DATA PROTECTION POLICY

This Data Protection Policy provides definitive information on the prescribed measures used to establish and enforce the IT security program at [organization name]. The organization is committed to protecting its employees, clients, and itself from damaging acts that are intentional or unintentional. Effective IT security is a team effort involving the participation and support of every [organization name] user who interacts with data and information systems.

SCOPE

This policy applies to all [organization name] data, information systems, activities, and assets owned, leased, controlled, or used by the organization, its agents, contractors, or stakeholders. These policies, standards, and procedures apply to all of [organization name]. employees, contractors, and sub-contractors and their respective facilities supporting the organization’s business operations, wherever the organization’s data is stored or processed, including any third-party contracted by the organization to handle, process, transmit, store, or dispose of its data.

POLICY

In protecting and securing data, [organization name] will ensure a safe physical environment.

This policy provides detailed information on our IT security program. However, the following overarching guidelines should be kept top of mind at all times:

* Access to technological assets and intellectual property will be restricted to authorized personnel only.
* Organization-owned devices should be stored in secure locations when not in use.

**Data Classification**

Data will be classified based on its sensitivity, and access to sensitive data is restricted to authorized personnel only. This policy classifies data into (XX) categories:

* **Confidential data** requires the highest level of security due to the risk it poses to [organization name]. It includes data protected by federal or provincial laws, such as Personal Information (PI), nonpublic financial information (NFI), and Protected Health Information (PHI).
* **Restricted data** includes all other non-public data that could harm an individual's privacy or negatively impact the organization’s finances, operations, or reputation. Access to restricted data should be limited to those with legitimate reasons, and a reasonable level of security should be applied.
* **Public data** has no restrictions on distribution and poses no harm to the organization or its stakeholders.
* [add other classifications as deemed necessary.]

**Employee Access**

[organization name] must prevent the loss of restricted, confidential, or sensitive data in order to avoid reputational harm and negative consumer effects. The protection of data is a crucial business necessity, but access to data and the ability to work efficiently are also essential. As such, access to organization systems and data will be granted only on an as-needed basis. Security initiatives begin with the vetting of prospective employees, and access to systems and data follows strict guidelines.

Prior to Employment

The objective is to ensure that employees and contractors understand their responsibilities and are suitable for the roles for which they are considered. In addition, candidates should be vetted in the hiring process to minimize the risk of compromising internal IT sources. The contractual agreements with employees and contractors should outline the employees and the organization’s responsibilities for information security.

During Employment

[organization name] has developed policies and procedures to ensure that the IT network is utilized appropriately and remains secure.

Position Categorization

Upon hire, an employee will be categorized as either a "general" user or a user with "administrative access." The classification of the employee will be noted in the access agreement. It is the responsibility of [organization name] to make the determination of categorization for each employee.

The organization, considering the recommendation, reserves the right to change the classification of any employee at any time for operational reasons. Should this occur, this action will not constitute constructive dismissal.

Third-Party Security

All third parties (not employees of [organization name]) that have access to the organization’s network will be required to read, follow, and acknowledge that they understand [organization name]’s policies and procedures.

**Physical Security**

[organization name] will ensure access to technological assets and intellectual property is restricted to authorized personnel only. The following measures will be implemented to ensure access control:

* Each employee and contractor with access to organization data and devices is issued a unique set of login credentials.
* Employees with remote access to organization data and devices will use multifactor authentication.
* Physical access control measures such as biometric readers, access cards, and CCTV cameras are implemented to prevent unauthorized entry into restricted areas.
* When not in use, organization-owned devices are stored in secure locations, such as locked cabinets, safes, or data centres.
* Employees and contractors must log off and lock their computer screens when they are away from their desks.
* Encryption is required to protect sensitive data stored on organization-owned devices.

**Information Security Awareness and Training**

All [organization name] employees, contractors, and third-party vendors must be trained on the importance of information security and their roles and responsibilities in protecting organization data and assets.

This training will be developed and delivered on an annual basis. The training may be delivered more frequently, based on security and/or operational requirements, for all or specific employees, as determined by the organization.

This training will include education concerning [organization name]'s IT policies, protocols, and procedures. In addition, training will include:

* Information security basics
* Information security
* Safeguarding information
* Data privacy and storage
* Breaches of privacy
* Data encryption
* Use of personal devices and organization devices
* Information assets
* [Add information as needed.]

Vendor Education and Training

All vendors who are provided with access to [organization name]’s IT network will be required to comply with the organization’s IT policies.

**Security Alerts and Notification Process**

[organization name]’s IT network will be monitored to ensure that it is safe and secure.

In the case of a potential threat, security measures will be immediately put in place.

**Data Backup and Encryption**

Data security will be ensured by backing up and encrypting data according to the following guidelines:

* All intellectual property data will be backed up regularly, and backups will be stored securely offsite to protect against data loss in the event of a disaster.
* Backups will be tested periodically to ensure that data can be restored accurately and completely.
* Access to backup data is restricted to authorized personnel only.
* Sensitive data will be encrypted when at rest and in transit to protect against unauthorized access.
* Encryption keys are stored securely, and access to them is restricted to authorized personnel only.
* Employees and contractors must use encryption tools when handling sensitive data on their devices, such as laptops or smartphones.

**General Employee and Third-Party Responsibilities**

The responsibilities of every [organization name] employee are as follows:

* Complete [organization name] training in security awareness.
* Notify supervisors or managers immediately of any unknown, unescorted, or otherwise unauthorized individuals on organization property.
* Avoid referencing, accessing, or using sensitive or confidential data in public or via non-organization-controlled systems or channels of communication. (e.g., using external email services that [organization name] does not host).
* Ensure printed documents are stored in secure locations (e.g., a drawer with a lock).
* Ensure that assets containing [organization name] information are not left unattended or vulnerable (e.g., left exposed at workstations or visible in the backseat of a car).
* Use strong passwords on all [organization name] systems in accordance with the password policy. These credentials must be unique and cannot be used on any other external systems or services. Passwords should be changed periodically (e.g., every 90 days).
* Notify management immediately if a device containing organization information is lost (e.g. mobiles, laptops, etc.).
* Notify management immediately when you suspect that a certain system or process is not compliant with this policy or the information security objective.
* Utilize only organization-provided or approved transfer mechanisms when transferring data within the organization (e.g., encrypted USB keys, file shares, email, etc.). [organization name] will provide employees with suitable systems or equipment. Employees must not use alternative mechanisms to manage organization data.
* Ensure that any data being transferred on a portable device (e.g., USB stick, laptop) is encrypted in accordance with industry standards and applicable laws and regulations.
* Remote employees must take additional precautions to ensure data is handled appropriately.
* Remote employees must log out of the remote connection when they are not using the computer or device to access information. Leaving the connection open could expose the organization’s data to malicious harm.
* Return all records in any format that contains organization data upon termination of employment.

Note: Any suspected or confirmed security incidents must be reported immediately to management. Further questions regarding these responsibilities should be directed to management.

**Appropriate Use of Computers, Email, and the Internet**

Employees should only use organization computers, email, and technology for business as outlined in the employment contract, job description, or by the organization. Personal use of the organization's network is acceptable if not abused.

During breaks, lunch, and off-work hours, employees can use organization computers, technology, and the internet for personal use. [organization name] employees who post on social media must be professional and respectful. Any activity that reflects poorly on the organization or endangers equipment, people, or organization policy is not allowed.

Refer to [organization name].’s Social Media Policy and Use of Technology Policy for further details.

**Use of Personal Devices**

When authorized in writing by management, certain employees may use personal electronic devices for work. Such devices include cell phones, tablets, laptops, and computers. Only employees working on [INSERT NATURE OF WORK, e.g., sales] may be issued authorization to use personal devices for work.

This authorization is subject to the following guidelines:

* The personal device must pass an inspection.
* Employees may be required to install organization-approved anti-virus, mobile device management software, and “remote-wipe” software.
	+ The software stores all organization-related information, including calendars, e-mails, and applications, in a password-protected location.
	+ The “remove-wipe” software remotely deletes sensitive organization information from a misplaced or stolen device.
* Employees must not use cloud-based apps or backups that allow the transfer of organization data to unsecured parties.
* Employees can't use unsafe websites.
* Personal devices must not synchronize with home devices.

[organization name] may monitor and preserve any data, voice mail, telephone logs, Internet use, and network traffic to determine proper use.

The organization reserves the right to review, retain, or release personal and organization-related data on personal devices during an investigation or litigation. No employee may disable monitoring software or systems.

**Remote Work**

Remote access will be strictly controlled. Authentication with a one-time password or public or private keys with strong passphrases will be used to enforce control. Remote employees should adhere to the following:

* Never disclose email or system login credentials, especially passwords, to anyone, including family members.
* Never save their passwords on the computer/device used for remote access to prevent any third party from gaining access to the computer/device.
* Ensure that their organization-owned or personal devices remotely connected to the organization network are not simultaneously connected to any other networks, with the exception of user-controlled personal networks.
* Never use non-[organization name] email accounts (e.g., Hotmail, Yahoo, or Gmail) or other external resources to conduct [organization name] business.
* Never reconfigure equipment for split-tunnelling or dual-homing.
* Get approval for non-standard hardware configurations and security configurations from management.
* Install and use the most recent anti-virus software.
* Ensure personal equipment used to connect to [organization name] networks meets the remote access requirements of organization-owned equipment.

For further information on remote work, refer to [organization name]’s Working from Home Policy.

**Disciplinary Actions**

Should any employee or third party breach the terms of this policy, they may be subject to discipline, up to and including termination with cause. Personal sanctions, including limited or restricted access, may also be necessary at the determination of management.

**Termination of Employment**

At the termination of employment of an employee, termination protocols will be initiated relating to IT security.

A Termination Checklist must be completed for all terminations.