الموضوع/ الضوابط الأساسية للأمن السيبرانى
Essential Cybersecurity Controls

1. CYBER SECURITY	1. الأمن السيبراني
1.1 DEFINITION OF CYBER SECURITY	**1.1 تعريف الأمن السيبرانى**
Cyber security is defined as the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance, and technologies that can be used to protect the member organization's information assets against internal and external threats.	الأمن السيبرانى هو الذي يُعنى بتطبيق التقنيات، والعمليات، والضوابط؛ بهدف حماية الأنظمة، وشبكات الحواسيب، والبرامج، والأجهزة، والبيانات من التعرض للهجمات الإلكترونية الداخلية والخارجية. ويشمل أيضا على مجموع الوسائل التقنية والتنظيمية والادارية التي يتم استخدامها لمنع الاستخدام الغير مصرح به وسوء الاستغلال واستعادة المعلومات الالكترونية ونظم الاتصالات والمعلومات التي تحتويها وذلك بهدف ضمان توافر واستمرارية عمل نظم المعلومات وتعزيز حماية وسرية وخصوصية البيانات الشخصية واتخاذ جميع التدابير اللازمة لحمايتها.
1.2 COMPLIANCE WITH THE CYBERSECURITY LAW OF KUWAIT	**1.2 الامتثال لقانون الأمن السيبرانى لدولة الكويت**
Contractor and Contractor's employees and Subcontractors and employees of Subcontractors shall comply with the Cybersecurity Law of the State of Kuwait.	يجب على المقاول وموظفي المقاول والمقاولين من الباطن وموظفي المقاولين من الباطن الامتثال لقانون الأمن السيبراني لدولة الكويت.
1.3 COMPLIANCE WITH CYBERSECURITY POLICY	**1.3 الامتثال لسياسة الأمن السيبراني**
Contractor and its Sub-Contractors and all employees working under the contract shall comply with the Company's Security policies, procedures, and Cyber Security Checklist Quality Assurance Template for Contracts/ Projects.	يجب على المقاول والمقاولين من الباطن وجميع الموظفين العاملين بموجب العقد الامتثال لسياسة الأمن السيبراني للشركة ونموذج ضمان الجودة لقائمة مراجعة الأمن السيبراني للعقود / المشاريع.
1.4 EMERGING THREATS	**1.4 التهديدات الناشئة**

Contractor shall continuously align with emerging threats and make sure that the highlighted risks will not affect PIC. If there are any risks emerging, Contractor shall raise the issue as per Service Level Agreement time allocations.	يجب على المقاول المواءمة باستمرار مع التهديدات الناشئة والتأكد من أن المخاطر لن تؤثر على الشركة. في حال ظهور أي مخاطر تؤثر على الشركة، يجب على المقاول ابلاغ الشركة وفقا لتخصيصات الوقت في اتفاقية مستوى الخدمة.
1.5 ACCESS CONTROL	**1.5 التحكم بالولوج والصلاحيات**
Contractor shall limit information system access to authorized users and only to the types of transactions that authorized users are permitted to execute. Written approval shall be acquired for access.	يلتزم المقاول بضمان حماية الولوج إلى الأصول المعلوماتية والتقنية للشركة، ومنع الولوج غير المصرح به والتقييد بما هو مطلوب فقط لإنجاز الأعمال المتعلقة بالشركة. يلتزم المقاول بالحصول على موافقة خطية للولوج الى الأنظمة.
1.6 AWARENESS AND TRAINING	**1.6 التوعية والتدريب بالأمن السيبرانى**
The Contractor shall ensure that the Contractor's employees are aware of the Information and Operations Security risks associated with their activities related to the security of Information assets and Information/Operations systems covered in the contract. Further, the Contractor shall ensure that its employees are adequately trained to carry out their assigned Information / Operations Security related duties and responsibilities. Evidence of training/awareness and risk assessment shall be submitted prior to commencement.	يجب على المقاول التأكد من أن موظفي المقاول على دراية بمخاطر أمن المعلومات والعمليات المرتبطة بأنشطتهم المتعلقة بأمن أصول المعلومات وأنظمة المعلومات / العمليات المشمولة في العقد. علاوة على ذلك، يجب على المقاول التأكد من أن موظفيه مدربين تدريباً كافياً لتنفيذ الواجبات والمسؤوليات المتعلقة بأمن المعلومات / العمليات. على المقاول تسليم بيانات التدريب أو التوعية التي تمت مع دليل المخاطر المتعلقة بالمشروع قبل البدء بالأعمال.
1.7 AUDIT AND ACCOUNTABILITY	**1.7 المسؤولية والتدقيق الدوري للأمن السيبرانى**

The Contractor shall conduct periodic Internal Cybersecurity Audits upon request by the Company's Contract Supervisor, in areas and systems related to the contract. The contractor is responsible to address and resolve all the findings and the relevant vulnerabilities with no additional cost. Failing to rectify the findings within a stipulated period based on the Company Service Level Agreement, the Company has the right to seek security services from qualified partners to take the necessary actions to close the findings in its environment. Cost of this activity shall be retained by the Contractor or shall be deducted from any dues the Contractor has with the company. No Claim by the contractor for any consequent additional costs.	يجب على المقاول إجراء عمليات تدقيق داخلية دورية للأمن السيبراني في المجالات والأنظمة المتعلقة بالعقد بناءً على طلب مشرف العقد. المقاول مسؤول عن معالجة وإصلاح نقاط الضعف ذات الصلة بعمليات التدقيق الداخلية للأمن السيبرانى والتي أبلغ عنها المشرف على عقد الشركة. في حالة فشل المقاول أو تعثره في معالجة وإصلاح نقاط الضعف في خلال فترة زمنية مناسبة، يحق للشركة طلب خدمات أمنية من شركاء مؤهلين لاتخاذ الإجراءات اللازمة لإغلاق جميع نتائج التدقيق ونقاط الضعف وعلى المقاول تحمل مسؤولية الالتزام بدفع مستحقات وفواتير الخدمات المقدمة من الشركات والشركاء المؤهلين بدون أي تأخير أو خصمها من اية استحقاقات لدى الشركة لسدادها. ولا تلتزم الشركة أو أي من تابعيها بدفع أي مبالغ للمقاول.
1.8 CYBERSECURITY BREACHES & INCIDENT RESPONSE	**1.8 اختراقات الأمن السيبراني والاستجابة لحوادث وتهديدات الأمن السيبرانى**
The Contractor shall notify the Contract Supervisor of any Cybersecurity breach or incident or finding within the Service Level Agreement time allocations.	يجب على المقاول إخطار ممثل الشركة أو المشرف على العقد عن أي محاولة لاختراق الأمن السيبرانى أو أنظمة الحماية الخاصة بها خلال الفترات المحددة في جدول الخدمات SLA.
1.9 MEDIA PROTECTION	**1.9 حماية الوسائط**

The Contractor shall protect (i.e., physically control and securely store) information system media containing the Company's Information, both paper and digital. Further, the Contractor shall limit access to the Company's information system media to authorized users, sanitize or destroy information system media containing Company's information before disposal or release for reuse subject to the approval of the Company's representative. Validation of the activity shall be submitted to the Contract Supervisor.	يجب على المقاول حماية (أي التحكم المادي والتخزين الآمن) لوسائط نظام المعلومات التي تحتوي على معلومات الشركة، الورقية والرقمية. كما يجب على المقاول تقييد الوصول إلى وسائط نظم معلومات الشركة للمستخدمين المصرح لهم فقط، وتعقيم أو تدمير وسائط نظام المعلومات التي تحتوي على معلومات الشركة قبل التخلص منها أو الإفراج عنها لإعادة استخدامها بشرط موافقة ممثل الشركة. يجب على المقاول تسليم وثائق تأكد صحة النشاط الى مشرف العقد.
1.10 PATCH MANAGEMENT	**1.10 حزم التحديثات والإصلاحات**
The Contractor shall ensure that all the patches, fixes and updates once released by their respective. Vendors are tested and installed on the systems covered in the scope of the contract, without any additional cost. All installation of patches, fixes and upgrades require Company's pre-approvals.	يجب على المقاول التأكد من أن جميع التصحيحات والإصلاحات والتحديثات الأمنية بمجرد إصدارها من قبل البائعين المعنيين يتم اختبارها وتثبيتها على الأنظمة التي يغطيها نطاق العقد، دون أي تكلفة إضافية. كما تتطلب جميع عمليات تثبيت التصحيحات والإصلاحات والترقيات الى موافقات الشركة المسبقة.
1.11 WORK STOPPAGE	**1.11 إيقاف العمل**
The Company's Representative may stop Contractor's work, or a part of the Contractor's work if it is seen as crossing beyond the Company's Risk acceptance threshold or violating Company's Information Security Policy or the Cybersecurity Laws of the State of Kuwait.	يجوز لممثل الشركة إيقاف عمل المقاول، أو جزء من عمل المقاول إذا كان يُنظر إليه على أنه يتجاوز حد قبول المخاطر للشركة أو ينتهك سياسة أمن معلومات الشركة أو قوانين الأمن السيبراني لدولة الكويت.