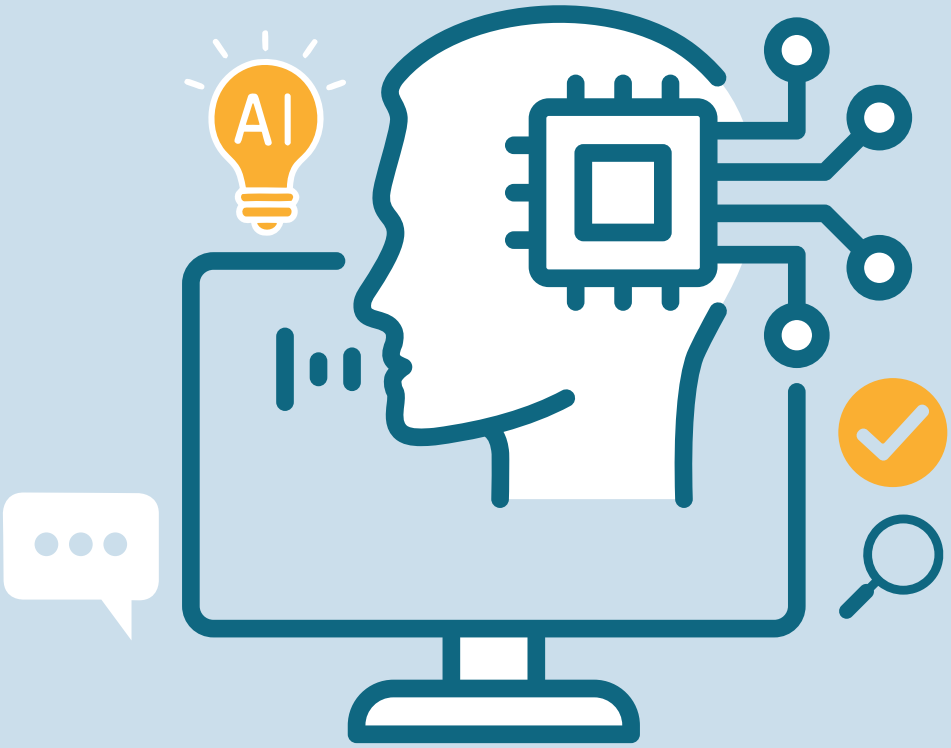
Digital Privacy & Cybersecurity for Small Centres



AMSSA
Strengthening Diversity In BC

Intro: Why Privacy & Cybersecurity Matter

Purpose

This guide is designed to help small settlement organizations strengthen their privacy and cybersecurity practices in practical, accessible ways. It focuses on protecting sensitive client information, staff data, and organizational systems while recognizing that many small teams operate with limited technical resources or dedicated IT support.

Why it matters

Settlement organizations often work with highly sensitive information such as immigration documents, identification, personal contact information, and case notes. Protecting this information is essential to maintaining trust with clients and partners.

Cybersecurity incidents can disrupt services, damage organizational reputation, and create legal or regulatory risks if personal information is exposed.

As organizations adopt more digital tools for communication, file storage, and service delivery, protecting accounts, devices, and data becomes an essential part of responsible program delivery.

Why it's achievable

Many people assume cybersecurity requires complex technical expertise, but most effective protections are actually simple practices and habits that staff can follow every day. Actions such as using strong passwords, enabling multi-factor authentication, recognizing suspicious emails, and limiting access to sensitive information can significantly reduce risk.

The goal is not to eliminate every possible threat, but to make your organization much harder to target, and better prepared to respond if something does go wrong.

This guide focuses on practical steps that small teams can implement, even without IT staff, using tools and systems they may already have.

Understanding the Risks

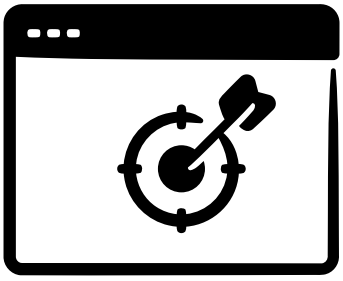
Common Cyber Risks

Small organizations face many of the same threats as larger ones, but often with fewer resources to manage them. Common risks include:

- Phishing emails
- Weak or reused passwords
- Malware or ransomware
- Careless distribution of sensitive info

Why Small Organizations Are Targeted

Cybercriminals often focus on smaller organizations because they may have fewer security protections in place. Staff are often busy, multitasking, and managing many responsibilities, which can make it easier for suspicious emails or requests to slip through unnoticed. Limited cybersecurity training can also increase risk.



The Reality of Cyber Incidents

It's often thought that cyber attacks require sophisticated hacking techniques. In reality, most incidents begin with simple human actions such as clicking a malicious link, sharing login information, or using weak passwords.

The good news is that improving everyday practices can prevent many common security incidents.

Simple Cybersecurity Practices Every Organization Should Adopt

1 Use Multi-Factor Authentication (MFA)

Multi-factor Authentication adds a second step when logging in, such as a code sent to your phone. Even if a password is stolen, MFA can help prevent unauthorized access.

2 Use Strong Password Practices

Strong, unique passwords help prevent unauthorized access to your accounts. Avoid reusing passwords across systems and consider using a password manager to store them securely.

3 Keep Systems Updated

Regular updates help fix security vulnerabilities that attackers can exploit. Enable automatic updates on computers, phones, and software whenever possible.

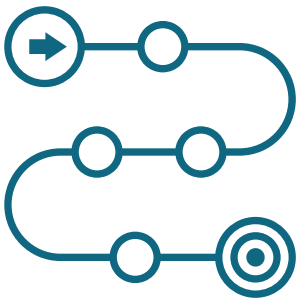
4 Provide Regular Staff Training

Regular training helps staff recognize common threats such as phishing and suspicious links. Even brief reminders can significantly reduce the risk of accidental security incidents.

Tips for Effective Cybersecurity

- Lock your computer when stepping away from your desk
- Confirm recipient addresses before sending sensitive information
- Store files in approved systems, not on personal devices or USB drives
- Report lost devices or suspicious activity immediately
- Have a plan for responding to security incidents
- Use separate Wi-Fi networks for staff and for guests or clients
- Have a written IT policy, and provide training on your procedures and standards

Creating a Simple Security Process



Why it's important

Even small organizations benefit from clear, simple procedures. When staff know what to do if something goes wrong, security incidents can be addressed more quickly and with less confusion. Establishing a few basic processes helps protect client information and ensures staff respond consistently to common situations.

Incident Response

Staff should understand what steps to take if something suspicious occurs. This includes knowing who to notify if unusual activity is detected, how to report lost or stolen devices, and what to do if an account may have been compromised. Having clear reporting procedures helps the organization respond quickly and limit potential damage.

Staff Onboarding and Offboarding

Managing system access when staff join or leave is an important part of protecting information. New staff should only be given access to the systems and data required for their role. When staff leave the organization, access to accounts and systems should be removed immediately.

Vendor & Partner Access

External vendors or partners may sometimes require access to systems or information to perform their work. Access should be limited to only what is necessary for the task and removed once the work is complete. This helps reduce the risk of unnecessary exposure to sensitive information.

Your IT Policy

Every organization that handles client information should have a clear IT policy. An IT policy helps staff understand how technology should be used, how information should be protected, and what to do when something goes wrong. It does not need to be complex or technical, but it should be documented, taught to staff and consistently followed.

What to Include

Acceptable Use of Technology

Defines how staff may use organizational computers, networks, email, and internet access for work purposes.

Access Control

Outlines how access to systems and information is granted, reviewed, and removed.

Device Security

Sets expectations for securing laptops, mobile phones, and other devices used for work.

Change Management

Ensures that significant changes to systems, software, or infrastructure are reviewed and documented.

Incident Reporting & Response

Explains how staff should report security concerns, lost devices, or suspected breaches.

Vendor & Third-Party Access

Establishes rules for granting access to service providers & external partners.

Password and Authentication

Establishes rules for strong passwords, account protection, and the use of multi-factor authentication.

Data Protection & Privacy

Describes how sensitive client and organizational information must be stored, shared, and protected.

Approved Software & Applications

Defines which software and cloud services are approved for organizational use.

Email & Communications

Provides guidance on identifying suspicious messages and safely handling attachments and links.

Backup & Data Recovery

Defines how important data is backed up and how systems can be restored after a failure or attack.

Remote Work & Network Access

Sets expectations for securely accessing organizational systems from home or public networks.

Other resources

Canadian Centre for Cyber Security

Provides practical cybersecurity guidance, alerts, and tools for organizations of all sizes.
https://www.cyber.gc.ca

Office of the Privacy Commissioner of Canada

Offers guidance on privacy obligations & best practices for protecting personal information.
https://www.priv.gc.ca

BC Office of the Information and Privacy Commissioner

Provides resources on privacy responsibilities and information protection for organizations operating in British Columbia.
https://www.oipc.bc.ca

Get Cyber Safe

A Government of Canada public awareness program that provides simple advice on staying safe online.
https://www.getcybersafe.gc.ca

National Cyber Threat Assessment

Provides insight into current cyber threats affecting Canadian organizations.
https://www.cyber.gc.ca/en/guidance/national-cyber-threat-assessment-2025-2026

Cyber101 - Free Cybersecurity Awareness Training

Provides short, beginner-friendly training modules that help staff recognize common cyber threats and improve cybersecurity awareness.
https://www.cyber101.com

Affiliation of Multicultural Societies and Service Agencies of British Columbia
Metrotower II, Suite 2308, 4720 Kingsway, Burnaby, British Columbia, V5H 4N2
1 888 355-5560 | 604 718-2780 | amssa@amssa.org | www.amssa.org