Ooredoo Oman

Information Security Policy – External Version

Classification: **Public**

1- Purpose:

The purpose of this information security policy is to provide management with directives for information security policies, standards, procedures and controls that shall govern, manage, and operate information security in Ooredoo Oman. The objective of this policy is to ensure:

1. A robust and a homogenous Information Security Framework and operations across Ooredoo Oman.
2. All services and their supporting infrastructures are adequately protected against the various security threats.
3. Services and infrastructure resilience to security incidents and attacks.
4. Information security compliance to information security policies, standards, applicable laws and regulatory requirements.
5. A uniform cyber security workforce skills and capabilities in Ooredoo Oman.
6. A security-conscious culture across Ooredoo Oman.

2- Policy Applicability:

This policy applies to all Ooredoo Oman's infrastructure used to deliver Ooredoo Oman's products and services to Customers including all internal Users who have access to the Company's information including, but not limited to, Company employees, consultants, contractors, sub-contractors, vendors, third parties, suppliers and their employees and anyone who has been provided access to information or Information Assets owned by Ooredoo Oman or operated by it.

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.

Company	Omani Qatari Telecommunications Company SAOG (the "Company" or "Ooredoo Oman")
Customers	Consumer or business consumers who have subscribed to or purchased products or services from Ooredoo Oman.
Endpoint Devices	Refers to Ooredoo Oman's owned or managed desktop computers, laptops, smart phones, tablets and other devices.
Information Asset	Refers to tangible and intangible data that has value to the Company including, but not limited to, data relating or connected to Ooredoo Oman and data entrusted to it by another party. This includes data in electronic and physical forms including, but not limited to, documents, emails facsimiles, envelops and data resulting from the use of applications.
Information Security Framework	Consists of an IS policy, supporting procedures, guidelines and standards an organization follows to manage its cybersecurity risk and to ensure Ooredoo Oman's Information Assets and information processing facilities are adequately protected.
IS	Information Security
Personal Data	Data that makes a natural person identifiable directly or indirectly by reference to one or more identifiers such as a name, civil number, electronic identifiers data, spatial data, or without reference to one or more factors related to genetic, physical, mental, psychological, social or cultural identity or economic.

Sensitive Personal Data	Personal Data related to the racial origin, children, health condition, physical or psychological, religion, marital relations, or criminal actions, or any other Personal Data, identified by the relevant local regulator, which it determines may cause serious damages to the Individual if misused or disclosed.
Staff/User(s)	Refers to all the Company workforce including, but not limited to, employees, consultants, contractors, sub-contractors, vendors, suppliers and their employees any third parties who have been provided access to information or Information Assets owned by the Company or operated by it.
Minimum Baseline Security Standards	Refers to list of minimum security requirements needed which should be implemented in organizations' information processing facilities, systems, application, etc. to ensure its confidentiality, integrity and availability.
Top Secret	This classification level needs to protect information assets, the breach of which can adversely affect Ooredoo Oman's reputations, finances or its market competitiveness. For example: Financial reports, Proprietary information, Future product plans, accounting data, etc.
Confidential	This classification level needs to protect information assets, the breach of which can expose Ooredoo Oman's sensitive information like customer or personal information. For example: NDA with client and vendors, salaries and personal data, etc.
Internal	This classification level needs to protect information assets, the breach of which can adversely affect Ooredoo Oman's internal procedures, disrupting routines and result in degraded productivity of employees or delayed delivery of products into the markets. For example: Standard Operation Procedure, etc.
Public	This classification level is for those information assets that can be shared with general public without any restrictions. For example: Product Brochures , Newsletters, Reports required by regulatory authorities, etc.
Disaster Recovery Plan (DRP)	A disaster recovery plan (DR or DRP) is a formal document created by an organization that contains detailed instructions on how to respond to unplanned incidents such as natural disasters, power outages, cyber-attacks and any other disruptive events.

4- Cybersecurity Governance:

- Ooredoo Oman shall be committed to secure its products and services and deliver them to its Customer in a secure manner.
- Ooredoo Oman shall be committed to establish, implement, manage, monitor and continuously improve a consistent and reliable information security practices in Ooredoo Oman to ensure protection of Information Assets, and to allow access, use and disclosure of information in accordance with the applicable security policies, standards, laws and regulations.
- Duties and areas of responsibilities of employees shall be adequately segregated to reduce the opportunities for unauthorized or unintentional modification or misuse of the Information Assets.
- Security requirements shall be identified and reviewed across all phases of any project.
- Ooredoo Oman shall be committed to continuously develop, implement and maintain information security awareness and training program for all users to ensure understanding of Ooredoo Oman's information security policies and the changing cyber security threats.
- Ooredoo Oman shall publish practical materials that educate Customers on how to protect themselves from cybersecurity risks relevant to the Company's products and services.

5- Endpoint Security:

- Ooredoo Oman shall establish and deploy frameworks and technologies to secure all its Endpoint Devices from unauthorized access and use, malware infection and data leakage.
- Ooredoo Oman shall ensure adequate protection of all its Information Assets throughout the phases of the asset's life cycle.
- Minimum Baseline Security Standards (MBSS) shall be established, implemented and enforced within Ooredoo Oman.

6- Telecommunication and Enterprise Network Security:

- Ooredoo Oman shall ensure adequate security controls, countermeasures and safeguards during planning, design, implementation and testing of its telecommunication and enterprise network infrastructures.
- Ooredoo Oman shall define, implement, maintain and continuously improve security policies, standards, procedures, guidelines and security controls for the various service models it hosts.

7- Data Privacy and Data Protection:

- Ooredoo Oman shall be committed to comply with all applicable data privacy and protection laws and regulations.
- Ooredoo Oman shall define, establish, implement and maintain a data privacy framework and the associated security controls to protect the privacy, confidentiality and integrity of Personal Data and Sensitive Personal Data of its Staff, Customers and business partners in accordance with applicable laws and regulations.
- Ooredoo Oman shall be committed to ensure Personal Data and Sensitive Personal Data are identified, maintained, transferred, stored, processed and disposed in a secure manner by implementing adequate technical and administrative security controls in accordance with applicable laws and regulations.
- Ooredoo Oman shall ensure that its workforce is fully aware of data privacy and protection requirements during collection, usage, transfer, retention and disposal in accordance with applicable laws and regulations.
- Ooredoo Oman shall define, implement and maintain information security policies and standards for information classification, labelling and handling (i.e., Public, Internal, Confidential and Top Secret) to avoid information leakage and unauthorized access.
- Ooredoo Oman shall plan, design, implement, deploy, maintain and continuously improve the appropriate data security and protection controls that are proportionate to the information classification.

8- Cryptography:

- Ooredoo Oman shall establish, implement and maintain an encryption management framework to protect confidential and sensitive data which Ooredoo Oman receives, stores, manages, processes and transmits through Ooredoo Oman's network in accordance the Personal Data Protection Law issued by Royal Decree 6/2022 (and its amendments) and any other applicable laws and regulations.
- Ooredoo Oman shall establish, implement and maintain cryptographic key management guidelines for secure key generation, ownership, usage, distribution, storage, backup and recovery, and revocation to protect the keys throughout their lifecycle.

9- Physical and Environment Security:

- Ooredoo Oman shall establish, implement and maintain physical security framework to protect Ooredoo's Information Assets and facilities hosting information against unauthorized access, physical and environmental damage.

10- Application Security:

- Ooredoo Oman shall establish, implement and maintain application security policies, standards, procedures guidelines and tools for application security including, acquisition, development, and maintenance of applications and information systems.

11- Application Security:

- Ooredoo Oman shall establish, implement and maintain application security policies, standards, procedures guidelines and tools for application security including, acquisition, development, and maintenance of applications and information systems.

12- Third Party Relationships:

- Ooredoo Oman shall establish, implement and maintain third party security policy and security compliance monitoring process to ensure third party's adherence to Ooredoo Oman's information security policies, standards and procedures.
- Ooredoo Oman shall regularly conduct an information security risk assessment of its existing and potential third parties.

13- Security Monitoring and Operations:

- Ooredoo Oman shall define, plan, design, implement, monitor, maintain and continuously improve security monitoring and operations' framework and infrastructure (people, process and technology) to ensure 24/7 monitoring and timely detection of information security incidents.

- Ooredoo Oman shall plan, design, implement and monitor employee access to Ooredoo systems and applications.
- Ooredoo Oman shall define a mechanism through which security researchers or Customers can submit vulnerabilities they discover within Ooredoo Oman’s applications and services.
- Ooredoo Oman shall ensure that Users are able to share any vulnerabilities they discover within Ooredoo Oman’s applications and services through designated procedures.

14- Business Continuity and Disaster Recovery:

- Ooredoo Oman shall be committed to accommodate security operations, monitoring and incident response as part of the Company’s business continuity plans for all critical business processes, crisis communication plan and IT disaster recovery plan.