

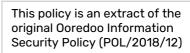


Ooredoo Information Security Policy – External Version

سياسة أمن المعلومات في أريدٌ – النسخة الخارجية

1.	PURPOSE	الغرض	1.
1.1.	The purpose of this information security	تهدف هذه الســـياســــة الى توفير دعم	1.1
	policy is to provide Ooredoo's Top	وتوجــه الـــإدارة العليـــا في أريـــدُ من خلال	
	Management's direction and support through information security and data	سـياســات، ومعايير، وإجراءات وضــوابط أمن	
	protection policies, standards,	المعلومات وحماية البيانات التي تضـــبط	
	procedures and controls that shall	وتدير وتشــــغل أمن المعلومات في أريدُ	
	govern, manage, and operate information	والتي تضمن:	
	security in Ooredoo ensuring: 1. A robust and a homogenous	1. إطار عمل وعمليات أمن معلومات قوية	
	Information Security Framework and	ومتجانسة في أريدُ.	
	operations across Ooredoo.	2. حماية كافة الخدمات والبنية التحتية	
	2. All services and their supporting	الداعمة بشــكل كافٍ من التهديدات الأمنية	
	infrastructures are adequately protected	المختلفة.	
	against the various security threats.3. Services and infrastructure resilience	3. مرونــة الخــدمــات والبنيــة التحتيــة أمــام	
	to security incidents and attacks.	الحوادث والهجمات الأمنية.	
	4. Information security compliance to	4. امتثال أمن المعلومات لسياسات ومعايير	
	information security policies, standards,	أمن المعلومــات والمتطلبــات القــانونيـــة	
	national legal and regulatory requirements.	والتنظيمية الوطنية.	
	5. A uniform cyber security workforce	5. مهارات وقدرات موحدة في مجال الأمن	
	skills and capabilities in Ooredoo.	 السيبراني في أريدُ	

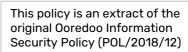






	6. A security-conscious culture across Ooredoo.	6. وجود بيئــة واعيــة و مــدركــه لــأمن	
	ooreado.	المعلومات في أريدُ.	
2.	SCOPE	المجال	2.
2.1.	This policy applies to all Ooredoo's infrastructure used to deliver Ooredoo's products and services to Customers including all internal users who have access 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 الســـياســـة على كافة أنحاء البنى التحتية المســـتخدمة لتوفير منتجات وخـدمــات أريــدُ للعملاء، وتشـــمــل كــافــة المســـتخدمين المســـموح لهم باســـتخدام معلومات الشــــركة بما في ذلك موظفي الشـــركة والاســـتشـــاريين والمتعاقدين والمـتعــاقــدين من البــاطن والمـوردين والموزعين و موظفيهم و أي شـــخص تم تزويده بصـلاحية الوصول إلى المعلومات أو أصول المعلومات التي تمتلكها أريدُ أو تدار بواسطتها.	2.1
3.	EXCEPTIONS	الاستثناءات	3.
3.1.	None	لا يوجد	3.1
4.	DEFINITIONS	التعريفات	4.
follow meani	olying the statements of this policy, the ing words and expressions have the ings hereby assigned to them, unless the xt otherwise states.	طبيق أحكام هذه السياسة، ستكون للكلمات ات التالية المعاني الموضحة قرين كل منها، ما ض السياق معنى آخر.	 والعبار
4.1.	The Company / Ooredoo Ooredoo Q.P.S.C. a Qatari Public Shareholding Company	الشركة / أريدُ أريدُ ش.م.ق.ع.، شـــركة مســـاهمة قطرية عامة	4.1

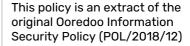






	(Ooredoo Qatar)	(أريدُ قطر).	
4.2.	Asset Owner Refers to a Department or person who is responsible for an asset in The Company and authorized to request, approve and terminate the provision of access to the Corporate's information or information processing device.	المسؤول عن الأصل الإدارة أو الشخص المسـؤول عن أصـل في الشـــركة 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 الـأفراد أو الشـــركــات المشتركون أو الذين قاموا بشراء منتجات أو خدمات من أريدُ.	4.3
4.4.	Third Party Data Processor A natural or legal person who processes Personal Data for Ooredoo.	معالج بيانات الطرف الثالث وهو الشـــخص الطبيعي أو القانوني الذي يقوم بمعالجة البيانات الشــخصــية لصـــالح أريدُ.	4.4
4.5.	Endpoint Devices Refers to Ooredoo owned or managed desktop computers, laptops, smart phones, tablets and other devices.	أجهزة المستخدمين تشـــير إلى أجهزة الكمبيوتر الشــخصــية والمحمولـة والهواتف الـذكيــة والـأجهزة اللوحية وغيرها من الأجهزة التي تمتلكها أو تديرها أريدُ.	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	الأصل المعلوماتي	4.7







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.

ويشـــير إلى البيـانـات الملموســـة وغير الملموســـة والتي تمتلك قيمة بالنســبة للشــركة، بما في ذلك البيانات المتعلقة أو المتصلة بـــ أريدُ والبيانات الموكلة إليها من طرف آخر. ويتضـمن هذا البيانات بأشــكالها الـالكترونيـة والمـاديـة، بمـا في ذلـك على ســبيل المثال لا الحصــر الوثائق ورســائل البريـد الـالكتروني والفـاكس والمظـاريف والبيانات الناتجة عن استخدام التطبيقات.

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 ســيــاســـــة أمن المعلومــات والإجراءات والتوجيهـات والمعـايير الداءـمة التي تتبعها الشــــركة لإدارة مخاطر الأمن السـيبراني ولضـمان حماية أصــول معلومات أريـدُ ومرافق معـالجـة المعلومـات بشــــكـل كافِ.

4.9. **IS**

Information Security.

I S

4.9

4.10

4.8

أمن المعلومات

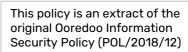
4.10. Personal Data

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.

الىيانات الشخصية

البيانات التي تتم معالجتها من قبل أريدُ أو بالنيابة عنها والتي تنتمي إلى و/ أو تكون حول شــخص لـه هويـة محـددة، أو يمكن التحقق بشـــكل معقول منه من خلال تلك البيانات أو الجمع بين تلك البيانات وغيرها من البيانات .

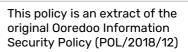






4.11.	Sensitive Personal Data Personal Data related to the racial origin, children, health condition, physical or psychological, religion, marital relations, or criminal actions, or any other Personal Data, identified by MCIT, which it determines may cause serious damages to the Individual if misused 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	4.11
		أضرار خطيرة على الفرد في حال سوء استخدامها أو الإفصاح عنها	
4.12.	MCIT Ministry of Communications and Information Technology.	MCI T وزارة الاتصالات وتكنولوجيا المعلومات	4.12
4.13.	Staff/User(s) Refers to all The Company employees, consultants, contractors, subcontractors, 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, application, etc. to ensure its confidentiality, integrity and availability.	الحد الأدنى للمعايير الأمنية يشير إلى قائمة الحد الأدنى من المتطلبات الأمنية اللازمة والتي يجب تنفيذها في أجهزة وأنظمة وتطبيقات معالجة معلومات الشركة وغيرها، وذلك لضمان سريتها وسلامتها وتوفرها.	4.14

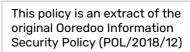






4.15.	Corporate Information Security (CIS)	إدارة أمن معلومات الشركة (CIS)	4.15
	The Corporate Information Security		
	Department within the CEO Office of	إدارة أمن معلومات الشركة التابعة لمكتب	
	Ooredoo Qatar.	الرئيس التنفيذي في أريدُ قطر.	
4.16.	Business Units	وحدات العمل	4.16
	Refers to Ooredoo Business Units such as	وتشير إلى وحدات العمل مثل التكنولوجيا،	
	Technology, Commercial, CEO Officeetc.		
		والوحدة التجارية، وحدة مكتب الرئيس	
		التنفيذيالخ.	
5.	Policy Statement	بيان السياسة	5.
F 4	Out a reason with a Consequence		F 1
5.1.	Cybersecurity Governance	حوكمة الأمن السيبراني	5.1
5.1.1.	Ooredoo shall be committed to secure its	تلتزم أريـدُ بتـأمين منتجـاتهـا وخـدمـاتهـا	5.1.1
	products and services and deliver them	وتوفيرها إلى عملائها بأسلوب آمن.	
F 4 2	to its Customers in a secure manner.		5.1.2
5.1.2.	The information security organization structure along with information security	يجب وضــع هيكلة أمن المعلومات مع أدوار	5.1.2
	roles and responsibilities shall be	ومسؤوليات أمن المعلومات والحفاظ عليها	
	developed, maintained and assigned at all	وتخصيصها على كافة المستويات، من أجل	
	levels to manage information security	إدارة أمن المعلومـات في أريــدُ عبر كــافــة	
	within Ooredoo and across all Business	وحدات العمل والخدمات بما يضـــمن فهم	
	Units and services and ensuring that the	الموظفين لها.	
	Staff understand them.	· 0 3	
5.1.3.	Ooredoo shall be committed to adopt a	تلتزم أريدُ بتبني نظام إدارة أمن معلومات	5.1.3
	systematic Information Security	"	
	Management System (ISMS) that	منظم يقوم بوضع وتنفيذ وتشغيل ومراقبة	
	establishes, implements, operates,	والمحافظـة والتحســين المســـتمر لـأمن ـــــــــــــــــــــــــــــــــــ	
	monitors, maintain, and continuously	المعلومات، وذلك لتحقيق أهداف الشـــركة	
	improves information security to achieve	المعتمدة على تقييم المخاطر ومســــتويات	
	business objectives based on risk		

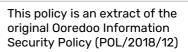






	assessment and acceptance levels to effectively treat and manage information	القبول للتعامل مع مخاطر أمن المعلومات	
	security risks.	وإدارتها بشكل فعال.	
5.1.4.	The Corporate Information Security Department shall be responsible to define and maintain the information security policies, standards, procedures, guidelines and practices within Ooredoo Qatar.	يقع على عاتق إدارة أمن معلومات الشـركة مسؤولية تحديد سياسات ومعايير وإجراءات وتوجيهــات وممــارســــــات أمن معلومــات الشركة في أريدُ والحفاظ عليها.	5.1.4
5.1.5.	This Information Security policy shall be	تكون سياسة أمن المعلومات مدعومة على	5.1.5
	supported, at minimum, by domain- specific information security policies,	الـأقـل، بســـيــاســــات ومعــايير وإجراءات	
	standards, procedures and guidelines for	وتوجيهات أمن المعلومات الخاصة بالمجالات	
	the following domains:	التالية:	
	Information Security Governance	1. حوكمة أمن المعلومات	
	2. Identity and Access Management	2. إدارة الهوية والوصول	
	3. Network Security	3. أمن الشبكة	
	4. Endpoint Security	4. أمن أجهزة المستخدمين	
	5. Application Security6. Cloud Security	5. أمن التطبيقات	
	7. Data Privacy and Data Protection	6. الأمن السحابي (كلاود)	
	8. Change and Patch Management	7. خصوصية البيانات وحماية البيانات	
	9. Security Monitoring and	8. إدارة التغيير والتحديث	
	Operations	9. المراقبة والعمليات الأمنية	
	10. Security Incident Management11. Physical and Environmental	10. إدارة الحوادث الأمنية	
	Security	11. الأمن المادي والبيئي	
5.1.6.	An Information security steering committee (ISSC) consisting of representatives from the different	يجب تأسيس لجنة تسيير أمن المعلومات مكونة من مختلف إدارات الشركة، وذلك	5.1.6

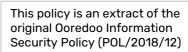






	business functions in the organization shall be established to facilitate the information security projects' and initiatives' deployment, implementation and maintenance of the information security framework(s). The committee to report to CEO directly.	لتسهيل تنفيذ مشاريع ومبادرات أمن المعلومات والحفاظ على إطار (أطر) عمل أمن المعلومات. وتتبع اللجنة الرئيس التنفيذي مباشرة .	
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.	يجـب تحـديـد أدوار ومســـؤوليــات أمن المعلومات وتنفيذها بشــكل مناســب كجزء من ميثاق الموارد البشرية للسلوك المهني وأخلاقيات العمل واتفاقيات عدم الإفصـــاح مع موظفي أريدُ 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 فصــل واجبات ومســؤوليات الموظفين بشـــكـل كــاف، وذلــك للتقليــل من فرص التعديل غير المقصـــود 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 مشـــروع، من مرحلة البداية والتخطيط والتصــميم والتنفيذ وصــولاً إلى إغلاق المشروع.	5.1.9
5.1.10.	Ooredoo 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.	تلتزم أريــدُ بوضـــع وتنفيــذ إجراءات إدارة مخاطر أمن المعلومات والمحافظة عليها، وذلــك لـــإدارة المخــاطر والتخفيف منهـــا	5.1.10

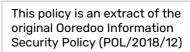






		والتقليل من الآثار المحتملة على أصـــول	
		المعلومات إلى مستوى مقبول.	
5.1.11.	Ooredoo shall ensure that internal and	تضـــمن أريــدُ القيــام بتقييمــات وعمليــات	5.1.11
	external security assessments and audits	تدقيق أمنية داخلية وخارجية لمنتجاتها	
	are conducted for its products, services and infrastructure to ensure	وخدماتها وبنيتها التحتية، وذلك لضــــمان	
	effectiveness of and continual	الفعــاليـــة والتحســـين المســــتمر لــأمن	
	improvement to information security.	المعلومات.	
5.1.12.	Ooredoo shall be committed to	تلتزم أريدُ بالاســــتمرار في تطوير وتنفيذ	5.1.12
	continuously develop, implement and	برنــامج التـوعيــة والتــدريــب عـلـى أمـن	
	maintain information security awareness and training program for all Users to	المعلومات لكافة المســتخدمين والمحافظة	
	ensure understanding of Ooredoo	عليه، وذلك لضـــمان فهم ســـياســــات أمن	
	information security policies and the	معلومات أريدُ وتهديدات الأمن الســـيبراني	
	changing cyber security threats.	المتغيرة.	
5.1.13.	Ooredoo shall publish practical materials	تقوم أريـدُ بنشـــر المواد التطبيقيــة التي	5.1.13
	that educate Customers on how to protect themselves from cybersecurity	تثقف عملاءها حول كيفية حماية أنفسـهم	
	risks relevant to The Company's products	من مخــاطر الـــأمن الســــيبراني المتعلقــة	
	and services.	بمنتجات وخدمات الشركة.	
5.2.	Endpoint Security	أمن أجهزة المستخدمين	5.2
5.2.1.	Ooredoo shall establish and deploy	تضــع أريدُ وتنشــر أطر عمل وتقنيات لتأمين	5.2.1
	frameworks and technologies to secure	كـافــة أجهزة المســــتخــدمين لــديهــا من	
	all its Endpoint Devices from unauthorized access and use, malware	الوصــول والاســتخدام غير المصــرح به ومن	
	infection and data leakage.	البرمجيات الخبيثة وتسريب البيانات.	
5.2.2.	An Acceptable Use policy (AUP) shall be	يتم وضــع ســياســة للاســتخدام المقبول	5.2.2
	established to provide rules that protect	لتحـديـد القواعـد التي تحمي كـل من أريـدُ	
	both Ooredoo and its Staff from potential liability, reduce information security risks,	" وموظفيها من أي عواقب محتملة، والتقليل	
	nazmej, roddod i normadori ocodirej risko,		

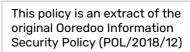






5.2.3.	promote good practice and ensure that all Users are aware of their roles, responsibilities and obligations when using Ooredoo Information Assets. Minimum Baseline Security Standards (MBSS) shall be established, implemented and enforced for Endpoint Devices' operating system, applications and	من مخـاطر أمن المعلـومـات، وتعزيـز الممارســـات الجيدة، وضـــمان إدراك كافة المســـتخدمين لأدوارهم ومســـؤولياتهم والتزامــاتهم أثنــاء اســـتخــدام أصـــول المعلومات. يجب وضــع الحد الأدنى من المعايير الأمنية وتنفيذه فيما يتعلق بنظام تشــغيل أجهزة المســـتخـدمين والتطبيقــات ومســــتويــات	5.2.3
5.2.4.	network layers. Ooredoo shall ensure adequate protection of all its Information Assets throughout the phases of the Asset's life cycle.	الشبكة. تضــمن أريدُ الحماية الكافية لكافة أصـــول 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 أريـدُ بوضــع وتنفيــذ إجراءات إدارة الأصـــول والمحافظة عليها لمتابعة مخزون الأصـــول من أجهزة المســـتخدمين، وذلك لضــمان إعادة أصــول المعلومات عند إنهاء عقد المســتخدمين، ولضــمان حماية أصــول 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 safeguards during planning, design, implementation and testing of its	تضمن أريدُ وجود الضوابط الأمنية والإجراءات المضــــادة والإجراءات الوقائية أثناء تخطيط	5.3.1

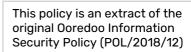






	Telecommunication and Enterprise	وتصـــميم وتنفيــذ واختبــار البنى التحتيــة	
	network Infrastructures.	للاتصالات وشبكة الشركة.	
5.3.2.	Ooredoo shall establish, implement and	تقوم أريدُ بوضع وتنفيذ أطر العمل والأدوات	5.3.2
	maintain adequate frameworks and	الأمنية الكافية والمحافظة عليها لإدارة	
	security tools for network access	الوصول إلى الشبكة وإدارة الوصول عن بعد	
	management, remote access management, network security	وإدارة التهيئــة الــأمنيــة للشــــبكــة وأمن	
	configuration management,	و؛ وب " " " و و الاتصال وتبادل/ نقل المعلومات وأمن البريد	
	communication security, information		
	exchange/transfer and email security to	الــالكتروني، وذلــك للحمــايــة من اختراقــات	
	protect from unauthorized network	الشبكة ومخاطر سوء الاستخدام والانتهاك.	
	intrusions and risks of misuse and abuse.		
5.3.3.	Ooredoo shall define, implement,	تقوم أريدُ بتحديد وتنفيذ وتحسين سياسات	5.3.3
	maintain and continuously improve cloud	ومعايير إجراءات وضـــوابط الأمن الســـحابي	
	security policies, standards, procedure and security controls for the various	(الكلاود) باســـــتمرار، وذلك لمختلف نماذج	
	cloud service models it hosts or is	خدمات كلاود التي تستضيفها أو التي يتم	
	subscribed to; Software as a Service	الاشــــتراك بها: البرمجيات كخدمة (SaaS)	
	(SaaS), Platform as a Service (PaaS) and	والمنصــــــــــــــــــــــــــــــــــــ	
	Infrastructure as a Service (laaS).	كخدمة (I aaS).	
5.4.	Information Classification and	تصنيف وحماية المعلومات	5.4
	Protection		
5.4.1.	Ooredoo shall define, implement and	تقوم أريدُ بتحديد وتنفيذ والمحافظة على	5.4.1
	maintain information security policies	ســـياســــات ومعايير أمن المعلومات فيما	
	and standards for information	يتعلق بتصـــنيف المعلومات وتســـميتهـا	
	classification, labelling and handling to avoid information leakage and	والتعـامـل معهـا، وذلـك لتجنـب تســـريـب	
	avoid information leakage and unauthorized access.	والتعاومات أو الوصول غير المصرح به إليها.	
	andanonzed docess.	المعلومات او الوصول عير السطرح به إنيسا.	

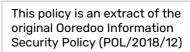






5.4.2.	Ooredoo shall plan, design, implement, deploy, maintain and continuously improve appropriate data protection controls that are proportionate to the information classification level.	تقوم أريدُ بتخطيط وتصــميم وتنفيذ ونشــر والمحافظة على الضـــوابط الملائمة لحماية البيانات بما يتوافق مع مســـتوى تنصـــيف 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.	تضــع أريـدُ إطـار عمـل لـإدارة الهويـة و الوصــول، وتتضـمن سـياسـات ومعايير إدارة الهوية والهوية والوصــول المتميز، وإدارة الوصــول المتميز، وإدارة الوصـــول عن بعــد، وإدارة كلمـات المرور، وغيرهـا، بـالـإضـــافـة إلى الـأدوات الأمنية لضـــمان حوكمة وإدارة و عمليات ثابتة لإدارة الهوية والوصــول في أريدُ أثناء التحــاق الموظفين بــالعمــل 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.	تضع أريدُ الإجراءات والأدوات لمراقبة الالتزام وقيـــاس فعـــاليـــة تنفيـــذ إدارة الهويـــة 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 أريدُ بوضـــع وتنفيذ إطار عمل لإدارة التشـــفير والمحافظة عليه، وذلك لحماية البيانات الســرية والحســاســة التي تتلقاها أريدُ وتخزنها وتديرها وتعالجها وتنقلها عبر شبكة أريدُ.	5.6.1

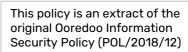






5.6.2.5.7.5.7.1	Ooredoo shall establish, implement and maintain cryptographic key management standards for secure key generation, ownership, usage, distribution, storage, backup and recovery, and revocation to protect the keys throughout their lifecycle. Physical and Environmental security Ooredoo shall establish, implement and maintain physical security framework to protect Ooredoo's Information Assets	تقوم أريدُ بوضع وتنفيذ معايير إدارة مفتاح التشـــفير لإنشـــاء مفتاح أمني وامتلاكه واســـتخدامه وتوزيعه وتخزينه والنســـخ اللحتياطي والاســـترجاع والإلغاء والمحافظة عليه، وذلك لحمـايــة المفـاتيح طوال مـدة خدمتها. الأمن المادي والبيئي تقوم أريدُ بوضـــع وتنفيذ إطار عمل للأمن المـادي والمحـافظـة عليـه، وذلـك لحمـايــة المـادي والمحـافظـة عليـه، وذلـك لحمـايــة	5.6.2 5.7 5.7.1
5.7.2	and facilities hosting information against unauthorized access, physical and environmental damage. 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.	أصـــول المعلومات في أريدُ والمرافق التي تســتضــيف المعلومات ضــد الوصــول غير المصرح به والضرر المادي والبيئي. تقوم أريدُ بتنفيذ ضوابط إدارية وفنية للأمن المادي على كافة مرافق المباني والمواقع ومراقبة التزامها بشـــكل مســـتمر 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 أريدُ بوضع وتنفيذ سياسات ومعايير وإجـراءات وتـوجـيـهــات وأدوات حـمــايــة التطبيقات والمحافظة عليها، بما في ذلك شــــراء وتطوير وصــــيانة التطبيقات ونظم المعلومات.	5.8.1
5.8.2	Ooredoo shall ensure that security requirements are developed, considered and implemented alongside functional	تضـــمن أريـدُ وضـــع المتطلبـات الـأمنيـة ودراســــتها وتنفيذها إلى جانب المتطلبات	5.8.2

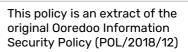






and technical requirements at all phases مشروع of project planning and implementation		
at project planning and implementation	التشغيلية والفنية في كافة مراحا	
برمجيــات	تخطيط وتنفيــذ دورة تطوير الـ	
of Software Development Life Cycle	.(SDLC)	
(SDLC).		E 0 7
	يجــب اتبــاع معــايير وإجراءات وت	5.8.3
procedures and guidelines shall be الأنظمة followed for all systems and applications	التطوير الآمن فيما يتعلق بكافة	
	والتطبيقات، وذلك لإيجاد خدمة آم	
	آمن وتصـــميم آمن ضـــمن بيئــان	
testing and production environments.	والاختبار والإنتاج.	
5.8.4 Ooredoo shall ensure that all new الجديدة	تضـــمن أريدُ أن كافة التطبيقات	5.8.4
applications, systems that are acquired, التي تم	ســــواء التي يتم شــــراؤهـــا أو	
developed or enhanced undergo system والتقييم acceptance testing and security	تطويرها، تخضــع لاختبارات القبول	
	الأمني بهدف تحديد الثغرات ونقاه	
security gaps and vulnerabilities before	الأمنية قبل إطلاقها.	
their launch.		
5.9. Third party relationships	علاقات الطرف الثالث	5.9
5.9.1 Ooredoo shall establish, implement and	تقوم أريدُ بوضـــع وتنفيذ والمحاذ	5.9.1
maintain third party security policy and ت مراقبة	تقوم أريدُ بوضـــع وتنفيذ والمحاذ سياسة أمن الطرف الثالث وإجراءا	5.9.1
maintain third party security policy and security compliance monitoring process	سياسة أمن الطرف الثالث وإجراءا	5.9.1
maintain third party security policy and security compliance monitoring process to ensure third party's adherence to	سياسة أمن الطرف الثالث وإجراءا الالتزام الأمني، وذلك لضــمان التزا	5.9.1
maintain third party security policy and security compliance monitoring process to ensure third party's adherence to	سياسة أمن الطرف الثالث وإجراءا الالتزام الأمني، وذلك لضــمان التزا الثالث بســــياســــات ومعايير وإجر	5.9.1
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.	سياسة أمن الطرف الثالث وإجراءا الالتزام الأمني، وذلك لضــمان التزا الثالث بســـياســــات ومعايير وإجر المعلومات في أريدُ.	5.9.1
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. 5.9.2 Ooredoo shall ensure agreements and contracts with third parties and their	سياسة أمن الطرف الثالث وإجراءا الالتزام الأمني، وذلك لضــمان التزا الثالث بســـياســـات ومعايير وإجر المعلومات في أريدُ. تضــمن أريدُ بأن تشــمل الاتفاقيات	
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. 5.9.2 Ooredoo shall ensure agreements and contracts with third parties and their sub-contractors include the obligation to	سياسة أمن الطرف الثالث وإجراءا الالتزام الأمني، وذلك لضــمان التزا الثالث بســـياســـات ومعايير وإجر المعلومات في أريدُ. تضــمن أريدُ بأن تشــمل الاتفاقيات مع الأطراف الثالثة والمتعاقدين م	
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. 5.9.2 Ooredoo shall ensure agreements and contracts with third parties and their sub-contractors include the obligation to follow Ooredoo's information security	سياسة أمن الطرف الثالث وإجراءا الالتزام الأمني، وذلك لضــمان التزا الثالث بســـياســـات ومعايير وإجر المعلومات في أريدُ. تضــمن أريدُ بأن تشــمل الاتفاقيات مع الأطراف الثالثة والمتعاقدين الباطن بالتزامهم باتباع سياسات و	
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. 5.9.2 Ooredoo shall ensure agreements and contracts with third parties and their sub-contractors include the obligation to follow Ooredoo's information security	سياسة أمن الطرف الثالث وإجراءا الالتزام الأمني، وذلك لضــمان التزا الثالث بســـياســـات ومعايير وإجر المعلومات في أريدُ. تضــمن أريدُ بأن تشــمل الاتفاقيات مع الأطراف الثالثة والمتعاقدين م	

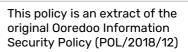






5.9.3	Ooredoo shall define Key Performance Indicators (KPIs) and regularly perform or review security assessments for its third party systems or outsourced services. Ooredoo shall regularly conduct an information security risk assessment of its existing and potential third parties.	تحدد أريدُ مؤشــرات الأداء الرئيســية وتقوم بانتظام بأداء ومراجعة التقييمات الأمنية لأنظمة الطرف الثالث أو الخدمات المتعاقد عليها خارجياً. تقوم أريــدُ بــإجراء تقييم مخــاطر أمن المعلومات بانتظام للأطراف الثالثة الحاليين والمحتملين.	5.9.4
5.10.	Change and Patch Management	إدارة التغيير والتحديثات	5.10
5.10.2	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. Ooredoo shall establish a process to ensure that security changes, configurations and patch deployments are conducted in a planned, managed and secure manor.	تقوم أريـدُ بتوثيق وتنفيـذ وتطبيق إطـار عمـل لـإدارة التغيير والتحديثات واتفـاقـيات مســـتوى الخدمة لكافة التغييرات الأمنية على مرافق معـالجـة المعلومـات والـأنظمة والتطبيقات والإجراءات، وذلك لضـمان تنفيذ التغييرات والتحـديثـات الـأمنيـة في الوقـت المناســـب وبشــكل آمن للتقليل من التأثير على سرية النظام أو سلامته أو توفره. تقوم أريدُ بوضــع إجراءات لضـــمان تنفيذ التغييرات والتهـيئـات 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	تقوم أريدُ بتحديد وتخطيط وتصميم وتنفيذ ومتابعة إطار عمل وبنية تحتية للمراقبة والعمليات الأمنية (الأشـــخاص والإجراءات والتكنولوجيــا) والحفــاظ عليهــا وتطويرهــا	5.11.1

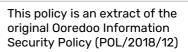






	technology) to ensure 24/7 monitoring	بشـكل مسـتمر، وذلك لضـمان المراقبة على	
	and timely detection of and response to information security incidents.	مدارة الســــاعـة في كـل أيـام الـأســـبوع	
information security incluents.	information security incidents.	والكشــف والاســتجابة في الوقت المناســب	
		لحوادث أمن المعلومات.	
5.11.2	Ooredoo shall plan, design, implement	تقوم أريدُ بتخطيط وتصميم وتنفيذ ومراقبة	5.11.2
	and monitor Users' access to Ooredoo systems and applications.	وصـول المسـتخدمين إلى أنظمة وتطبيقات	
		أريدُ.	
5.11.3	Ooredoo shall plan, design, implement,	تقوم أريــدُ بتخطيط وتصـــميم وتنفيــذ	5.11.3
	review, maintain and continuously	ومراجعــة والمحــافظــة على والتحســـين	
	improve vulnerability management, penetration testing, threat intelligence	المســــتمر لإدارة الثغرات واختبـار الـاختراق	
	and threat hunting technologies,	وتقنيات وإجراءات وإمكانيات جمع	
	processes and competencies necessary	المعلومــات عن التهــديــدات واصـــطيــاد	
	to identify, classify, remediate and	التهديدات الضـــرورية لتحديد وتصـــنيف	
	mitigate security vulnerabilities.	وتصحيح والتخفيف من الثغرات الأمنية.	
5.11.4	Ooredoo shall address security	تقوم أريـدُ بمعـالجـة الثغرات الـأمنيـة عنـد	5.11.4
	vulnerabilities when they are discovered	اكتشــافها في الإطار الزمني المحدد وتوفر	
	at defined timeframes and provide fixes	" الإصلاحات كلما انطبق ذلك.	
5.11.5	as applicable. Ooredoo shall clearly disclose what, if	تقوم أبيد باللغور لميث كلمام أمري	5.11.5
5.11.5	any, security modifications it has made to	تقوم أريدُ بالإفصـــاح بشـــكل واضـــح عن	
	a mobile operating system and effect of	التغييرات الـأمنيـة (إن وجـدت) التي أجرتهـا	
	such modification updates sent to	على نظـام تشـــغيـل الجوال وتــأثير تلـك	
	Customers.	التحديثات التي تم إرسالها إلى العملاء.	F 44 /
5.11.6	Ooredoo shall ensure that people are able to share any vulnerabilities they discover	تضـــمن أريدُ بأن يكون الناس قادرين على	5.11.6
	within Ooredoo applications and services	مشــــاركـة أيـة ثغرات يكتشـــفونهـا في	
	through designated procedures.	تطبيقــات وخــدمــات أريــدُ عبر الـــإجراءات	
		المخصصة لذلك.	

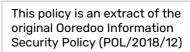






5.11.7	Ooredoo shall define a mechanism through which security researchers or Customers can submit vulnerabilities they discover within Ooredoo applications and services. Ooredoo shall be committed not to pursue legal action against researchers who report vulnerabilities within the terms of The Company's vulnerability reporting mechanism.	تحدد أريدُ آلية يمكن من خلالها للباحثين في المجـــال الـــأمني أو العملاء تقـــديم الثغرات التي يكتشـــفونهـا في تطبيقــات وخدمات أريدُ. تلتزم أريدُ بعدم الملاحقة القانونية ضـــد أي بـاحثين يقومون بـالــإبلاغ عن ثغرات ضــــمن شروط آلية الإبلاغ عن الثغرات في الشركة.	
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. 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.	تلتزم أريــدُ بــالتعــامــل مع حوادث الــأمن السيبراني والاستجابة لها بالشكل المناسب ووفقاً للمعايير الأمنية المعروفة وأفضـــل الممارســـات من حيث الأشـــخاص والإجراءات والتكنولوجيا. يجب تحديد سياسة (سياسـات) التعامل مع الحوادث والاســــتجابة لها ودعمها من خلال خطة وإجراءات وضوابط التعامل مع الحوادث والاســــتجابة لها، وذلك لكشـــف حوادث وهجمـات الـأمن الســـيبراني والـإبلاغ عنهـا والاســـتجابة لها واحتوائها والقضــاء عليهـا والتعافي منهـا.	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	تقوم أريـدُ بـإجراء تمـارين محـاكـاة مكتبيـة وتمارين الأمن السيبراني سنوياً للتعامل مع والاســــتجابة للحوادث الأمنية وذلك لاختبار وتقييم مــدى جــاهزيــة وإمكــانيــة فريق	5.12.3

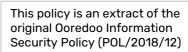






	detect, report, respond, contain,	الاســـتجابة للحوادث من الكشــف عن حوادث	
	eradicate and recover from cybersecurity incidents and attacks.	وهجمات الـأمن الســـيبراني والـإبلاغ عنهـا	
	moracine and accord.	والاســـتجابة لها واحتوائها والقضــاء عليها	
		والتعافي منها.	
5.12.4	Ooredoo shall establish a digital forensics investigation framework to ensure the	تقوم أريدُ بوضع إطار عمل للتحقيق الجنائي	5.12.4
	integrity of data during identification,	الرقمي وذلك لضـمان ســلامة البيانات أثناء	
	collection, examination, and analysis.	التحديد والجمع والفحص والتحليل.	
5.12.5	All suspected Personal Data breaches	يجب الإبلاغ عن جميع الانتهاكات المشــــتبه	5.12.5
	shall be reported to the Group Chief Legal, Regulatory & Governance Officer	بها للبيانات الشـخصـية إلى رئيس الشـؤون	
	(GCLRGO) or his delegate. Where the	القانونية والتنظيمية والحوكمة للمجموعة	
	GCLRGO determines that a Personal Data	أو من يفوضه. وعندما يحدد رئيس الشؤون	
	breach entails the possibility of material	القانونية والتنظيمية والحوكمة أن الانتهاك	
	damage to the Personal Data or privacy	للبيانات الشـخصـية يؤدي إلى إمكانية ضـرر	
	rights of affected individuals, Ooredoo Qatar shall notify the affected individuals	مادي على البيانات الشـــخصـــية أو حقوق	
	and the respective department at the	الخصوصية للأفراد المتأثرين، يجب على أريدُ	
	Ministry of Communication and	إبلاغ الأفراد المتأثرين والإدارة المعنية في	
	Information Technology.	وزارة الاتصالات وتكنولوجيا المعلومات.	
5.12.6	The CEO, Board and other relevant	يجب إبلاغ الرئيس التنفيذي ومجلس الإدارة	5.12.6
	entities as applicable shall be notified	والجهات المعنية الأخرى كلما انطبق ذلك	
	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	تحدد أريدُ الخطوات الواجب اتخاذها للتعامل	5.12.7
	it would take to address the impact of a data breach on its Customers.	مع تأثير انتهاك البيانات على العملاء.	

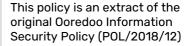






5.13.	Information Security Aspects in	جوانب أمن المعلومات في اســــتمرارية	5.13
	Business Continuity	الأعمال	
5.13.1	Ooredoo shall be committed to embed information security continuity in its business continuity management systems in compliance with the Business Continuity Management Policy.	تلتزم أريدُ بضمان استمرارية أمن المعلومات في أنظمة إدارة اســــتمرارية الأعمال بما يتوافق مع ســـياســـة إدارة اســـتمرارية 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 أريدُ بوضــع وتنفيذ و المحافظة على إجراءات وضوابط لضمان المستوى المطلوب من الـاســـتمراريــة لـأمن المعلومـات 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 أريدُ بالتحقق من ضــوابط اســتمرارية أمن المعلومات التي تم وضــعها وتنفيذها على فترات زمنية منتظمة، وذلك لضـــمان 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 cybersecurity laws, regulations and applicable international security standards.	تلتزم أريدٌ بوضــع وتنفيذ إجراءات مراقبة امتثال أمن المعلومات والمحافظة عليها، وذلك لضـــمان الالتزام بســـياســـات أمن المعلومــات وقوانين الــأمن الســـيبراني الوطنيـة واللوائح ومعـايير الـأمن الــدوليـة المعمول بها.	5.14.1
5.14.2	Ooredoo shall be committed to perform security audits, reviews, technical security assessments (i.e., penetration	تلتزم أريدُ بإجراء عمليات التدقيق الأمني والمراجعـات والتقييمـات الـأمنيــة التقنيــة (مثــل اختبــار الــاختراق وتقييم الثغرات)	5.14.2





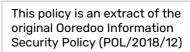


testing and vulnerability assessment) and compliance reviews at planned intervals or when a significant change occur to ensure security control effectiveness to mitigate the respective cybersecurity risks. The frequency of penetration testing and vulnerability assessment shall be defined by Ooredoo's Corporate Information Security team and any critical findings shall be reported to the CEO and the Board.

ومراجعات الامتثال في فترات زمنية مخطط لها أو عند حدوث تغيير هام، وذلك لضــمان فعالية الضوابط الأمنية للتخفيف من مخاطر الأمن الســيبراني ذات الصــلة. ويجب تحديد فترات إجراء اختبار الاختراق وتقييم الثغرات من قبل فريق أمن معلومات الشـركة، ويجب الــإبلاغ عن أي نتــائج حرجــة إلى الرئيس التنفيذي ومجلس الإدارة.

5.15.	Policy Enforcement	nent <u>تنفيذ السياسة</u>	
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 أريدُ واســــتشــــارييها والمتعاقدين معها والمتعاقدين من الباطن والموزعين والمردين مســــؤولين بشـــكــل مســــــقــل عن قراءة وفهم واتبــاع هــذه 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 أريدُ.	5.15.2
5.16.	Policy Amendment	<u>تعديل السياسة</u>	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 الســـياســـة كافة الإصـــدارات السـابقة (سـواء كانت سـياســة أو تعميماً أو مذكرات أو تعليمات أو أي شــــكل آخر) فيما يتعلق بموضوعها.	5.16.1

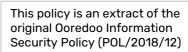






	Any change to the provisions of this policy shall be preliminarily reviewed and recommended by the Audit & Risk Management Committee (ARC) and finally approved by Ooredoo's Board of Directors. Any deviation on the implementation of this policy shall be approved by the Board of Directors.	أي تغيير على أحكام هذه السياسة يجب أن تتم مراجعته والتوصية به أولاً من قبل لجنة التـدقيق وإدارة المخـاطر (ARC) واعتمـاده بشكل نهائي من مجلس إدارة أريدُ. أي تغيير على تنفيذ هذه الســـياســـــــــــــــــــــــــــــــ	5.16.2 5.16.3
			4
6.	REFERENCES	المراجع	6.
	(Processes, Procedures, guidelines,	(الإجراءات، و العمليات، و التوجيهات و/أو	
	and/or any relevant document)	أية وثائق ذات صلة).	
6.1.	Identity and Access Management		6.1
	Policy	سياسة إدارة الهوية والوصول	
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.	Logging and Monitoring Policy	سياسة السجلات والمراقبة الأمنية	6.8
6.9.	Information Security Incident Management Policy	سياسة إدارة حوادث أمن المعلومات	6.9







6.10.	Protection of Personal Data Privacy	سياسة حماية خصوصية البيانات الشخصية	6.10
6.11.	(Law No. 13/2016)	(القانون رقم 13 لسنة 2016)	6.11
	Concerning Privacy and Protection of	,	
	Personal Data	بشأن حماية خصوصية البيانات الشخصية	
6.12.	Encryption Management Standard	معيار إدارة التشفير	6.12
6.13.	Business Continuity Management Policy	سياسة إدارة استمرارية الأعمال	6.13
6.14.	ISO 27001:2013 - Information	I SO 27001: 2013 – أمن المعلومــات –	6.14
	technology - Security techniques -	التقنيات الأمنية – ميثاق ممارســــة ضـــــوابط	
	Code of practice for information		
	security controls.	أمن المعلومات	
6.15.	Payment Card Industry Data Security	معيار أمن بيانات صـــناعة بطاقات الدفع	6.15
	Standard (PCI-DSS)	(PCI - DSS)	
		(1 cl - 255)	
6.16.	Qatar National Information Assurance	سياسة تأمين المعلومات الوطنية – النسخة	6.16
	(NIA) Policy v2.0	2. 0	
6.17.	Security Policy	سياسة الأمن	6.17
6.18.	Information Security Management	إ إجراءات إدارة أمن المعلومات	6.18
	Process		
6.19.	Enterprise Risk Management Process	إجراءات إدارة المخاطر	6.19
6.20.	Vulnerability Management Process	إجراءات إدارة الثغرات	6.20
	I I I I I I I I I I I I I I I I I I I		. 04
6.21.	User Access and Identity Management Process	إجراءات إدارة وصول وهوية المستخدم	6.21
6.22.	Control of Documented Information	9-4 11 - 1 1 - 1 1 - 1 1 - 1	6.22
0.22.	Process	إجراءات إدارة المعلومات الموثقة	J.22
	1 100000		





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

6.23.	HR policy	سياسة الموارد البشرية	6.23
6.24.	Law No. 14 of 2014 Promulgating the Cybercrime Prevention Law	القانون رقم 14 لســـنة 2014 بإصـــدار قانون مكافحة الجرائم الالكترونية	6.24
6.25.	Decree-Law No. 34 of 2006, Promulgating the Telecommunications Law	المرسوم بقانون رقم 34 لسنة 2006 بإصدار قانون الاتصالات	6.25
6.26.	Decree Law No 16 of 2010 Promulgating the Electronic Transactions and Commerce Law	المرسـوم بقانون رقم 16 لسـنة 2010 بإصـدار قانون المعاملات والتجارة الالكترونية	6.26

7. VERSION HISTORY

Version No.	Date	Approved by	Description of Change	Policy Reference
3	Nov 6, 2023	Senior Director Corporate Information Security & Government Affairs	Editorial Changes	POL/2018/12

