Oracle
Special Metals Ltd

Confidential Information Protection Policy

Purpose

This policy establishes guidelines and controls to protect confidential and sensitive information belonging to Oracle Special Metals Ltd from unauthorised access, disclosure, alteration, or destruction.

Scope

This policy applies to:

- All employees, contractors, consultants, and third parties
- All information systems, devices, and storage media
- All forms of information (digital, physical, verbal)

Definitions

- **Confidential Information:** Non-public information that could harm the company if disclosed (e.g., financial data, trade secrets, customer data).
- **Sensitive Information:** Information requiring protection due to legal, regulatory, or business impact.
- **Public Information:** Information approved for public release.

Information Classification

All information must be classified into one of the following categories:

- Public
- Internal Use Only
- Confidential
- Highly Confidential

Data owners are responsible for assigning and reviewing classifications according to company management.

Access Control

- Access to confidential information must follow the **principle of least privilege**.
- Role-based access control (RBAC) must be implemented.
- Multi-factor authentication (MFA) is needed for sensitive systems.
- Access rights must be reviewed quarterly.

Data Handling and Storage

Oracle Special Metals Ltd Unit 2 Lennox Road, Basingstoke, RG22 4AP, United Kingdom
Telephone: 01256 975 005
Managing Directors: Rupert Gordon & Mark Glynn

Company Registered in England and Wales No: 13064279
VAT No: GB365548369

- Confidential data must be encrypted at rest and in transit.
- Physical documents must be stored in locked cabinets.
- Portable devices must use encryption and secure authentication.
- Data must not be stored on unauthorized personal devices.

Data Transmission

- Use secure communication channels
- Do not share confidential information via unsecured platforms.
- Verify recipient identity before sharing sensitive data.

Third-Party Access

- Conduct due diligence and risk assessments before granting access.
- Limit access strictly to required information.

Incident Management

- All suspected or actual data breaches must be reported immediately.
- Incidents must be logged and investigated.
- Appropriate corrective and preventive actions must be implemented.

Employee Responsibilities

- Always protect confidential information.
- Follow company security procedures.
- Report suspicious activities immediately.
- Participate in mandatory security training.

Data Retention and Disposal

- Retain data only as long as necessary.
- Dispose of data securely (e.g., shredding, secure deletion).
- Follow legal and regulatory retention requirements.

Monitoring and Compliance

- Systems and access may be monitored for security compliance.
- Regular audits must be conducted.

- Non-compliance may result in disciplinary action.

Policy Review

This policy must be reviewed annually or upon significant changes to business or regulatory requirements.

Enforcement

Violations of this policy may result in disciplinary action, including termination and legal consequences.

30/11/2023