Information Security Policy – External Version

سياسة آمن المعلومات – النسخة الخارجية

1.	PURPOSE	الغرض	.1
1.1.	This Information Security policy is the primary component of the Company's Corporate Information Security Framework, which shall include a set of information security documentation consisting of policies, standards and procedures. The objective of the Ooredoo Information Security Policy is to ensure business resilience with appropriate levels of information security through preserving: • **Confidentiality –** where access to information/data shall be confined to those with appropriate authority. • **Integrity –** where information shall be complete and accurate. All information and information assets shall operate precisely/accurately, according to appropriate specifications. • **Availability –** where information shall be accessible and delivered to those authorized, at the time when it is needed.	تعد هذه السياسة المختصة بأمن المعلومات المكون الأساسي لإطار عمل نظام الأمن المعلوماتي في الشركة ، والذي يشتمل بالإضافة إليها على مجموعة من الوثائق الأخري تتضمن السياسات و المعايير و الإجراءات. وتهدف سياسة أمن معلومات Ooredoo إلى التأكد من تحقيق مرونة العمل مع المحافظة علي المستوي المطلوب لأمن المعلومات من خلال المحافظة على ما يلي: • **السرية**: من خلال حصر الوصول إلى المعلومات/ البيانات في الأشخاص و الجهات التي تمتلك الصلاحية المناسبة لذلك. • **السلامة**: من خلال ضمان أن تكون المعلومات مكتملة و دقيقة ، وأن تدار كافة المعلومات وأصول المعلومات وفقاً للمواصفات المطلوبة تماماً. • **التوفر:** من خلال توفير المعلومات وتقديمها إلى الأشخاص المصرح لهم وفي وقت الحاجة إليها.	1.1

	This policy covers all corporate information assets including but not limited to systems, applications and networks or any physical asset owned by the Company or operated by it.	تحكم هذه السياسة كافة أصول المعلومات بالشركة ، بما في ذلك دون حصر ، الأنظمة والتطبيقات والشبكات أو أي من الأصول االعينية التي تمتلكها الشركة أو تدار بواسطتها.	
2.	**SCOPE**	**المجال**	**.2**
2.1.	This policy applies to all 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 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 توجد	**3.1**
4.	**DEFINITION**	**التعريفات**	**.4**
In this policy, words and expressions shall have the meanings assigned to them, unless the context otherwise requires.		في تطبيق أحكام هذه السياسة، تكون للكلمات والعبارات التالية المعاني الموضحة قرين كل منها، ما لم يقتض السياق معنى آخر.	
4.1.	**The Company:** Ooredoo Q.P.S.C., a Qatari Public Shareholding Company (Ooredoo).	**الشركة:** Ooredoo ش.م.ق.ع.، شركة مساهمة قطرية عامة (Ooredoo).	**4.1**
4.2.	**Information Assets:** Knowledge or data that has value to the Company.	**الأصول المعلوماتية:** المعلومات أو البيانات ذات القيمة للشركة.	**4.2**
4.3.	**Information systems:**	**نظم المعلومات:**	**4.3**

	Includes, but shall not be limited to, applications, databases, operating systems, networks and security devices and any part of the Company's information technology infrastructure.	تشـتمل ، دون حصـر، علي التطبيقات وقواعد البيانات وأنظمة التشغيل والشبكات والأجهزة الأمنيـة و أي جزء من أجزاء البنيـة التحتيـة لتكنولوجيا المعلومات في الشركة.	
4.4.	**Threats:** Potential cause of an unwanted incident, which may result in harm to a system or the Company.	**التهديدات :** سـبب محتمل لحادث غير مرغوب فيه، والذي قد يتسبب في الضرر لأي نظام معلوماتي أو للشركة.	4.4
4.5.	**Vulnerabilities:** Weaknesses in an asset or control that can be exploited by one or more threats.	**الثغرات:** وهي أي نقاط ضـعف في أي أصـل معلوماتي أو في نظام تحكم يمكن اسـتغلالها لتوجيه تهديد أو أكثر.	4.5
4.6.	**Networks:** Includes the telecommunications and any information technology networks owned by the Company or operated by it.	**الشبكات:** تتضـمن شـبكات الاتصـالات و أي تكنلوجيا معلومات مملوكة للشركة أو تدار بواسطتها.	4.6
5.	**Policy Statement**	**بيان السياسة**	**.5**
5.1.	Ooredoo Information Security Policies are mandatory and shall be complied with by all 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.	إن سـياسـات أمن معلومات Ooredoo إلزامية، ويجـب التقيـد بهـا من قبـل جميع موظفي الشـركـة والاسـتشـاريين والمتعـاقـدين والمتعاقدين من الباطن والموردين والموزعين و موظفيهم و أي شـخص تم تزويده بصـلاحية الوصـول إلى المعلومات أو أصـول المعلومات التي تمتلكها Ooredoo أو تدار بواسطتها.	5.1
5.2.	Information Security Risk management shall be used to identify threats, vulnerabilities, probability and impact to the Company's information assets.	تسـتخدم إدارة مخاطر أمن المعلومات لتحديد التهديدات والثغرات واحتمالية ومدى تأثر أصـول معلومات الشركة.	5.2

5.3.	Information Security controls and countermeasures shall be implemented based on risks and value of the information.	تطبق وسائل التحكم و الإجراءات الاحترازية وفقاً للمخاطر وقيمة المعلومات.	**5.3**
5.4.	Information Security requirements shall be adopted and deployed within all information systems and processes in the Company.	يتم تبني وتطبيق متطلبات أمن المعلومات في جميع أنظمة المعلومات والعمليات في الشركة.	**5.4**
5.5.	Information Security Awareness Programs and campaigns shall be conducted to ensure all stakeholders are aware of Ooredoo Information Security policies, standards and procedures.	توضع وتنفذ برامج وحملات التعريف بأمن المعلومات، وذلك للتأكد من إطلاع جميع المستفيدين وأصحاب المصلحة على سياسات ومعايير وإجراءات أمن معلومات Ooredoo .	**5.5**
5.6.	**RESPONSIBILITIES**	**المسؤوليات**	**5.6**
5.6.1.	The ultimate responsibility for Information Security in the Company rests with the respective Business Unit Chief Officer.	تقع المسؤولية النهائية عن أمن المعلومات في الشركة على عاتق رئيس الإدارة المختص.	**5.6.1**
5.6.2.	Each Business Unit line manager is responsible for ensuring that their respective permanent and temporary staff under him/her are aware of: • The information security policies applicable in their work areas. • Their personal responsibilities for information security in the Company. • Channels for approaching the Corporate Information Security team on information security related matters.	يكون المدير المباشر مسؤولاً عن التأكد من أن موظفيه الدائمين والمؤقتين والمتعاقدين على دراية بما يلي: • سياسات أمن المعلومات المعمول بها في مجالات عملهم. • مسؤولياتهم الشخصية عن أمن المعلومات بالشركة. • قنوات التواصل مع فريق أمن معلومات الشركة بخصوص المسائل المتعلقة بأمن المعلومات.	**5.6.2**
5.6.3.	All persons working for the Company, including Company employees, consultants, contractors, sub-contractors,	يكون كافة الأفراد العاملين لدي الشركة، سواء موظفي الشركة أو الاستشاريين والمتعاقدين والمتعاقدين من الباطن والموردين والموزعين	**5.6.3**

	vendors, suppliers and their employees and anyone who has been provided access to information or information assets owned by the Company or operated by it are responsible for adhering to all applicable Information Security policies.	و موظفيهم و أي شخص تم تزويده بصلاحية الوصول إلى المعلومات أو أصول المعلومات التي تمتلكها الشركة أو تدار بواسطتها ، مسؤولين عن الالتزام بكافة سياسات أمن المعلومات المنطبقة للشركة.	
5.6.4.	The Corporate Information Security department shall be responsible for ensuring the establishment, maintenance and ongoing improvement of the Information Security Framework for the Company. This includes: 1) Establishment, maintenance and improvement of Information Security infrastructure, policies, standards, processes. 2) Managing the Information Security risk assessment program (risks to Confidentiality, Integrity and Availability of information) 3) Managing and performing Information Security assessments for the Company's information systems. 4) Launching, maintaining and improving Information Security awareness programs for the Company's employees and consultants. 5) Establishing Information Security incident response teams and reporting lines 6) Ensuring compliance to local government and legal and	تكون إدارة آمن معلومات الشركة مسؤولة عن التأكد من تأسيس إطار عمل لأمن المعلومات خاص بالشركة وصيانته وإجراء التحسينات المستمرة عليه و ذلك يشمل على: 1) وضع البنية التحتية والسياسات والمعايير وإجراءات عمليات أمن المعلومات والمحافظة عليها وتطويرها. 2) إدارة برنامج تقييم مخاطر أمن المعلومات (المخاطر المتعلقة بسرية المعلومات وسلامتها وتوفرها). 3) تنظيم و إدارة عمليات تقييم أمن المعلومات لأنظمة الشركة المعلوماتية. 4) وضع برامج التعريف والتوعية بأمن المعلومات لموظفي الشركة و مستشاريها والمحافظة عليها وتطويرها. 5) تشكيل فرق للتعامل مع الحوادث الخاصة بأمن المعلومات و التبليغ بشأنها.	5.6.4

	regulatory frameworks for Information Security requirements.	٦) ضـمان التوافق مع المتطلبات الحكومية و الأطر القـانونيـة والتنظيميـة المحليـة الخاصة بأمن المعلومات.	
5.7.	**PROCEDURES**	**الإجراءات**	**5.7**
5.7.1.	The Corporate Information Security department shall establish the needful processes and procedures to implement this policy.	تضع إدارة أمن المعلومات الإجراءات والعمليات اللازمة لتنفيذ هذه السياسة.	**5.7.1**
5.8.	**Policy Enforcement**	**تنفيذ السياسة**	**5.8**
5.8.1.	All Ooredoo employees are independently responsible for reading, understanding and following the Information Security Policy.	يكون كـل موظف من موظفي Ooredoo مسـؤولاً بشـكل مسـتقل عن قراءة وفهم واتباع سياسة أمن المعلومات.	**5.8.1**
5.8.2.	Each employee is also obliged to speak up and raise concerns about actual or possible violations to the Corporate information Security Department.	ويلتزم كل موظف بإبلاغ إدارة أمن معلومات الشركة بوجود أي انتهاكات فعلية أو محتملة.	**5.8.2**
5.8.3.	Any violation of this Policy by any of the Company employees shall entail disciplinary action under the relevant Ooredoo policy.	سـيترتب علي أي إنتهاك لهذه السـياسـة من جـانـب أي من موظفي الشـركـة الإحـالـة للإجراءات التأديبية وفقاً للسـياسـة المعمول بها في Ooredoo.	**5.8.3**
5.9.	**<u>Policy Amendment and exception</u>**	**<u>تعديل واستثناءات السياسة</u>**	**5.9**
5.9.1.	This policy supersedes all previous releases (policy, circular, memos, instructions or any other form) on its subject-matter.	تلغي هذه السـياسـة و تسـود علي كافة الإصـدارات السـابقة (سـواء كانت سـياسـة أو تعميماً أو مذكرات أو تعليمات أو أي شكل آخر) فيما يتعلق بموضوعها.	**5.9.1**
5.9.2.	Any change to the provisions of this policy shall be reviewed, and approved by the Chief Executive Officer.	أية تغيير على أحكام هذه السـياسـة يجب أن تتم مراجعتـه واعتمـاده من الرئيس التنفيـذي للشركة.	**5.9.2**

6.	REFERENCES (Procedures, guidelines, and/or any relevant document)	المراجع (الإجراءات، التوجيهات و/أو أية وثائق ذات صلة).	.6
6.1.	**Procedures/Guidelines**	**الإجراءات /التوجيهات**	6.1
6.1.1.	Vulnerability E2E Process	الإجراءات المتكاملة لمعالجة الثغرات.	6.1.1
6.1.2.	IT Infrastructure Setup Process	إجراءات تركيب انظمة تكنلوجيا المعلومات.	6.1.2
6.1.3.	Telecom/Data Center Sites Installation and Cabling E2E Process	الإجراءات المتكاملة لتركيب الأعمال و تمديد الكيابل بمواقع الإتصالات و مراكز المعلومات.	6.1.3
6.1.4.	Enterprise Risk Management Methodology Process	القواعد الإجرائية لإدارة المخاطر التجارية.	6.1.4
6.1.5.	Technology Change Management & Planned Activity Process	إجراءات إدارة التغييرات التكنلوجية المخطط لها و غير المخطط لها.	6.1.5
6.1.6.	Incident Management Process	إجراءات إدارة الحوادث.	6.1.6
6.2.	**Relevant Documents**	**الوثائق ذات الصلة**	6.2
6.2.1.	Acceptable Use Policy	سياسات الاستخدام المقبول	6.2.1
6.2.2.	Ani-Malware Policy	سياسة الحماية من البرمجيات الضارة	6.2.2
6.2.3.	Clear Screen Desk Policy	سياسة سرية المعلومات في المكاتب وأجهزة الكمبيوتر	6.2.3
6.2.4.	Encryption Policy	سياسة التشفير	6.2.4
6.2.5.	Enterprise Wireless Policy	سياسة الاتصال بالشبكة اللاسلكية	6.2.5
6.2.6.	Identity and Access Management Policy	سياسة إدارة الهوية والوصول إلى المعلومات	6.2.6
6.2.7.	Information Security Incident Management Policy	سياسة إدارة حوادث أمن المعلومات	6.2.7

6.2.8.	Information Classification Policy	سياسة تصنيف المعلومات	**6.2.8**
6.2.9.	Information Management Policy	سياسة إدارة المعلومات	**6.2.9**
6.2.10.	Mobile Computing Policy	سياسة الأجهزة المحمولة	**6.2.10**
6.2.11.	Network Security Policy	سياسة امن الشبكات	**6.2.11**
6.2.12.	Vulnerability Management Policy	سياسة إدارة وتقييم الثغرات	**6.2.12**
6.2.13.	Protection of Personal Data Privacy Policy	حماية خصوصية البيانات الشخصية	**6.2.13**

7. VERSION HISTORY

Version No.	Date	Approved by	Policy Reference
2	Apr 11, 2018	CEO	This policy is an extract of the Information Security Policy (reference POL/2018/12)