

INFORMATION SECURITY POLICY

DOCUMENT INFO

DOCUMENT CODE - REVISION	EFFECTIVE DATE
MGT-POL-001-3	2024-08-12
TITLE	STANDARD
INFORMATION SECURITY POLICY	ISO 27001
AUTHOR	DATE CREATED
JAY EDADES	2024-07-18
APPROVED BY	DATE APPROVED
PETER MORRISON	2024-08-12

REVISION HISTORY

REVISION	DATE	REMARKS	REQUESTED BY
1	2023-05-18	Consolidated	Jay Edades
2	2023-09-18	Updated the sentence from 'which will be accredited' to 'which has been accredited to' after receiving the ISO 27001 Certification	Peter Morison
3	2024-08-12	Added document info on first page to track version control.	Jay Edades

INFORMATION SECURITY POLICY

Introduction:

The security of data and information assets is critical to the future success of PTI (Paperless Trail Inc.).

The management team of PTI is fully committed to ensuring the Confidentiality, Integrity, and Availability of information. To this end, we have implemented an ISMS (Information Security Management System) which has been accredited to ISO 27001.

Objective & Scope:

The objective of this Information Security Policy is to set high-level policies and principles for information security within our organization. This Policy applies to all permanent, temporary, or contractual staff of PTI.

The ISMS will encompass all PTI's internal information, and in particular, Data and Information that PTI receives, handles, and processes, on behalf of our stakeholders (employees, customers, and suppliers).

The ISMS will comprise the information security policies, procedures, work instructions, and a comprehensive risk management framework to effectively manage and protect the data and information of PTI and its stakeholders (including customers) from security threats, whether internal or external, deliberate, or accidental.

Commitment:

The management of PTI is committed to ensuring that:


- Appropriate & necessary resources are allocated to effectively implement, operate, and review the ISMS.
- Stakeholders (employees & customers) are aware of information security risks. That this awareness is enhanced through regular training.
- Applicable legal, regulatory, and contractual requirements related to information security are met and regularly reviewed.
- The ISMS remains effective through a process of periodic reviews to continuously improve the suitability and adequacy of the ISMS.
- Information security responsibilities are fully communicated to all stakeholders (employees, customers, and suppliers).

Exceptions

Any exceptions to this policy must be documented and agreed to by the Management Committee.

Non-compliance

Failure to comply with this policy and supporting policies and procedures may be considered a disciplinary offense.



Peter N. Morrison | September 2023
President