

	DATA PROTECTION POLICY			Page 1 of 3
	Doc. No	JO-IS-POL-004	Rev	

DATA PROTECTION POLICY

1. Purpose

The purpose of this policy is to define JERA's approach to data protection, ensuring the privacy, security, and compliance of personal and business-critical data. This policy establishes the required measures to prevent unauthorized access, disclosure, or modification of data, aligning with ISO 27001 and global data protection regulations such as GDPR.

2. Scope

This policy applies to all JERA employees, contractors, and third-party service providers who process, store, or transmit data within JERA's IT infrastructure, including Microsoft 365, SharePoint, cloud services, and on-premises systems.

3. Data Protection Principles

JERA adheres to the following data protection principles:

- **Lawfulness, Fairness, and Transparency:** Data must be processed legally and transparently.
- **Purpose Limitation:** Data must be collected for specified, explicit, and legitimate purposes.
- **Data Minimization:** Only necessary data should be collected and processed.
- **Accuracy:** Data must be kept accurate and up-to-date.
- **Storage Limitation:** Data should only be retained for as long as necessary.
- **Integrity and Confidentiality:** Data must be protected against unauthorized access and breaches.

4. Data Classification and Handling

4.1. Data Classification Levels

JERA classifies data into the following categories:

- **Public:** Data that can be openly shared.
- **Internal:** Data intended for internal use only.
- **Confidential:** Business-sensitive data requiring controlled access.
- **Restricted:** Highly sensitive data with strict access controls.

4.2. Data Handling Guidelines

- Confidential and restricted data must be encrypted both in transit and at rest.
- Data access must be role-based and restricted to authorized users only.
- Employees must follow secure data handling procedures when sharing or transferring data.

 JERA <small>An O&M EPC Service Company</small>	DATA PROTECTION POLICY			Page 2 of 3
	Doc. No	JO-IS-POL-004	Rev	

5. Data Storage and Retention

- Data retention periods must comply with regulatory requirements and business needs.
- Personal and sensitive data must be securely deleted when no longer required.
- Backup and recovery procedures must be in place to prevent data loss.

6. Data Subject Rights

Under GDPR and other applicable regulations, JERA acknowledges the following data subject rights:

- Right to access personal data.
- Right to rectification of inaccurate data.
- Right to erasure (right to be forgotten).
- Right to restrict or object to processing.
- Right to data portability.

7. Data Breach Management

7.1. Incident Detection and Reporting

- Any suspected data breach must be reported to the IT Security Team immediately.
- Security logs must be continuously monitored for potential breaches.

7.2. Breach Response Procedures

- The Incident Response Procedure (JO-IS-PRO-003) must be followed in case of a data breach.
- Affected individuals and regulatory authorities must be notified as per legal requirements.

8. Compliance and Monitoring

- Data protection audits must be conducted annually.
- Employees must complete mandatory data protection training.
- Non-compliance with this policy may result in disciplinary actions, including termination.

9. Review and Maintenance

This policy will be reviewed annually or when significant changes occur in the business or regulatory landscape to ensure ongoing compliance.

10. Reference Documents

The following documents are related to this policy and should be referred to for further details:

DOCUMENT	DOCUMENT TITLE
JO-IS-POL-001	Information Security Policy
JO-IS-PRO-001	Information Security Procedure
JO-IS-MAN-001	Information Security Management Manual
JO-IS-POL-002	Access Control Policy
JO-IS-POL-003	Cybersecurity Policy
JO-IS-POL-004	Data Protection Policy
JO-IS-PRO-002	Risk Management Procedure
JO-IS-PRO-003	Incident Response Procedure
JO-IS-PRO-004	Information Security Training Program

11. Approval

Signed on behalf of JERA,

Name:	Stephen Lumsley
Title:	CEO, JERA
Signature:	
Date:	01-01-2025