Ooredoo Oman

Data Protection Policy

External Version

Classification: **Public**

1. Purpose

The purpose of this Data Protection Policy is to outline how the Company protects information against unauthorized access, loss, misuse, alteration, or destruction. This policy focuses on technical and organizational security measures implemented to safeguard data processed by the Company.

2. Applicability

This policy applies to all information assets handled by the Company, including data stored, processed, or transmitted through company-owned systems, networks, applications, and cloud services.

3. Definitions

In the application of this policy, the following words and expressions have the meanings hereby assigned to them, unless the context otherwise requires:

Access	Refers to permission or ability to obtain or use an information resource.
Company	Ooredoo Oman

Responsibilities

4. Data Protection Principles

The Company is committed to:

- Protecting data against unauthorized or unlawful access
- Maintaining data integrity and accuracy
- Ensuring data availability for authorized business use
- Preventing accidental loss, damage, or disclosure

5. Security Measures

The Company implements appropriate security controls, including but not limited to:

- Access control and authentication mechanisms
- Encryption of data in transit and at rest where applicable
- Network and system security monitoring
- Secure configuration and regular patching of systems
- Logging and monitoring of security-relevant events

6. Access Control

Access to systems and data is granted strictly on a need-to-know and least-privilege basis. User access rights are reviewed periodically and promptly revoked when no longer required.

7. Incident Management

The Company maintains procedures to detect, respond to, and manage information security incidents. Any suspected or confirmed security incidents are investigated and handled in accordance with internal incident response processes.

8. Third-Party Protection

Where third parties process or access company data, appropriate security requirements are enforced through contractual and technical controls to ensure an adequate level of data protection.

9. Employee Responsibilities

All employees and authorized users are required to comply with the Company's information security policies and are responsible for protecting information assets against unauthorized access or misuse.

10. Policy Review

This policy is reviewed periodically and updated as necessary to reflect changes in technology, threats, and business operations.