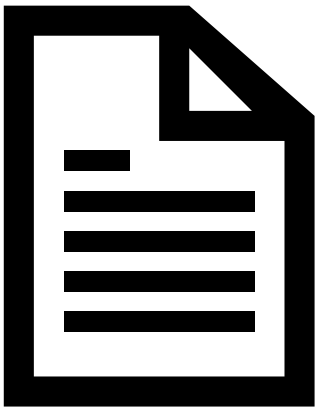

ACCEPTABLE USE POLICY

SecureNet Global (SNG)

Updated August 2025

Contents

Purpose

The purpose of this policy is to outline the acceptable, responsible and safe use of SNG's digital resources and information. These rules are in place to protect SNG's assets and information from inappropriate use. Authorized access to the digital resources and information can protect SNG to expose to risks including cyberattacks, compromise of network systems and services, reputational damage and legal issues.

Scope

This policy applies to all members of SecureNet Global (SNG) including Executive Management, IT, Information Security, Research & Development, Security Operations Center (SOC), Sales & Marketing, Finance & HR, Client Support, Contractors, and Volunteers, regardless of work location (onsite, remote, or hybrid).

This policy is applicable for any use of Information Assets including:

- **Hardware:** Computers, Laptops, Mobile devices, Printers.
- **Software & Applications:** Operating Systems, desktop & web-based applications.
- **Data:** Structured & Unstructured data such as databases, files, audios, videos, images, documents.
- **Cloud Services:** Microsoft 365 (Exchange, SharePoint, Teams, OneDrive) and other approved cloud-based services.
- **Network Services:** Corporate VPN, VoIP, firewalls, wireless access, and related network systems.

Statement of Policy

Roles & Responsibilities

1. **Policy Owner:** *Chief Information Security Officer (CISO)*

Responsible for overall ownership of this policy and ensuring alignment with organizational security objectives and regulatory requirements.

2. **Policy Review and Update:** *Information Security Department*

Led by Information Security Manager, responsible for reviewing this policy at least annually, or when significant changes occur, and updating it as needed.

3. **Policy Implementation and Execution:** *Human Resources (HR) Department*

Responsible for communicating the policy to all employees, ensuring acknowledgment during onboarding, and coordinating enforcement with the Information Security team.

4. **Policy Compliance Measurement:** *Information Security Department*

Responsible for monitoring adherence to this policy through technical controls, audits, and incident reporting.

5. **Policy Adherence:** *All Users*

- All employees, contractors, and third parties are required to read, understand, and comply with the Acceptable Use Policy.

Acceptable Use

- Users must only use company-approved technology, systems and services.
- All enterprise assets are issued solely for business use and must be returned upon termination or contract completion.
- Users must protect Personally Identifiable Information (PII), confidential, or regulated data (including information governed by **PIPEDA**) and prevent unauthorized access.
- Users are responsible for safeguarding information, systems, and assets under their care, and must report any loss, theft, or damage immediately to IT.
- Passwords must be securely managed using approved password managers and comply with the company's Password Policy.
- Users must keep knowledge about information and information systems gained during employment confidential and confidentiality must be maintained after employment ceases.
- All IT systems and services are for legitimate business purposes only; personal use is not permitted.
- Employees will be responsible for all the network traffic generated by their devices, adhering to stipulated limitations for business purposes.
- Employees must maintain the latest system software update to protect it from viruses, worms, trojans, and other harmful programs.
- Only authorized personnel may post or represent the company on social media or external websites.
- Users must secure their workstation and lock their screen when away

Prohibited Use

- Making false, misleading, or fraudulent statements on behalf of the company is prohibited.
- Employees should not try to hide their identity from the system and misuse it to threaten, intimidate, or harass anyone.
- Letting other employees or external individuals use the company assets is prohibited.

- Users-assigned accounts must only access assets, operating systems, applications, files, and data to which they have been granted access. The ability to inadvertently read, execute, modify, delete, or copy data does not imply permission to do so.
- Downloading, storing, or sharing copyrighted, obscene, or illegal materials is prohibited.
- Employees are strictly prohibited from using the system network systems to probe into the personal details of others and publish sensitive information regarding employees on a public forum.

Remote Work & BYOD

- All work-related data and activities must be conducted using company-approved assets.
- Users must not connect enterprise assets to open, unencrypted WiFi networks.
- Users must be aware of their surroundings when working remotely to ensure others are not shoulder surfing or viewing sensitive material.
- Personal devices must not be connected to the enterprise network without formal authorization.
- Enterprise data must not be stored on personal devices without formal authorization.
- In cases where enterprise data resides on a personal device, the company reserves the right to remotely wipe the device if it is lost, stolen, compromised, or upon termination of employment.

Monitoring, Privacy & Violation

The enterprise reserves the right to monitor, access, and disclose all information generated and actions performed using enterprise IT assets. Files, messages (including attachments), and logs may be retained and used as evidence in litigation, audits, and investigations.

When using enterprise resources, the user shall have no expectation of privacy. Access and use of the Internet, including communication by e-mail and instant messaging and the content thereof, are not confidential, except in certain limited cases recognized by law.

Users who are aware of any event which threatens the availability, integrity or confidentiality of enterprise data, or which breaches any standard, policy, procedure, or any associated requirement, or is contrary to law, must immediately contact IT or their immediate manager.

Review & Revision

The policy shall be owned by the Information Security Department and reviewed annually under the direction of the Information Security Manager and CISO. The review will include input from IT, HR, Legal and other relevant departments to ensure alignment with operational, regulatory, and technological changes. The CISO is responsible for final approval and communicating updates to all employees.

Enforcement & Disciplinary Action

Compliance with this policy is mandatory for all employees, contractors, and third-party users. Any violation of this policy may result in disciplinary action appropriate to the nature and severity of the breach. Disciplinary measures may include, but are not limited to:

- Verbal or written warnings
- Temporary or permanent suspension of system access
- Mandatory retraining or counselling
- Formal disciplinary proceedings up to and including termination of employment or contract
- Legal action where a violation involves criminal or civil offenses

All confirmed or suspected violations must be reported to the Information Security Manager or Human Resources Department for investigation and appropriate action.

Acknowledgement / Agreement

I acknowledge that I have read, understood, and agree to comply with the terms of the Acceptable Use Policy. I understand that company IT systems and data are provided solely for authorized business purposes, and any misuse may result in disciplinary action or legal consequences.

Employee Name: _____
Employee Signature: _____
Date: _____

(For Digital Form)

By clicking I Agree, I confirm that I have read and understood the Acceptable Use Policy.