This policy is an extract of the original Ooredoo Information Security Policy (POL/2018/12)

Ooredoo Information Security Policy – External Version

سياسة أمن المعلومات في Ooredoo - النسخة الخارجية

1.	PURPOSE	الغرض	1.
1.1.	The purpose of this information security policy is to provide Ooredoo's Top Management's direction and support through information security and data protection policies, standards, procedures and controls that shall govern, manage, and operate information security in Ooredoo ensuring: 1. A robust and a homogenous Information Security Framework and operations across Ooredoo. 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.	تهدف هذه السياسة الى توفير دعم وتوجه الإدارة العليا في Ooredoo من خلال سياسات، ومعايير، وإجراءات وضوابط أمن المعلومات وحماية البيانات التي تضبط وتدير وتشغل أمن المعلومات في Ooredoo والتي تضمن: 1 . إطار عمل وعمليات أمن معلومات قوية ومتجانسة في Ooredoo. 2 . حماية كافة الخدمات والبنية التحتية الداعمة بشكل كافٍ من التهديدات الأمنية المختلفة. 3 . مرونة الخدمات والبنية التحتية أمام الحوادث والهجمات الأمنية. 4 . امتثال أمن المعلومات لسياسات ومعايير أمن المعلومات والمتطلبات القانونية والتنظيمية الوطنية. 5 . مهارات وقدرات موحدة في مجال الأمن السيبراني في Ooredoo	1.1

	5. A uniform cyber security workforce skills and capabilities in Ooredoo. 6. A security-conscious culture across Ooredoo.	6 . وجود بيئة واعية و مدركه لأمن المعلومات في Ooredoo.	
2.	**SCOPE**	**المجال**	**2.**
2.1.	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.	تنطبق هذه السياسة على كافة أنحاء البنى التحتية المستخدمة لتوفير منتجات وخدمات Ooredoo للعملاء، وتشمل كافة المستخدمين المسموح لهم باستخدام معلومات الشركة بما في ذلك موظفي الشركة والاستشاريين والمتعاقدين والمتعاقدين من الباطن والموردين والموزعين و موظفيهم و أي شخص تم تزويده بصلاحية الوصول إلى المعلومات أو أصول المعلومات التي تمتلكها Ooredoo أو تدار بواسطتها.	2.1
3.	**EXCEPTIONS**	**الاستثناءات**	**3.**
3.1.	None	لا يوجد	3.1
4.	**DEFINITIONS**	**التعريفات**	**4.**
In applying the statements of this policy, the following words and expressions have the meanings hereby assigned to them, unless the context otherwise states.		في تطبيق أحكام هذه السياسة، ستكون للكلمات والعبارات التالية المعاني الموضحة قرين كل منها، ما لم يقتض السياق معنى آخر.	

4.1.	**The Company / Ooredoo** Ooredoo Q.P.S.C. a Qatari Public Shareholding Company (Ooredoo Qatar)	**الشركة / Ooredoo** Ooredoo ش.م.ق.ع.، شركة مساهمة قطرية عامة (Ooredoo قطر).	4.1
4.2.	**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.	**المسؤول عن الأصل** الإدارة أو الشخص المسؤول عن أصل في الشركة والمفوض بطلب واعتماد وإلغاء منح الوصول إلى معلومات الشركة أو جهاز معالجة المعلومات.	4.2
4.3.	**Customers** Consumer or Business Consumers who have subscribed to or purchased products or services from Ooredoo.	**العملاء** وهم العملاء من الأفراد أو الشركات المشتركون أو الذين قاموا بشراء منتجات أو خدمات من Ooredoo.	4.3
4.4.	**Third Party Data Processor** A natural or legal person who processes Personal Data for Ooredoo.	**معالج بيانات الطرف الثالث** وهو الشخص الطبيعي أو القانوني الذي يقوم بمعالجة البيانات الشخصية لصالح Ooredoo.	4.4
4.5.	**Endpoint Devices** Refers to Ooredoo owned or managed desktop computers, laptops, smart phones, tablets and other devices.	**أجهزة المستخدمين** تشير إلى أجهزة الكمبيوتر الشخصية والمحمولة والهواتف الذكية والأجهزة اللوحية وغيرها من الأجهزة التي تمتلكها أو تديرها Ooredoo.	4.5
4.6.	**Individual** A natural person whose Personal Data is being processed.	**الفرد** وهو الشخص الطبيعي الذي تتم معالجة بياناته الشخصية.	4.6

4.7.	**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.	**الأصل المعلوماتي** ويشـــير إلى البيـانـات الملموســـة وغير الملموســـة والتي تمتلك قيمة بالنســـبة للشـــركة، بما في ذلك البيانات المتعلقة أو المتصـلة بـــــ Ooredoo والبيانات الموكلة إليها من طرف آخر. ويتضـــمن هذا البيانات بأشكالها الالكترونية والمادية، بما في ذلك على سبيل المثال لا الحصر الوثائق ورسائل البريـد الـالكتروني والفـاكس والمظـاريف والبيانات الناتجة عن استخدام التطبيقات.	4.7
4.8.	**Information Security Framework** Consists of an information security policy, supporting procedures, guidelines and standards The Company follows to manage its cybersecurity risk and to ensure Ooredoo Information Assets and information processing facilities are adequately protected.	**إطار عمل أمن المعلومات** يتكون من ســـيـاســـة أمن المعلومـات والإجراءات والتوجيهات والمعايير الداعمة التي تتبعها الشـــركة لإدارة مخاطر الأمن السـيبراني ولضـمان حماية أصـول معلومات Ooredoo ومرافق معـالجـة المعلومـات بشكل كافٍ.	4.8
4.9.	**IS** Information Security.	**IS** أمن المعلومات	4.9
4.10.	**Personal Data** Data processed by or on behalf of Ooredoo, which belongs to and/or is about an Individual who has a verified identity, or who can be reasonably verified through such data by combining such data with any other data.	**البيانات الشخصية** البيـانـات التي تتم معـالجتهـا من قبـل Ooredoo أو بـالنيـابـة عنهـا والتي تنتمي إلى و/ أو تكون حول شـــخص لـه هويـة محددة، أو يمكن التحقق بشـــكل معقول	4.10

		منه من خلال تلك البيانات أو الجمع بين تلك البيانات وغيرها من البيانات.	
4.11.	**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 MCIT, which it determines may cause serious damages to the Individual if misused or disclosed.	**البيانات الشخصية الحساسة** وهي البيانات الشخصية المتعلقة بالأصل العرقي أو الأطفال أو الحالة الصحية أو الوضع الجسدي أو النفسي أو الدين أو العلاقات العائلية أو الجنايات أو أي بيانات شخصية أخرى، تحددها وزارة الاتصالات وتكنولوجيا المعلومات، والتي قد تسبب أضرار خطيرة على الفرد في حال سوء استخدامها أو الإفصاح عنها	4.11
4.12.	**MCIT** Ministry of Communications and Information Technology.	**MCIT** وزارة الاتصالات وتكنولوجيا المعلومات	4.12
4.13.	**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.	**الموظف/ المستخدم (المستخدمون)** تشير إلى موظفي الشركة والاستشاريين والمتعاقدين معها والمتعاقدين من الباطن والموردين والموزعين وموظفيهم وأي طرف ثالث تم منحه ميزة الوصول إلى المعلومات أو أصول المعلومات التي تمتلكها أو تديرها الشركة.	4.13
4.14.	**Minimum Baseline Security Standards** Refers to list of minimum security requirements needed which should be implemented in Company's Information processing facilities, systems,	**الحد الأدنى للمعايير الأمنية** يشير إلى قائمة الحد الأدنى من المتطلبات الأمنية اللازمة والتي يجب تنفيذها في أجهزة وأنظمة وتطبيقات معالجة معلومات	4.14

	application, etc. to ensure its confidentiality, integrity and availability.	الشركة وغيرها، وذلك لضمان سريتها وسلامتها وتوفرها.	
4.15.	**Corporate Information Security (CIS)** The Corporate Information Security Department within the CEO Office of Ooredoo Qatar.	**إدارة أمن معلومات الشركة (CIS)** إدارة أمن معلومات الشركة التابعة لمكتب الرئيس التنفيذي في Ooredoo قطر.	4.15
4.16.	**Business Units** Refers to Ooredoo Business Units such as Technology, Commercial, CEO Office…etc.	**وحدات العمل** وتشير إلى وحدات العمل مثل التكنولوجيا، والوحدة التجارية، وحدة مكتب الرئيس التنفيذي...الخ.	4.16
5.	**Policy Statement**	**بيان السياسة**	**5.**
5.1.	**Cybersecurity Governance**	**حوكمة الأمن السيبراني**	5.1
5.1.1.	Ooredoo shall be committed to secure its products and services and deliver them to its Customers in a secure manner.	تلتزم Ooredoo بتأمين منتجاتها وخدماتها وتوفيرها إلى عملائها بأسلوب آمن.	5.1.1
5.1.2.	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 and across all Business Units and services and ensuring that the Staff understand them.	يجب وضع هيكلة أمن المعلومات مع أدوار ومسؤوليات أمن المعلومات والحفاظ عليها وتخصيصها على كافة المستويات، من أجل إدارة أمن المعلومات في Ooredoo عبر كافة وحدات العمل والخدمات بما يضمن فهم الموظفين لها.	5.1.2
5.1.3.	Ooredoo shall be committed to adopt a systematic Information Security Management System (ISMS) that establishes, implements, operates, monitors, maintain, and continuously	تلتزم Ooredoo بتبني نظام إدارة أمن معلومات منظم يقوم بوضع وتنفيذ وتشغيل ومراقبة والمحافظة والتحسين المستمر لأمن المعلومات، وذلك لتحقيق	5.1.3

	improves information security to achieve business objectives based on risk assessment and acceptance levels to effectively treat and manage information security risks.	أهـداف الشـــركـة المعتمـدة على تقييم المخـاطر ومســـتويـات القبول للتعـامـل مع مخـاطر أمن المعلومـات وإدارتهـا بشـــكـل فعال.	
5.1.4.	The Corporate Information Security Department shall be responsible to define and maintain the information security policies, standards, procedures, guidelines and practices within Ooredoo Qatar.	يقع على عاتق إدارة أمن معلومات الشـركة مسؤولية تحديد سياسات ومعايير وإجراءات وتوجيهـات وممـارســـات أمن معلومـات الشركة في Ooredoo والحفاظ عليها.	5.1.4
5.1.5.	This Information Security policy shall be supported, at 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. Application Security 6. Cloud Security 7. Data Privacy and Data Protection 8. Change and Patch Management 9. Security Monitoring and Operations 10. Security Incident Management 11. Physical and Environmental Security	تكون سياسة أمن المعلومات مدعومة على الـأقـل، بســـيـاســـات ومعـايير وإجراءات وتوجيهات أمن المعلومات الخاصة بالمجالات التالية: 1 . حوكمة أمن المعلومات 2 . إدارة الهوية والوصول 3 . أمن الشبكة 4 . أمن أجهزة المستخدمين 5 . أمن التطبيقات 6 . الأمن السحابي (كلاود) 7 . خصوصية البيانات وحماية البيانات 8 . إدارة التغيير والتحديث 9 . المراقبة والعمليات الأمنية 10 . إدارة الحوادث الأمنية 11 . الأمن المادي والبيئي	5.1.5

5.1.6.	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). The committee to report to CEO directly.	يجب تأسيس لجنة تسيير أمن المعلومات مكونة من مختلف إدارات الشركة، وذلك لتسهيل تنفيذ مشاريع ومبادرات أمن المعلومات والحفاظ على إطار (أطر) عمل أمن المعلومات. وتتبع اللجنة الرئيس التنفيذي مباشرة.	5.1.6
5.1.7.	Information security roles and responsibilities shall be defined and appropriately enforced as part of the Human Resource's Code of Business Conduct and Ethics, and Non-Disclosure Agreements with Ooredoo Qatar's workforce and third parties.	يجب تحديد أدوار ومسؤوليات أمن المعلومات وتنفيذها بشكل مناسب كجزء من ميثاق الموارد البشرية للسلوك المهني وأخلاقيات العمل واتفاقيات عدم الإفصاح مع موظفي Ooredoo قطر والأطراف الثالثة.	5.1.7
5.1.8.	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.	يجب فصل واجبات ومسؤوليات الموظفين بشكل كاف، وذلك للتقليل من فرص التعديل غير المصرح به أو غير المقصود لأصول المعلومات أو إساءة استخدامها.	5.1.8
5.1.9.	Security requirements shall be identified and reviewed across all phases of a project; from initiation, planning, design, execution to project closure.	يجب تحديد ومراجعة المتطلبات الأمنية عبر جميع مراحل أي مشروع، من مرحلة البداية والتخطيط والتصميم والتنفيذ وصولاً إلى إغلاق المشروع.	5.1.9
5.1.10.	Ooredoo shall be committed to establish, implement and maintain Information	تلتزم Ooredoo بوضع وتنفيذ إجراءات إدارة مخاطر أمن المعلومات والمحافظة عليها،	5.1.10

	Security risk management process to manage and mitigate risks and reduce potential impacts on Information Assets to an acceptable level.	وذلك لإدارة المخاطر والتخفيف منها والتقليل من الآثار المحتملة على أصول المعلومات إلى مستوى مقبول.	
5.1.11.	Ooredoo shall ensure that internal and external security assessments and audits are conducted for its products, services and infrastructure to ensure effectiveness of and continual improvement to information security.	تضمن Ooredoo القيام بتقييمات وعمليات تدقيق أمنية داخلية وخارجية لمنتجاتها وخدماتها وبنيتها التحتية، وذلك لضمان الفعالية والتحسين المستمر لأمن المعلومات.	5.1.11
5.1.12.	Ooredoo 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.	تلتزم Ooredoo بالاستمرار في تطوير وتنفيذ برنامج التوعية والتدريب على أمن المعلومات لكافة المستخدمين والمحافظة عليه، وذلك لضمان فهم سياسات أمن معلومات Ooredoo وتهديدات الأمن السيبراني المتغيرة.	5.1.12
5.1.13.	Ooredoo shall publish practical materials that educate Customers on how to protect themselves from cybersecurity risks relevant to The Company's products and services.	تقوم Ooredoo بنشر المواد التطبيقية التي تثقف عملاءها حول كيفية حماية أنفسهم من مخاطر الأمن السيبراني المتعلقة بمنتجات وخدمات الشركة.	5.1.13
5.2.	**Endpoint Security**	**أمن أجهزة المستخدمين**	5.2
5.2.1.	Ooredoo shall establish and deploy frameworks and technologies to secure all its Endpoint Devices from unauthorized access and use, malware infection and data leakage.	تضع Ooredoo وتنشر أطر عمل وتقنيات لتأمين كافة أجهزة المستخدمين لديها من الوصول والاستخدام غير المصرح به ومن البرمجيات الخبيثة وتسريب البيانات.	5.2.1
5.2.2.	An Acceptable Use policy (AUP) shall be established to provide rules that protect	يتم وضع سياسة للاستخدام المقبول لتحديد القواعد التي تحمي كل من	5.2.2

	both Ooredoo and its Staff from potential liability, reduce information security risks, promote good practice and ensure that all Users are aware of their roles, responsibilities and obligations when using Ooredoo Information Assets.	Ooredoo وموظفيها من أي عواقب محتملة، والتقليل من مخاطر أمن المعلومات، وتعزيز الممارسات الجيدة، وضمان إدراك كافة المستخدمين لأدوارهم ومسؤولياتهم والتزاماتهم أثناء استخدام أصول المعلومات.	
5.2.3.	Minimum Baseline Security Standards (MBSS) shall be established, implemented and enforced for Endpoint Devices' operating system, applications and network layers.	يجب وضع الحد الأدنى من المعايير الأمنية وتنفيذه فيما يتعلق بنظام تشغيل أجهزة المستخدمين والتطبيقات ومستويات الشبكة.	5.2.3
5.2.4.	Ooredoo shall ensure adequate protection of all its Information Assets throughout the phases of the Asset's life cycle.	تضمن Ooredoo الحماية الكافية لكافة أصول المعلومات لديها طوال مراحل دورة حياة الأصل.	5.2.4
5.2.5.	Ooredoo shall be committed to establish, implement and maintain an 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.	تلتزم Ooredoo بوضع وتنفيذ إجراءات إدارة الأصول والمحافظة عليها لمتابعة مخزون الأصول من أجهزة المستخدمين، وذلك لضمان إعادة أصول المعلومات عند إنهاء عقد المستخدمين، ولضمان حماية أصول المعلومات بشكل كاف أثناء النقل والتخلص من كافة المعلومات الحساسة المخزنة على الوسائط بشكل آمن.	5.2.5
5.3.	**Telecommunication and Enterprise Network Security**	**أمن الاتصالات وشبكة الشركة**	5.3
5.3.1.	Ooredoo shall ensure adequate security controls, countermeasures and	تضمن Ooredoo وجود الضوابط الأمنية والإجراءات المضادة والإجراءات الوقائية	5.3.1

	safeguards during planning, design, implementation and testing of its Telecommunication and Enterprise network Infrastructures.	أثناء تخطيط وتصـميم وتنفيذ واختبار البنى التحتية للاتصالات وشبكة الشركة.	
5.3.2.	Ooredoo shall establish, implement and maintain adequate frameworks and security tools for network access management, remote access management, network security configuration management, communication security, information exchange/transfer and email security to protect from unauthorized network intrusions and risks of misuse and abuse.	تقوم Ooredoo بوضـــع وتنفيذ أطر العمل والأدوات الأمنية الكافية والمحافظة عليها لإدارة الوصول إلى الشبكة وإدارة الوصول عن بعد وإدارة التهيئة الأمنية للشـــبكة وأمن الاتصال وتبادل/ نقل المعلومات وأمن البريـد الـالكتروني، وذلـك للحمـايـة من اختراقات الشـبكة ومخاطر سـوء الاسـتخدام والانتهاك.	5.3.2
5.3.3.	Ooredoo 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 (IaaS).	تقوم Ooredoo بتحديد وتنفيذ وتحســين سـياسـات ومعايير إجراءات وضـوابط الأمن السحابي (الكلاود) باستمرار، وذلك لمختلف نماذج خدمات كلاود التي تســتضــيفها أو التي يتم الاشـــتراك بها: البرمجيات كخدمة (SaaS) والمنصـــة كخدمة (PaaS) والبنية التحتية كخدمة (IaaS).	5.3.3
5.4.	**Information Classification and Protection**	**تصنيف وحماية المعلومات**	5.4
5.4.1.	Ooredoo shall define, implement and maintain information security policies and standards for information classification, labelling and handling to avoid information leakage and unauthorized access.	تقوم Ooredoo بتحديد وتنفيذ والمحافظة على سياسات ومعايير أمن المعلومات فيما يتعلق بتصـــنيف المعلومات وتســـميتها والتعامل معها، وذلك لتجنب تســـريب المعلومات أو الوصول غير المصرح به إليها.	5.4.1

5.4.2.	Ooredoo shall plan, design, implement, deploy, maintain and continuously improve appropriate data protection controls that are proportionate to the information classification level.	تقوم Ooredoo بتخطيط وتصـــميم وتنفيذ ونشـــر والمحافظة على الضـــوابط الملائمة لحماية البيانات بما يتوافق مع مســـتوى تصنيف المعلومات وتسحينها باستمرار.	5.4.2
5.5.	**Identity and Access Management**	**إدارة الهوية والوصول**	5.5
5.5.1.	Ooredoo shall establish an Identity and Access management (IAM) framework including policies and standards for IAM, 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 staff onboarding, transfer and off-boarding across systems and applications.	تضـــع Ooredoo إطار عمل لإدارة الهوية و الوصـول، وتتضـمن سـياسـات ومعايير إدارة الهوية والوصـول، وإدارة الوصـول المتميز، وإدارة الوصـــول عن بعـد، وإدارة كلمـات المرور، وغيرهـا، بـالـإضـــافـة إلى الـأدوات الأمنية لضـــمان حوكمة وإدارة و عمليات ثابتة لإدارة الهوية والوصول في Ooredoo أثناء التحاق الموظفين بالعمل ونقلهم أو تركهم للعمل عبر الأنظمة والتطبيقات.	5.5.1
5.5.2.	Ooredoo shall establish processes and tools to monitor compliance and measure the effectiveness of Identity and Access Management implementation.	تضـــع Ooredoo الإجراءات والأدوات لمراقبة الالتزام وقياس فعالية تنفيذ إدارة الهوية والوصول.	5.5.2
5.6.	**Cryptography**	**التشفير**	5.6
5.6.1.	Ooredoo 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's network.	تقوم Ooredoo بوضـــع وتنفيذ إطار عمل لإدارة التشـــفير والمحافظة عليه، وذلك لحماية البيانات السـرية والحسـاسـة التي تتلقـاهـا Ooredoo وتخزنهـا وتـديرهـا وتعالجها وتنقلها عبر شبكة Ooredoo.	5.6.1

5.6.2.	Ooredoo shall establish, implement and maintain cryptographic key management standards for secure key generation, ownership, usage, distribution, storage, backup and recovery, and revocation to protect the keys throughout their lifecycle.	تقوم Ooredoo بوضع وتنفيذ معايير إدارة مفتاح التشفير لإنشاء مفتاح أمني وامتلاكه واستخدامه وتوزيعه وتخزينه والنسخ الاحتياطي والاسترجاع والإلغاء والمحافظة عليه، وذلك لحماية المفاتيح طوال مدة خدمتها.	5.6.2
5.7.	**Physical and Environmental security**	**الأمن المادي والبيئي**	5.7
5.7.1	Ooredoo 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.	تقوم Ooredoo بوضع وتنفيذ إطار عمل للأمن المادي والمحافظة عليه، وذلك لحماية أصول المعلومات في Ooredoo والمرافق التي تستضيف المعلومات ضد الوصول غير المصرح به والضرر المادي والبيئي.	5.7.1
5.7.2	Ooredoo 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.	تقوم Ooredoo بتنفيذ ضوابط إدارية وفنية للأمن المادي على كافة مرافق المباني والمواقع ومراقبة التزامها بشكل مستمر وقياس فعاليتها للتخفيف من مخاطر الأمن المادي.	5.7.2
5.8.	**Application Security**	**أمن التطبيقات**	5.8
5.8.1	Ooredoo shall establish, implement and maintain application security policies, standards, procedures, guidelines and tools including; acquisition, development, and maintenance of applications and information systems.	تقوم Ooredoo بوضع وتنفيذ سياسات ومعايير وإجراءات وتوجيهات وأدوات حماية التطبيقات والمحافظة عليها، بما في ذلك شراء وتطوير وصيانة التطبيقات ونظم المعلومات.	5.8.1

5.8.2	Ooredoo shall ensure that security requirements are developed, considered and implemented alongside functional and technical requirements at all phases of project planning and implementation of Software Development Life Cycle (SDLC).	تضمن Ooredoo وضع المتطلبات الأمنية ودراستها وتنفيذها إلى جانب المتطلبات التشغيلية والفنية في كافة مراحل مشروع تخطيط وتنفيذ دورة تطوير البرمجيات (SDLC).	5.8.2
5.8.3	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.	يجب اتباع معايير وإجراءات وتوجيهات التطوير الآمن فيما يتعلق بكافة الأنظمة والتطبيقات، وذلك لإيجاد خدمة آمنة وترميز آمن وتصميم آمن ضمن بيئات التطوير والاختبار والإنتاج.	5.8.3
5.8.4	Ooredoo 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.	تضمن Ooredoo أن كافة التطبيقات الجديدة سواء التي يتم شراؤها أو التي تم تطويرها، تخضع لاختبارات القبول والتقييم الأمني بهدف تحديد الثغرات ونقاط الضعف الأمنية قبل إطلاقها.	5.8.4
5.9.	**Third party relationships**	**علاقات الطرف الثالث**	5.9
5.9.1	Ooredoo 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.	تقوم Ooredoo بوضع وتنفيذ والمحافظة على سياسة أمن الطرف الثالث وإجراءات مراقبة الالتزام الأمني، وذلك لضمان التزام الطرف الثالث بسياسات ومعايير وإجراءات أمن المعلومات في Ooredoo.	5.9.1
5.9.2	Ooredoo shall ensure agreements and contracts with third parties and their sub-contractors include the obligation to	تضمن Ooredoo بأن تشمل الاتفاقيات والعقود مع الأطراف الثالثة والمتعاقدين معها من الباطن بالتزامهم باتباع سياسات	5.9.2

	follow Ooredoo's information security policies, standards, procedures and SLAs.	و معايير و إجراءات أمن المعلومات واتفاقيات مستوى الخدمة الخاصة بـــــــ Ooredoo.	
5.9.3	Ooredoo shall define Key Performance Indicators (KPIs) and regularly perform or review security assessments for its third party systems or outsourced services.	تحدد Ooredoo مؤشـــرات الأداء الرئيســية وتقوم بانتظام بأداء ومراجعة التقييمات الأمنية لأنظمة الطرف الثالث أو الخدمات المتعاقد عليها خارجياً.	5.9.3
5.9.4	Ooredoo shall regularly conduct an information security risk assessment of its existing and potential third parties.	تقوم Ooredoo بـإجراء تقييم مخـاطر أمن المعلومات بانتظام للأطراف الثالثة الحاليين والمحتملين.	5.9.4
5.10.	**Change and Patch Management**	**إدارة التغيير والتحديثات**	5.10
5.10.1	Ooredoo shall document, implement, and enforce Change and Patch Management framework and service level agreements (SLAs) for all security changes to information processing facilities, systems, applications and processes to ensure that all security changes and patches are timely and securely deployed to minimize the impact on the system's confidentiality, integrity or availability.	تقوم Ooredoo بتوثيق وتنفيـذ وتطبيق إطـار عمـل لـإدارة التغيير والتحـديثـات واتفاقيات مستوى الخدمة لكافة التغييرات الـأمنيـة على مرافق معـالجـة المعلومـات والـأنظمـة والتطبيقـات والـإجراءات، وذلـك لضــمان تنفيذ التغييرات والتحديثات الأمنية في الوقت المناســب وبشــكل آمن للتقليل من التأثير على سرية النظام أو سلامته أو توفره.	5.10.1
5.10.2	Ooredoo shall establish a process to ensure that security changes, configurations and patch deployments are conducted in a planned, managed and secure manor.	تقوم Ooredoo بوضع إجراءات لضمان تنفيذ التغييرات والتهيئـات والتحـديثـات الـأمنيـة بأسلوب مخطط له ومُدار وآمن.	5.10.2
5.11.	**Security Monitoring and Operations**	**المراقبة والعمليات الأمنية**	5.11

5.11.1	Ooredoo 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 and response to information security incidents.	تقوم Ooredoo بتحديد وتخطيط وتصـــميم وتنفيـذ ومتـابعـة إطـار عمـل وبنيـة تحتيـة للمراقبـة والعمليـات الـأمنيـة (الـأشـــخـاص والـإجراءات والتكنولوجيـا) والحفـاظ عليهـا وتطويرها بشـــكل مســـتمر، وذلك لضـــمان المراقبة على مدارة الســـاعة في كل أيام الأسـبوع والكشـف والاسـتجابة في الوقت المناسب لحوادث أمن المعلومات.	5.11.1
5.11.2	Ooredoo shall plan, design, implement and monitor Users' access to Ooredoo systems and applications.	تقوم Ooredoo بتخطيط وتصـــميم وتنفيذ ومراقبة وصـــول المســـتخدمين إلى أنظمة وتطبيقات Ooredoo.	5.11.2
5.11.3	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.	تقوم Ooredoo بتخطيط وتصـــميم وتنفيذ ومراجعـة والمحـافظـة على والتحســـين المســـتمر لـإدارة الثغرات واختبـار الـاختراق وتـقـنـيـات وإجـراءات وإمـكـانـيـات جـمـع المعلومـات عن التهـديـدات واصـــطيـاد التهديدات الضـــرورية لتحديد وتصـــنيف وتصحيح والتخفيف من الثغرات الأمنية.	5.11.3
5.11.4	Ooredoo shall address security vulnerabilities when they are discovered at defined timeframes and provide fixes as applicable.	تقوم Ooredoo بمعـالجـة الثغرات الـأمنيـة عند اكتشـــافها في الإطار الزمني المحدد وتوفر الإصلاحات كلما انطبق ذلك.	5.11.4
5.11.5	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.	تقوم Ooredoo بالإفصـاح بشـكل واضـح عن التغييرات الـأمنيـة (إن وجـدت) التي أجرتهـا على نظـام تشـــغيـل الجوال وتـأثير تلـك التحديثات التي تم إرسالها إلى العملاء.	5.11.5

5.11.6	Ooredoo shall ensure that people are able to share any vulnerabilities they discover within Ooredoo applications and services through designated procedures.	تضـــمن Ooredoo بأن يكون الناس قادرين على مشـــاركة أية ثغرات يكتشـــفونها في تطبيقات وخدمات Ooredoo عبر الإجراءات المخصصة لذلك.	5.11.6
5.11.7	Ooredoo shall define a mechanism through which security researchers or Customers can submit vulnerabilities they discover within Ooredoo applications and services.	تحـدد Ooredoo آليـة يمكن من خلالهـا للبـاحثين في المجـال الـأمني أو العملاء تقـديم الثغرات التي يكتشـــفونهـا في تطبيقات وخدمات Ooredoo.	5.11.7
5.11.8	Ooredoo shall be committed not to pursue legal action against researchers who report vulnerabilities within the terms of The Company's vulnerability reporting mechanism.	تلتزم Ooredoo بعـدم الملاحقـة القـانونيـة ضـــد أي باحثين يقومون بالإبلاغ عن ثغرات ضـــمن شـــروط آلية الإبلاغ عن الثغرات في الشركة.	5.11.8
5.12.	**Incident Handling and Response**	**التعامل مع الحوادث والاستجابة لها**	5.12
5.12.1	Ooredoo 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.	تلتزم Ooredoo بالتعـامل مع حوادث الأمن السيبراني والاستجابة لها بالشكل المناسب ووفقاً للمعايير الأمنية المعروفة وأفضـــل الممارســـات من حيث الأشـــخاص والإجراءات والتكنولوجيا.	5.12.1
5.12.2	An Incident handling and response policy(s) shall be defined and supported by security incident handling and response plan, procedures and controls to detect, report, respond, contain, eradicate and recover from cybersecurity incidents and attacks.	يجب تحديد سياسة (سياسات) التعامل مع الحوادث والاســـتجابة لها ودعمها من خلال خطة وإجراءات وضوابط التعامل مع الحوادث والاســـتجابة لها، وذلك لكشـــف حوادث وهجمات الأمن الســـيبراني والإبلاغ عنها والاســـتجابة لها واحتوائها والقضـــاء عليها والتعافي منها.	5.12.2

5.12.3	Ooredoo 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.	تقوم Ooredoo بإجراء تمارين محاكاة مكتبية وتمارين الأمن السيبراني سنوياً للتعامل مع والاستجابة للحوادث الأمنية وذلك لاختبار وتقييم مدى جاهزية وإمكانية فريق الاستجابة للحوادث من الكشف عن حوادث وهجمات الأمن السيبراني والإبلاغ عنها والاستجابة لها واحتوائها والقضاء عليها والتعافي منها.	5.12.3
5.12.4	Ooredoo shall establish a digital forensics investigation framework to ensure the integrity of data during identification, collection, examination, and analysis.	تقوم Ooredoo بوضع إطار عمل للتحقيق الجنائي الرقمي وذلك لضمان سلامة البيانات أثناء التحديد والجمع والفحص والتحليل.	5.12.4
5.12.5	All suspected Personal Data breaches shall be reported to the Group Chief Legal, Regulatory & Governance Officer (GCLRGO) or his delegate. Where the GCLRGO determines that a Personal Data breach entails the possibility of material damage to the Personal Data or privacy rights of affected individuals, Ooredoo Qatar shall notify the affected individuals and the respective department at the Ministry of Communication and Information Technology.	يجب الإبلاغ عن جميع الانتهاكات المشتبه بها للبيانات الشخصية إلى رئيس الشؤون القانونية والتنظيمية والحوكمة للمجموعة أو من يفوضه. وعندما يحدد رئيس الشؤون القانونية والتنظيمية والحوكمة أن الانتهاك للبيانات الشخصية يؤدي إلى إمكانية ضرر مادي على البيانات الشخصية أو حقوق الخصوصية للأفراد المتأثرين، يجب على Ooredoo إبلاغ الأفراد المتأثرين والإدارة المعنية في وزارة الاتصالات وتكنولوجيا المعلومات.	5.12.5
5.12.6	The CEO, Board and other relevant entities as applicable shall be notified	يجب إبلاغ الرئيس التنفيذي ومجلس الإدارة والجهات المعنية الأخرى كلما انطبق ذلك	5.12.6

	without undue delay when a material incidents or data breach(s) take place.	بدون أي تأخير غير مبرر عند حدوث حوادث مادية أو انتهاك (انتهاكات) للبيانات.	
5.12.7	Ooredoo shall define the necessary steps it would take to address the impact of a data breach on its Customers.	تحدد Ooredoo الخطوات الواجب اتخاذها للتعامل مع تأثير انتهاك البيانات على العملاء.	5.12.7
5.13.	**Information Security Aspects in Business Continuity**	**جوانب أمن المعلومات في استمرارية الأعمال**	5.13
5.13.1	Ooredoo shall be committed to embed information security continuity in its business continuity management systems in compliance with the Business Continuity Management Policy.	تلتزم Ooredoo بضمان استمرارية أمن المعلومات في أنظمة إدارة استمرارية الأعمال بما يتوافق مع سياسة إدارة استمرارية الأعمال.	5.13.1
5.13.2	Ooredoo shall establish, implement and maintain processes and controls to ensure the required level of continuity for information security during an adverse situation.	تقوم Ooredoo بوضع وتنفيذ و المحافظة على إجراءات وضوابط لضمان المستوى المطلوب من الاستمرارية لأمن المعلومات خلال الظروف السلبية.	5.13.2
5.13.3	Ooredoo shall verify the established and implemented information security continuity controls at regular intervals to ensure effectiveness during adverse situations.	تقوم Ooredoo بالتحقق من ضوابط استمرارية أمن المعلومات التي تم وضعها وتنفيذها على فترات زمنية منتظمة، وذلك لضمان فعاليتها خلال الظروف السلبية.	5.13.3
5.14.	**Information Security Compliance Monitoring**	**مراقبة الامتثال لأمن المعلومات**	5.14
5.14.1	Ooredoo shall be committed to establish, implement and maintain an information security compliance monitoring process to ensure compliance with information security polices, applicable national	تلتزم Ooredoo بوضع وتنفيذ إجراءات مراقبة امتثال أمن المعلومات والمحافظة عليها، وذلك لضمان الالتزام بسياسات أمن المعلومات وقوانين الأمن السيبراني	5.14.1

	cybersecurity laws, regulations and applicable international security standards.	الوطنية واللوائح ومعايير الأمن الدولية المعمول بها.	
5.14.2	Ooredoo shall be committed to perform security audits, reviews, technical security assessments (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. The frequency of penetration testing and vulnerability assessment shall be defined by Ooredoo's Corporate Information Security team and any critical findings shall be reported to the CEO and the Board.	تلتزم Ooredoo بإجراء عمليات التدقيق الأمني والمراجعات والتقييمات الأمنية التقنية (مثل اختبار الاختراق وتقييم الثغرات) ومراجعات الامتثال في فترات زمنية مخطط لها أو عند حدوث تغيير هام، وذلك لضمان فعالية الضوابط الأمنية للتخفيف من مخاطر الأمن السيبراني ذات الصلة. ويجب تحديد فترات إجراء اختبار الاختراق وتقييم الثغرات من قبل فريق أمن معلومات الشركة، ويجب الإبلاغ عن أي نتائج حرجة إلى الرئيس التنفيذي ومجلس الإدارة.	5.14.2
5.15.	**Policy Enforcement**	**تنفيذ السياسة**	5.15
5.15.1.	All Ooredoo employees, consultants, contractors, sub-contractors, vendors, suppliers and their employees are independently responsible for reading, understanding and following this policy.	يكون كل موظفي Ooredoo واستشاريها والمتعاقدين معها والمتعاقدين من الباطن والموزعين والمردين مسؤولين بشكل مستقل عن قراءة وفهم واتباع هذه السياسة.	5.15.1
5.15.2.	Non-compliances with this Information Security Policy shall be dealt in accordance with Ooredoo's applicable policies, procedures and contractual obligations.	سيتم التعامل مع عدم الالتزام بسياسة أمن المعلومات هذه وفقاً للسياسات والإجراءات والالتزام التعاقدية المطبقة في Ooredoo.	5.15.2
5.16.	**Policy Amendment**	**تعديل السياسة**	5.16

5.16.1.	This policy supersedes all previous releases (policy, circular, memos, instructions or any other form) on its subject-matter.	تلغي هذه السياسة كافة الإصدارات السابقة (سواء كانت سياسة أو تعميماً أو مذكرات أو تعليمات أو أي شكل آخر) فيما يتعلق بموضوعها.	5.16.1
5.16.2.	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's Board of Directors.	أي تغيير على أحكام هذه السياسة يجب أن تتم مراجعته والتوصية به أولاً من قبل لجنة التدقيق وإدارة المخاطر (ARC) واعتماده بشكل نهائي من مجلس إدارة Ooredoo.	5.16.2
5.16.3.	Any deviation on the implementation of this policy shall be approved by the Board of Directors.	أي تغيير على تنفيذ هذه السياسة يجب اعتماده من مجلس الإدارة.	5.16.3
6.	**REFERENCES** (Processes, Procedures, guidelines, and/or any relevant document)	**المراجع** (الإجراءات، و العمليات، و التوجيهات و/أو أية وثائق ذات صلة).	**6.**
6.1.	Identity and Access Management Policy	سياسة إدارة الهوية والوصول	6.1
6.2.	Information Classification Policy	سياسة تصنيف المعلومات	6.2
6.3.	Acceptable Use Policy	سياسة الاستخدام المقبول	6.3
6.4.	Encryption Policy	سياسة التشفير	6.4
6.5.	Network Security Policy	سياسة أمن الشبكات	6.5
6.6.	Enterprise Wireless Security Policy	سياسة الاتصال بالشبكة اللاسلكية	6.6

6.7.	Application Security Policy	سياسة أمن التطبيقات	6.7
6.8.	Anti-Malware Policy	سياسة الحماية من البرمجيات الخبيثة	6.8
6.9.	Logging and Monitoring Policy	سياسة السجلات والمراقبة الأمنية	6.9
6.10.	Information Security Incident Management Policy	سياسة إدارة حوادث أمن المعلومات	6.10
6.11.	Protection of Personal Data Privacy	سياسة حماية خصوصية البيانات الشخصية	6.11
6.12.	(Law No. 13/2016) Concerning Privacy and Protection of Personal Data	(القانون رقم 13 لسنة 2016) بشأن حماية خصوصية البيانات الشخصية	6.12
6.13.	Encryption Management Standard	معيار إدارة التشفير	6.13
6.14.	Business Continuity Management Policy	سياسة إدارة استمرارية الأعمال	6.14
6.15.	ISO 27001:2013 – Information technology – Security techniques – Code of practice for information security controls.	ISO 27001:2013 – أمن المعلومات – التقنيات الأمنية – ميثاق ممارسة ضوابط أمن المعلومات	6.15
6.16.	Payment Card Industry Data Security Standard (PCI-DSS)	معيار أمن بيانات صناعة بطاقات الدفع (PCI-DSS)	6.16
6.17.	Qatar National Information Assurance (NIA) Policy v2.0	سياسة تأمين المعلومات الوطنية – النسخة 2.0	6.17
6.18.	Security Policy	سياسة الأمن	6.18
6.19.	Information Security Management Process	إجراءات إدارة أمن المعلومات	6.19
6.20.	Enterprise Risk Management Process	إجراءات إدارة المخاطر	6.20

6.21.	Vulnerability Management E2E Process	الإجراءات المتكاملة لإدارة الثغرات	6.21
6.22.	User Access and Identity Management Process	إجراءات إدارة وصول وهوية المستخدم	6.22
6.23.	Control of Documented Information Process	إجراءات إدارة المعلومات الموثقة	6.23
6.24.	HR policy	سياسة الموارد البشرية	6.24
6.25.	Law No. 14 of 2014 Promulgating the Cybercrime Prevention Law	القانون رقم 14 لسنة 2014 بإصدار قانون مكافحة الجرائم الالكترونية	6.25
6.26.	Decree-Law No. 34 of 2006, Promulgating the Telecommunications Law	المرسوم بقانون رقم 34 لسنة 2006 بإصدار قانون الاتصالات	6.26
6.27.	Decree Law No 16 of 2010 Promulgating the Electronic Transactions and Commerce Law	المرسوم بقانون رقم 16 لسنة 2010 بإصدار قانون المعاملات والتجارة الالكترونية	6.27

7. VERSION HISTORY

Version No.	Date	Approved by	Description of Change	Policy Reference
3	Oct 3, 2022	BoD	Major Changes	POL/2018/12