Privacy Policy

Content

Review Procedure

The Managing Director will review the policy as required. The review schedule is directed in response to organisational and/or legislative changes and requirements. The review will be undertaken in consultation with workers, company representatives and other relevant parties. All relevant persons will be made aware of changes made as a result of the review.

This policy will be reviewed if:

- there are changes in the workplace that may affect policy;
- policy is not effective;
- there are legislative changes that affect the policy;
- there is a breach of this policy;
- this policy reviewed at least annually.

Document Control

Distribution Record Register

Copy	Issued to	Controlled Copy		Authorised by	Recipient Signature	Issue Date
		Y	N			
1		☐	☐			
2		☐	☐			
3		☐	☐			
4		☐	☐			
5		☐	☐			

Amendment Record Register

ISSUE #: 1
ISSUE DATE: 1 MARCH 2023

Rev. #	Date	Details		Description of Changes	Approved By
		Section #	Para. #		
1					
2					
3					
4					
5					

Regulations and Guidelines

Fair Work Act 2009

Disclaimer: *This document contains material to assist in addressing Occupational Health and Safety management obligations. Although every effort has been made to ensure the accuracy of this information at the time of publication, it is provided as guidance only and does not provide legal advice on meeting your obligations.*

Privacy Policy

DEFINITION

"We, us, our, our company or the organisation" means Peritus Technology Pty Ltd

POLICY

Peritus Technology Pty Ltd is committed to the protection of employee privacy. Accordingly, we will collect only information that is relevant and necessary to your employment. This policy details our ongoing obligations to you in respect of how we manage your Personal Information.

The information will not be used for any purpose other than that for which it was collected. We may need to disclose personal information to service providers, agents, contractors, or others from time to time. If we do this, we require these parties to protect your information.

We will use various physical and electronic security measures, including restricting physical access to our offices, secure methods of record disposal, firewalls and secure databases to keep personal information secure from misuse, loss or unauthorised use or disclosure.

RESPONSIBILITIES

We are responsible for ensuring that:

- the identification, implementation, and maintenance of organisation information privacy policies and processes are implemented; and
- a process for receiving, documenting, tracking, investigating, and disposal of privacy-related information is established and administered; and
- action is taken on all complaints concerning the organisation's privacy policies and processes.

The nominated privacy officer is responsible for:

- performing initial and periodic information privacy risk assessments and monitoring activities; and
- working with management and other related personnel/departments to ensure that the organisation has and maintains appropriate privacy and confidentiality information; and
- provide training/orientation to all employees, contractors on required privacy policy provisions; and
- ensuring compliance with privacy processes; and
- manage access, storage and disposal of confidential information.

COLLECTION OF PERSONAL INFORMATION

Personal information can include but may not be limited to:

- Name, address, email, phone number; and
- Contact information for next of kin; and
- Bank accounts; and
- Working and holiday hours; and
- Production data; and
- Injury and health data; and
- Education and qualifications; and
- Tax information tax file number, ABN; and
- Insurance records; and
- Payroll information; and
- Superannuation accounts; and
- Salary and wage information; and
- Criminal records; and
- Employee's compensation.

We will only collect personal information as necessary. All information will only be collected by lawful and fair means and not in an unreasonably intrusive way. For example, Peritus Technology Pty Ltd will collect information in the following manner.

Payroll information is to be kept confidential. Payroll information will not be provided to any other staff member or third parties unless the employee has provided prior written approval.

USE AND DISCLOSURE OF COLLECTED CONFIDENTIAL INFORMATION

We will only use and disclose personal information for the following purposes:

- To establish, maintain and manage employee and contractor functions such as communication, recruitment, taxation, payroll; and
- To establish, maintain and manage customer functions such as invoicing, taxation, communication; and
- Health and employee's compensation claim concerning any injuries, illnesses while at work; and
- Professional services including legal, human resources, industrial relations, accounting and insurance services; and
- Otherwise as permitted or required by law; and
- Otherwise, with the individual's consent.

EXTERNAL DISCLOSURE OF CONFIDENTIAL INFORMATION

Apart from the use by the organisation, we will only disclose personal information to external individuals and bodies as required to fulfil business requirements which may include:

- Technology and other support service providers; and
- Security providers; and
- External consultants and agencies for legal services, human resources, industrial relations, accounting, and insurance purposes.

All employees, contractors, suppliers and customers must report immediately any known or suspected breaches of confidential information by an unauthorised person for an unauthorised purpose. Reportable breaches of information may include:

- Unauthorised access to a system that stores confidential information; and
- Loss or theft of a system or a physical record that contains confidential information; and
- Computers hacked or compromised; and
- Passwords compromised.

SECURITY OF CONFIDENTIAL INFORMATION

We will take all reasonable steps to protect the personal information it holds from misuse, loss and unauthorised access, modification or disclosure. No employee, contractor or supplier is permitted to store confidential information on any personal computer or portable storage device unless authorised.

Reasonable steps will be taken to ensure personal information remains accurate and up to date. Peritus Technology Pty Ltd provides the right to access the personal information held by the information owner. Any request for access to this information or enquiries concerning the privacy, or currency, of any held information, can be made by contacting: the Privacy Officer: ***Ian McLachlan*** by email ***ian.mclachlan@peritech.com.au***

Where no longer required, personal information will be destroyed or de-identified except where the information is required to be kept by law or court order.

DISPOSAL OF CONFIDENTIAL INFORMATION

All employees will be given instructions for properly disposing of hard copy, digital data, and materials containing personal and confidential information.

We will securely dispose of confidential information. Before destroying records containing confidential information, the privacy officer will:

- have authorization/endorsement to dispose of the records from *Ian McLachlan* and
- check and confirm that records are no longer needed for ongoing business; and
- ensure records are not required for any current or pending legal action; and
- consider any other potential reason to retain confidential records, e.g., legislated record-keeping timeframes.

Destruction of records will be undertaken in the most appropriate and secure manner. It will be undertaken as soon as possible after authorisation is given, e.g., shredding of paper-based records or physical destruction or overwriting digital media. Failure to follow documented disposal procedures may lead to disciplinary action.

DESTRUCTION METHOD TABLE

(Examples given. Add or modify this table to suit your business processes)

Record Medium	Non-Sensitive	Moderately Sensitive	Highly Sensitive
Hard disc drive	• *Overwriting* • *Purging*	• *Purging* • *Physical destruction*	• *Physical destruction*
CD/DVD	• *Overwriting* • *Purging*	• *Purging* • *Physical destruction*	• *Physical destruction*
Mobile phone / Tablet	• *Overwriting* • *Purging*	• *Purging* • *Physical destruction*	• *Physical destruction*
Paper record	• *Single Shredding*	• *Cross shredding*	• *Cross shredding* • *Burning*

After the destruction process is complete, professional paper shredding and hard drive and media destruction services must provide a Certificate of Destruction confirming the time, date and method of destruction.

Signature:  **Date: 01 March 2023**