchewan has a social media policy in place for employees. To access the policy, visit [www.employeeservices.gov.sk.ca/ITSecurity](http://www.employeeservices.gov.sk.ca/ITSecurity).

## Security considerations for social media use

- Some security considerations for personal social media use may be less obvious than others. For example, features like geolocation and hashtagging can sometimes broadcast more information than you hope to.
- Geolocation is a feature used in many social media platforms that can tell others where you are. When this feature is enabled on some social media sites, it can attach a location to your photos or status updates.
- A hashtag is a text label on social media platforms that make it easier for users to find messages with a specific theme or content. As an example, on the Twitter social media site, users can search #SKLegDome to find Tweets about the Saskatchewan Legislative building's dome rehabilitation project.
- Make sure you either disable or properly manage your geolocation feature.
- Ensure any posts containing hashtags provide only the kinds of information you are comfortable sharing widely. Hashtags may override privacy settings, making your posts searchable beyond your intended audience.



# USB drive storage

## Drive safely

USB flash drives can be a convenient way of bringing files with you, whether it's to a meeting room or alternate work space.

When copying your files to a USB drive, your working files must also be kept on the Government of Saskatchewan network where they are backed up.

Government-issued, encrypted flash drives must be used for any sensitive data. Drives like these require a password to protect the data stored on them in the case of loss or theft.

Users should also be careful not to lose flash drives containing work information. If a drive containing government information is lost or stolen, it must be immediately reported to your supervisor and to the IT Service Desk at 306-787-5000.

Personal flash drives should never contain work information, and vice versa.

Be careful not to leave any flash drives laying around, and on the flip side, don't plug in any unknown flash drives you have found. Instead, turn it into your Ministry Security Officer.

## Where to get an encrypted flash drive

Encrypted USB flash drives can be ordered by submitting an IT Service Request. Plan ahead and place your order for any flash drives you may need now, so the drives are there when you need them.





# Working on the go

## **Hop on the IT security bandwagon**

Working on the go is a necessity for many jobs nowadays. As a result, we must be mindful of how, where and what we access when we work from different devices or networks.

## **Connecting remotely to the government network**

Users who have a government laptop can connect to the government network remotely from any Internet connection, anywhere. This connection gives you access to your work emails, your home and group network drives and access to your applications.

If you do not have a government-issued laptop, you can also access the government network through a web portal. This can be carried out on any device, and anywhere with an Internet connection like a coffee shop, airport, hotel or your home.

To get access to government's network using either of these two methods, you must gain approval for this service and corresponding charges from your IT Service Approver and submit an IT Service Request.

## **Keeping your devices safe**

When travelling by car, either take your device with you, leave it in a locked trunk, or at the very least make sure it is hidden from view within the locked vehicle. Remember, heat and cold can damage your devices.

When flying, keep your devices with you as carry-on luggage, not checked baggage, and keep them in sight at all times.

When staying in a hotel, it's best to lock your devices in a hotel room safe if available. Otherwise, hide your devices out of plain sight.



# lost, stolen or found devices

## Lost devices

If your device has been lost or stolen, you must report the incident to your supervisor and to the IT Service Desk.

This applies to all mobile devices, like a laptop, memory stick, external hard drive, cell phone, smart phone or two factor authentication token/fob/device.

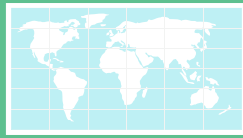
**If you are a supervisor, and your employee reports a lost or stolen device to you, please collect this information:**

- Is the device password protected?
- Is it encrypted?
- Can you describe the device, including the asset number and serial number?
- What were the circumstances surrounding the incident?
- Did you report this to the service desk?

Supervisors should also report lost or stolen devices to other ministry officials.

## Found devices

If you have found a government device, please report this to the IT Service Desk at 306-787-5000 and to your supervisor.



# Outlook

## Look out on Outlook

While it can be very convenient to actively share your calendar with other Outlook users like other members of your team, be aware that if you actively share your calendar with anyone, they will have the ability to see all of your meeting details. This is why calendar sharing should be limited.

If you do happen to share your calendar, make a point of keeping your delegated access up-to-date. Also be sure to mark anything sensitive as a private appointment. This can be done by clicking the lock icon in Outlook.

Calendar items for meetings on sensitive matters, as well as personal information like banking or doctor's appointments, are a good idea to mark as private. Sensitive information should be omitted entirely from the calendar subject line, and kept entirely within the actual meeting discussion.

In addition to managing calendar privacy settings, users should pay careful attention to Outlook's auto-fill feature. This feature may confuse you into unintentionally inviting the wrong person to a meeting. For example, you may invite Joan Smith when you mean to invite John Smith.

### How to check who has access to your Outlook 2010 calendar:

- Open Outlook.
- Open your calendar.
- Click the File tab, then Account Settings, then Delegate Access.
- From there, you can add or remove delegates as necessary.



# Our Policies

## Our Policies

All users in the Government of Saskatchewan's IT environment are bound by the IT Acceptable Usage policy and the newly released Information Security policy, which can be found at [www.employeeservices.gov.sk.ca/ITSecurity](http://www.employeeservices.gov.sk.ca/ITSecurity).

Keep in mind that our IT systems are meant for you to carry out your duties and responsibilities, and should be used for that purpose.

Here are some general tips to guide your use of government's IT resources.

### Limited personal use of Government's IT resources is allowed with certain conditions.

- Personal use of government systems should be minimal and for a short time, and should not be visible to the public.
- Employees should consider using their own devices for personal use.

### Remember, Government systems can't be used for the following activities:

- Activities that conflict with your duties and responsibilities.
- Illegal activities.
- Actions that violate management direction.
- Activities for personal gain (i.e. gambling, operating a business, managing investments).
- Anything that would harm the reputation of the public service.
- Activities that violate other workplace policies.

### Here are other things to remember when using Government systems:

- Don't change any software or hardware configurations.
- Only the IT division may install hardware or software on your system.
- Do not collect or disclose personal information or personal health information without authorization.
- Don't access offensive content, and keep your personal beliefs off government's systems.
- Don't harm anyone. (i.e. harassment, bullying).



## A Team Effort

### **Working together for IT security**

While we all know how important it is to protect sensitive data, this is a major task — it's not something that can be done by one person, branch, division or even ministry.

While the IT division of Central Services plays a big role in helping us keep our data safe, all users in government play an equally important part in keeping sensitive information secure.

Equipped with the information in this guide, employees of the Government of Saskatchewan should feel more comfortable handling the sensitive information placed in our care.

It's the sum of our efforts that help us safeguard the information in our trust and uphold our responsibility to all people of Saskatchewan.