OOREDOO TUNISIE
INFORMATION SECURITY POLICY

1. Purpose

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

1. A robust and a homogenous Information Security Framework and operations across Ooredoo Tunisia.
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, national legal and regulatory requirements.
5. A uniform cyber security workforce skills and capabilities in Ooredoo Tunisia.
6. A security-conscious culture across Ooredoo Tunisia.

2. Applicability

This policy applies to all Ooredoo's infrastructure used to deliver Ooredoo's products and services to Customers including all internal users who have access to the company's information including Company employees, consultants, contractors, sub-contractors, vendors, suppliers and their employees and anyone who has been provided access to information or information assets owned by Ooredoo 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.

Asset Owner	Refers to a Department or person who is responsible for an asset in The Company and authorized to request, approve and terminate the provision of access to the Corporate's information or information processing device.
Customers	Customer or Business Consumers who have subscribed to or purchased products or services from Ooredoo Tunisia.
Data Processor	A natural or legal person who processes Personal Data for Ooredoo Tunisia.
Endpoint Devices	Refers to Ooredoo Tunisia owned or managed desktop computers, laptops, smart phones, tablets and other devices.

Individual	A natural person who's Personal Data is being processed.
Information Asset	Refers to tangible and intangible data that has value to The Company including data relating or connected to Ooredoo 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 Information Assets and information processing facilities are adequately protected.
IS	Information Security
Personal Data	Data as defined by the organic act number 2004-63 dated in 27 of July 2004. Data processed by Ooredoo, regardless of their origin or form or means, which can lead, directly or indirectly, to the identification of a person. .
Processing	Processing of personal data: the automatic processing as well as non automatic processing of personal data carried out by an individual or legal entity especially obtaining, recording, storage, organization, alteration, use, distribution, dissemination, destruction or consultation
Sensitive Personal Data	Personal Data related to the racial or genetic origin, children, health condition, physical or psychological, religion, political, philosophical and trade union opinions, or any data on the legal requirement to report to judicial, police and military authorities
Staff/User(s)	Refers to all the Company employees, consultants, contractors, sub-contractors, vendors, suppliers and their employees any third parties who has 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
Processing of personal data:	the automatic processing as well as non-automatic processing of personal data carried out by an individual or legal Processing entity especially obtaining, recording, storage, organization, alteration, use, distribution, dissemination, destruction or consultation

-

4. Cybersecurity Governance

4.1. Ooredoo Tunisia shall be committed to secure its products and services and deliver them to its customer in a secure manner.

4.2. Ooredoo Tunisia shall be committed to establish, implement, manage, monitor and continuously improve a consistent and reliable information security practices in Ooredoo Tunisia to ensure protection of information assets, and to allow access, use and disclosure of information in accordance with the appropriate security policies, standards, laws and regulations.

4.3. This Information Security policy shall be supported, at a minimum, by domain specific information security policies, standards, procedures and guidelines for the following domains:

1. Information Security Governance
2. Identity and Access Management
3. Network Security
4. Endpoint Security
5. Cloud Security
6. Application Security
7. Data Privacy and Data Protection
8. Change and Patch Management
9. Security Monitoring and Operations
10. Security Incident Management

4.4 An Information security steering committee (ISSC) consisting of representatives from the different business functions in the organization shall be established to facilitate the information security projects' and initiatives' deployment, implementation and maintenance of the information security framework(s). (Refer to Annex 1 for ISSC Charter)

4.5 The information security organization structure along with information security roles and responsibilities shall be developed, maintained and assigned at all levels to manage information security within Ooredoo Tunisia across all Business units and services and ensuring that the individuals understand them.

4.6 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.

4.7 Security requirements shall be identified and reviewed across all phases of a project; from initiation, planning, execution to project closing.

4.8 Ooredoo Tunisia shall be committed to establish, implement and maintain Information Security risk management process to manage and mitigate risks and reduce potential impacts on Information Assets to an acceptable level.

4.9. Ooredoo Tunisia shall ensure that internal and external security assessments and audits are conducted for its products and services.

4.10 Ooredoo Tunisia shall be committed to continuously develop, implement and maintain information security awareness and training program for all Users to ensure understanding of Ooredoo information security policies and the changing cyber security threats.

4.11 Information Security requirements shall be identified and reviewed across all phases of a project; from initiation, planning, execution to project closing.

4.12. Information security roles and responsibilities shall be defined and appropriately enforced as part of the Human Resource's Code of Conduct and Non-Disclosure Agreements with Ooredoo Tunisia's workforce and third parties.

4.13. Ooredoo Tunisia 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

5.1 Ooredoo Tunisia shall establish and deploy frameworks and technologies to secure all its Endpoint Devices from unauthorized access and use, malware infection and data leakage.

5.2 An Acceptable Use policy (AUP) shall be established to provide rules that protect both Ooredoo Tunisia and its Staff from potential liability, reduce information security risks, promote good practice and ensure that all Staff are aware of their roles, responsibilities and obligations when using Ooredoo Information Assets.

5.3 Minimum Baseline Security Standards (MBSS) shall be established, implemented and enforced for Endpoint Devices' operating system, applications and network layers.

5.4 Ooredoo Tunisia shall ensure adequate protection of all its Information Assets throughout the phases of the Asset's life cycle.

5.5 Ooredoo Tunisia shall be committed to establish framework and technologies required to build Endpoint security program.

5.6 Ooredoo Tunisia shall be committed to establish, implement and maintain Asset management process to track asset inventory of Endpoint devices, to ensure Information assets are returned upon termination of User's contract and to ensure Information Assets are adequately protected during transit and all sensitive information stored on media are disposed securely.

6 Telecommunication and Enterprise Network Security

6.1 Ooredoo Tunisia shall ensure adequate security controls, countermeasures and safeguards during planning, design, implementation and testing of its Telecommunication and Enterprise network Infrastructures.

6.2 Ooredoo Tunisia shall establish, implement and maintain adequate frameworks and security tools for network access management, remote access management, network configuration management, communication security, information exchange/transfer and email security to protect from unauthorized network intrusions and risks of misuse and abuse.

6.3 Ooredoo Tunisia shall define, implement, maintain and continuously improve cloud security policies, standards, procedure and security controls for the various cloud service models it hosts or is subscribed to; Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (laaS).

7 Data Privacy and Data Protection

7.1 Ooredoo Tunisia shall be committed to comply with all applicable data privacy and protection laws and regulations.

7.2 Ooredoo Tunisia shall define, establish, implement and maintain a data privacy framework and the associated security controls to protect the privacy, confidentiality and integrity of Personal and Sensitive Personal Data of its staff, customers and business partners.

7.3 Ooredoo Tunisia 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.

7.4 Ooredoo Tunisia shall ensure that its workforce is fully aware of data privacy and protection requirements during collection, usage, transfer, retention, Processing and disposal.

7.5 Ooredoo Tunisia shall define Third Parties contractual obligations towards compliance with data privacy laws and regulations as applicable.

7.6 Ooredoo Tunisia shall ensure through the respective accountable Business Unit that Third Party processors of Personal Data and Sensitive Personal Data adhere to the aforementioned security controls through contractual obligations and ongoing Ooredoo Tunisia assessments of the Third Party compliance with the contractual obligations including obligations for the Third Party Processors to:

a. Advise Ooredoo Tunisia about any breach/violation to the security controls or any security risks threatening the Personal Data of Individuals, whatsoever, as soon as the Data Processor knows about the same;

b. Ensure that Personal Data is processed only for the legitimate purposes and immediately notify Ooredoo of any security breach or security risk of breach to Personal Data;

c. Ensure that the Data Processor's employees who process Personal Data have signed Ooredoo Tunisia compliant confidentiality and non-disclosure clauses and such NDA applies to customer information.

7.7 A Data protection framework and security controls shall be defined, planned, designed, implemented, maintained and continuously improved to adequate protect data based on

its classification, to track and monitor data movement, to dispose data securely and to ensure data's accuracy and availability when needed.

7.8 Ooredoo Tunisia shall define, implement and maintain information security policies and standards for information classification, labelling and handling (i.e., Public, Internal, Confidential and Restricted) to avoid information leakage and unauthorized access.

7.9 Ooredoo Tunisia shall plan, design, implement, deploy, maintain and continuously improve the appropriate data security and protection controls that are proportionate to the information classification.

8 Identity and Access Management

8.1 Ooredoo Tunisia shall establish an Identity and Access management (IAM) framework including IAM policy, Privilege Access Management (PAM), remote access management, password management, etc. and security tools to ensure a consistent governance, management and operations of User's Identity and Access management in Ooredoo during onboarding, transfer and off-boarding across systems and applications.

8.2 Ooredoo Tunisia shall establish processes and tools to monitor compliance and measure the effectiveness of Identity and Access Management implementation.

9 Cryptography

9.1 Ooredoo Tunisia shall establish, implement and maintain an encryption management framework to protect confidential and sensitive data which Ooredoo receives, stores, manages, processes and transmits through Ooredoo TUNISIA's network.

9.2 Ooredoo Tunisia 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.

10 Physical and environment security

10.1 Ooredoo Tunisia 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.

10.2 Ooredoo Tunisia shall enforce physical security administrative and technical controls to all its building facilities and sites and continuously monitor their compliance and measure their effectiveness to mitigate physical security risks.

11 Application Security

11.1 Ooredoo Tunisia 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.

11.2 Ooredoo Tunisia shall ensure that security requirements are developed, considered and implemented alongside functional and technical requirements at all phases of project planning and implementation including System Development Life Cycle (SDLC).

11.3 Secure development standards, procedures and guidelines shall be followed for all systems and applications to build a secure service, secure coding, secure architecture within development, testing and production environments.

11.4 Ooredoo Tunisia shall ensure that all new applications, systems that are acquired, developed or enhanced undergo system acceptance testing and security assessments to identify and close security gaps and vulnerabilities before their launch.

12 Third party relationships

12.1 Ooredoo Tunisia shall establish, implement and maintain third party security policy and security compliance monitoring process to ensure third party's adherence to Ooredoo's information security policies, standards and procedures.

12.2 Ooredoo Tunisia shall ensure agreements and contracts with third parties and their subcontractors include the obligation to follow Ooredoo's information security policies, standards, procedures and SLAs.

12.3 Ooredoo Tunisia shall define Key Performance Indicators (KPIs) and regularly perform or review security assessments for its third party systems or outsourced services.

12.4 Ooredoo Tunisia shall regularly conduct an information security risk assessment of its existing and potential third parties.

13. Change and Patch Management

13.1. Ooredoo Tunisia shall document, implement, and enforce Change and Patch Management framework and service level agreements (SLAs) for all changes to information processing facilities, systems, applications and processes to ensure that all changes and patches are timely and securely deployed to minimize the impact on the system's confidentiality, integrity or availability.

13.2. Ooredoo Tunisia shall establish a process to ensure that changes, configurations and patch deployments are conducted in a planned, managed and secure manor.

14. Security Monitoring and Operations

14.1 Ooredoo Tunisia 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.

14.2 Ooredoo shall plan, design, implement and monitor employee access to Ooredoo systems and applications.

14.3 Ooredoo shall plan, design, implement, review, maintain and continuously improve vulnerability management, penetration testing, threat intelligence and threat hunting technologies, processes and competencies necessary to identify, classify, remediate and mitigate security vulnerabilities.

14.4 Ooredoo shall address security vulnerabilities when they are discovered at a defined timeframe to review reports and provide fixes as applicable.

14.5 Ooredoo shall clearly disclose what, if any, security modifications it has made to a mobile operating system and effect of such modification updates sent to Customers.

14.6 Ooredoo shall define a mechanism through which security researchers or customers can submit vulnerabilities they discover within Ooredoo applications and services.

14.7 Ooredoo shall ensure that people are able to share any vulnerabilities they discover within Ooredoo applications and services through designated procedures.

14.8 Ooredoo shall be committed not to pursue legal action against researchers who report vulnerabilities within the terms of The Company's vulnerability reporting mechanism.

15. **Incident Handling and Response**

15.1 Ooredoo Tunisia shall be committed to appropriately handle and respond to cyber security incidents as per well-recognized security standards and best practices in terms of people, process and technology.

15.2 An Incident handling and response policy(s) shall be defined and supported by security incident handling and response plan, process, procedures and controls to detect, report, respond, contain, eradicate and recover from cybersecurity incidents and attacks.

15.3 Ooredoo Tunisia shall perform table-top and cyber security drill exercises annually for security incident handling and response to test and assess the incident response team's preparedness and capabilities to detect, report, respond, contain, eradicate and recover from cybersecurity incidents and attacks.

15.4 Ooredoo Tunisia shall establish a digital forensics investigation framework to ensure the integrity of data during identification, collection, examination, and analysis of data.

15.5 Ooredoo shall define and publish its processes for responding to data breaches and policies for notifying affected Customers.

15.6 Ooredoo shall notify the CEO and other relevant entities without undue delay when a data breach occurs and any material incidents to the Board.

15.7 Ooredoo shall define the necessary steps it would take to address the impact of a data breach on its Customers.

16. **Business Continuity and Disaster Recovery**

16.1 Ooredoo Tunisia 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.

16.2 Ooredoo Tunisia shall periodically carry out a comprehensive business impact analysis to assess the criticality of services, business functions, processes, infrastructure and technologies and associated resource requirements (i.e., infrastructure, technology, people, etc.) to ensure operational resilience and continuity of operations during and after disruption.

17. **Information Security Compliance Monitoring**

17.1. Ooredoo Tunisia shall be committed to establish, implement and maintain an information security compliance monitoring process to ensure compliance with information security polices, applicable national cybersecurity laws, regulations and applicable international security standards.

17.2. Ooredoo Tunisia shall be committed to perform audit review, technical security assessment (i.e., penetration testing and vulnerability assessment) and compliance reviews at planned intervals or when a significant change occur to ensure security control effectiveness to mitigate the respective cybersecurity risks and achieve information security objectives. The frequency of penetration testing and vulnerability assessment shall be defined by Ooredoo Tunisia Information Security team and any critical findings shall be reported to the CEO and the Board.

18. Policy Enforcement

18.1. All Ooredoo Tunisia employees, consultants, contractors, sub-contractors, vendors, suppliers and their employees are independently responsible for reading, understanding and following this policy.

18.2. Non-compliances with this Information Security Policy shall be dealt in accordance with Ooredoo HR disciplinary policies, procedures and contractual obligations.

19. Policy Amendment and exception

19.1. This policy supersedes all previous releases (policy, circular, memos, instructions or any other form) on its subject-matter.

19.2. Any change to the provisions of this policy shall be preliminarily reviewed and recommended by the Audit & Risk Management Committee (ARC) and finally approved by Ooredoo TUNISIA's Board of Directors.

20. References

1. ISO 27001:2013 International standard for Information Security Management Systems (ISMS)
2. Organic act 11 ^{0}2004-63 of July 27th 2004 on the protection of personal data
3. Decree No. 2007-3004 of November 27, 2007 setting the conditions and procedures for declaration and authorization for the processing of personal data
4. Decree No. 2013-4506 of November 6, 2013 on the creation of the technical agency for telecommunications and setting its administrative and financial organization and the terms of its operation

5. Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data Strasbourg, 28.1.1981
6. African Union Convention On Cyber Security And Protection Of Personal Data Malabo, June 27, 2014
7. Ranking Digital Rights (RDR) — RDR work with companies as well as advocates, researchers, investors, and policymakers to establish and advance Global Standards for corporate accountability.