DATA HANDLING & DATA SECURITY POLICY

Pacific Mining Parts, also known collectively as PMP Group (the "Company"), is committed to responsible data handling, security, and privacy protection across its global operations.

This policy applies to all PMP Group entities, employees' contractors, consultants, and authorised third parties who handle Company data in any jurisdiction where PMP Group operates.

Where local law imposes stricter requirements than this Policy, the stricter requirement will apply. In the event of any inconsistency between this Policy and applicable law, applicable law prevails.

PURPOSE

This policy outlines how the Company collects, processes, stores, protects, shares, and disposes of data, including personal, sensitive and business-related information, in alignment with:

- internationally recognised privacy and information security frameworks (e.g., OECD Privacy Principles and ISO/IEC 27001 information security standards),
- applicable local laws (including General Data Protection Regulation (GDPR), Australian Privacy Act 1988, and other relevant jurisdictions).

SCOPE

This policy applies to all the Company entities, employees, contractors, consultants, and authorised third parties who handle Company data in any jurisdiction where the Company operates.

DATA TYPES

This policy applies to:

- Personal Information (as defined in the Privacy Policy and applicable data protection laws)
- Sensitive information (e.g., health data, financial information)
- Business, operational, and technical data
- Website usage, communications, and telemetry data

For the purposes of this Policy, "Personal Information" and Sensitive Information" shall have the meanings given under applicable data protection laws in the relevant jurisdiction.

Sensitive information is handled in accordance with the Company's Privacy Policy and applicable law.

DATA COLLECTION & USE

Data is collected and processed only where necessary for legitimate business purposes. Where required by applicable data protection law, personal information will only be processed where a valid lawful basis exists, which may include:

- Performance of a contract
- Compliance with a legal or regulatory obligation
- Legitimate business interests
- Consent (where required by law)

Purposes include:

- Delivery of products and services
- Communication and relationship management
- Marketing and informational activities (in compliance with applicable direct marketing and electronic communication laws, including consent and unsubscribe requirements where required)
- Legal, regulatory, and contractual compliance

Data collection is limited to what is relevant and proportionate to these purposes.

DATA STORAGE & RETENTION

Data is stored using secure systems designed to protect against unauthorized access, alteration, or loss.

Data is retained only for as long as necessary to fulfill its intended purpose or comply with legal and regulatory obligations.

Retention periods are determined based on legal, regulatory, contractual, operational, and risk management requirements.

Once no longer required, data is securely destroyed, anonymised, de-identified, consistent with the Privacy Policy.

DATA SECURITY MEASURES

The Company implements appropriate technical and organisational measures proportionate to the nature, scope, context, and risk of processing activities, including:

- role based access controls
- Secure digital storage, encryption, and system protections
- Periodic review of data handling practices
- Employee awareness

Third-party service providers are subject to appropriate due diligence and contractual data protection and confidentiality obligations.

While the Company takes reasonable steps to protect data, absolute security cannot be guaranteed.

DATA SHARING & CROSS-BORDER TRANSFERS

Data may be shared with:

- Trusted third-party service providers under written agreements
- Affiliated entities for legitimate business purposes

Where data is transferred across borders, the Company ensures:

- Appropriate safeguards are in place. (e.g., Standard Contractual Clauses, binding corporate rules, or other legal mechanisms)
- Compliance with all local and international data protection laws

DATA BREACH RESPONSE

In the event of a data security incident, the Company will:

- Investigate and mitigate the impact promptly
- Notify affected individuals as required by applicable law
- Notify regulatory authorities within applicable legal timelines (e.g., GDPR within 72 hours)
- Document the breach and response actions

ACCESS, CORRECTION & INQUIRIES

Individuals whose personal information is collected may:

- Request access or correction
- Request erasure (right to be forgotten)
- Restrict or object to processing
- Request data portability

All requests must be submitted in accordance with the Privacy Policy. Identity verification may be required.

POLICY REVIEW

The Company reserves the right to review and update this policy periodically to ensure it remains current, effective, and aligned with legislative requirements, business needs, and best practice standards.

Signed

Duncan Scott	Grant Jones	Chris Henderson