KUWAIT NATIONAL PETROLEUM COMPANY (K.S.C)

CYBERSECURITY GUIDELINES FOR CONTRACTORS

		Signature	Date
Author	**Syed M. Rabbani,** Systems Analyst, Risk & Compliance		
Reviewers	**Abdulmajeed Al-Sabah,** Project Head, Risk & Compliance **Husain Al-Bustan,** Team Leader, Information Security		
Approver	**Naji Saleh Al-Marri** Manager, Information Technology	Signed digitally through the covering memo	As per the covering memo
Document Custodian: Information Technology Department			

Effective from: 31-Jan-2021 Next Revision Date: 31-Jan-2022	Document Reference: As on the Covering Memo Version 2.1

Version Control

Version	DATE	DESCRIPTION
1.0	18-Feb-2018	• Issued for Commercial Dept. to incorporate in Model Tender documents
2.0	16-July-2020	• Issued for Commercial Dept. to incorporate in Model Tender documents
2.1	17-Jan-2021	• Incorporated Legal department's comments • Issued for Commercial Dept. to incorporate in Model Tender documents

CONTENTS

CYBERSECURITY GUIDELINES FOR CONTRACTORS

1. INTRODUCTION:

Kuwait National Petroleum Company (hereinafter referred to as Company) runs a comprehensive Information Security Management System (ISMS) for its commitment to protecting the confidentiality, integrity and availability of its information and/or operations assets.

This document outlines the minimum Cybersecurity requirements for the Company, where its Contractors are required to comply with. Contractor, herein, shall mean an entity with whom the Company has entered into a contract / agreement / purchase order and shall include within its definitions, without limitation, all its contractors, consultants, suppliers and vendors.

Contractor and the Contractor's employees, shall make themselves familiar with these Guidelines prior to commencing any contracted work.

2. SCOPE AND APPLICATION:

Scope of these Guidelines is enterprise-wide, for all types of contracts.

This document is a generic guideline that shall apply to all types/classifications of contracts within the Company. It shall form part of every tender document, including Loaned Personnel Agreements.

Contractor is responsible for compliance with these Guidelines, the Contract Terms and Conditions, and Information security Laws of the State of Kuwait. All references to Contractor and Contractor employees shall equally apply to Subcontractors and Subcontractor's employees. Contractor shall ensure that Subcontractors are informed and comply with all aspects of these guidelines.

These Guidelines supplement and shall not supersede the Contract's terms and conditions. If there is a requirement for more information on a particular subject, Contractor should contact the Company Representative.

Following the requirements mentioned in this document shall not guarantee compliance with all applicable legal and regulatory requirements of the contract. Compliance with all applicable requirements of the contract is the sole responsibility of the Contractor.

3. COMPLIANCE WITH THE CYBERSECURITY LAW OF KUWAIT:

Contractor, and Contractor's employees, Subcontractors and employees of Subcontractors shall comply with the Cybersecurity Laws of the State of Kuwait.

4. INFORMATION RISK ASSESSMENT:

Contractor shall ensure that the Information Security risk assessment for the Company' assets covered in the scope of contract is conducted before mobilization and the results are communicated and understood by all parties prior to starting the execution of contract.

Unless otherwise agreed with Company's user department, the Contractor shall conduct periodic information security risks assessments for the Company's assets covered in the scope of contract, identifying the risks, implementing necessary controls and evaluating effectiveness of these controls.

5. ACCESS CONTROL:

Contractor shall only limit access to the Company's information/operations system to authorized users and to the extent permitted as per scope of the contract.

6. AWARENESS AND TRAINING:

The Contractor shall ensure that the Contractor's employees are aware of the Information and Operations Security risks associated with their activities related to 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. In addition, the Contractor's employees are obligated to attend Cybersecurity Awareness Sessions conducted by the Company from time to time.

7. ACCOUNTABILITY AND AUDIT:

Unless otherwise agreed with Company's user department, the Contractor is accountable of monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information/operations system activity in the areas and systems under the scope of contract. The contractor is responsible to address and resolve all the findings reported by the Company's internal or external Audit.

8. CYBERSECURITY BREACH NOTIFICATION:

The Contractor shall notify the Company's Representative of any Cybersecurity incident or breach within 4 hours of its knowledge.

9. IDENTIFICATION AND AUTHENTICATION:

The Contractor shall identify all information/operations system users, processes, and devices and validate (or verify) their identities as a prerequisite before allowing access to the Company's information/operations systems covered within the contract.

10. INCIDENT RESPONSE:

The Contractor shall establish a cybersecurity incident handling capability for the Systems covered under the contract and align with the Company's existing incident response process. Further, the Contractor shall track, document, and report incidents in line with the Company's existing processes.

11. MEDIA PROTECTION:

The Contractor shall protect (i.e., physically control and securely store) information system media containing Company's data, in hard and soft format. Further, the Contractor shall limit access to Company's information system media to authorized users only. The Contractor shall destroy information system media containing Company's information before disposal or release for reuse.

12. PATCH MANAGEMENT:

Contractor shall ensure that software patches, fixes and updates once released by their respective Vendors are tested and installed on the systems under the contract, at no additional cost. Installation of patches, fixes and updates shall require Company's prior approval.

13. PERSONNEL SECURITY:

The Contractor shall screen individuals prior to authorizing access to information and/or operations systems within the Company. Contractor shall ensure that Company's sensitive information remains protected during and after personnel actions; such as terminations and transfers of its contractors. Further, the Contractor shall keep the Company informed of all personnel actions (terminations and transfers) and security clearances.

14. PHYSICAL PROTECTION:

The Contractor shall limit physical access to the Company's information and/or operations systems, equipment, and the respective operating environments to authorized individuals. Further, the Contractor shall protect and monitor the physical facility and support infrastructure for the systems covered in the contract.

15. SYSTEM AND COMMUNICATIONS PROTECTION:

The Contractor shall monitor, control, and protect the Company's communications (i.e., information transmitted or received by the Company's information and/or operations systems) at the external boundaries and key internal boundaries of the information and/or operations systems within the scope of contract. Further, the Contractor shall employ architectural designs, software development techniques, and systems engineering principles that promote effective Information and/or operations Security within the systems in the scope of contract.

16. SYSTEM AND INFORMATION INTEGRITY:

The Contractor shall identify, report, and correct information and information and/or operations system flaws in a timely manner. Further, the Contractor shall provide protection from malicious code within the systems in the scope of the contract and monitor information and/or operations system security alerts and advisories, and take appropriate actions in response to ensure systems integrity.

17. WORK STOPPAGE:

The Company's Representative may stop Contractor's work, or a part of the work, if the execution of the contract puts the Company under information/operations security risk or violates Information security/Cybersecurity Laws of the State of Kuwait.

18. CYBERSECURITY RISKS DURING DEMOBILIZATION:

The Contractor shall follow all cybersecurity procedures and measures during demobilization. Contractor shall reassess Cybersecurity risks associated with demobilization, and shall address any new risks identified. Contractor shall provide the Company with necessary assurance that appropriate resources covered within the contract shall remain intact until the completion of all associated activities.

19. PARTICIPATION IN ANY CYBERSECURITY EMERGENCY:

In case of any Cybersecurity Emergency related to the scope of the contract, the Contractor is obliged to participate with the Company's personnel at the Company's discretion during the crisis and recovering phase of any disasters, at no additional cost to the Company.

20. PENALTY FOR NON-COMPLIANCE TO THESE GUIDELINES:

Non-compliance to any of these Cybersecurity Guidelines shall result in a penalty of up to 10% of the contract value, at the discretion of the Company. Penalties shall commensurate with the severity of violation as per the following table.

	Violation	Reference Section the Cybersecurity Guidelines	Penalty to be levied on the contractor
1.	Violation of Kuwait Cybersecurity Law	3	2%
2.	Violation of Access Control	4, 9, 13, 14, 15, 18	1%
3.	Failure to complete periodic risk assessment of assets (in the scope of contract) as required by Company.	5	0.5%
4.	Failure to achieve 90% of staff completing the annual cybersecurity training objective set by the Company.	6	0.5%
5.	Failure to resolve the Cybersecurity Audit findings in time.	7	1%
6.	Failure to report any Cybersecurity breach related to assets in the scope of contract within 4 hours.	8	2%
7.	Failure to resolve the Cybersecurity incidents (related to assets in the scope of contract) within 8 hours of their reporting.	10	0.5%
8.	Failure to purge the information on the media (associated with the assets in the scope of contract) before its disposal.	11	0.5%
9.	Failure to apply patches within the duration set by company, for the assets in the scope of contract.	12	0.5%
10.	Failure to ensure integrity of information in the assets in scope of contract.	16	0.5%
11.	Failure to participate in the Cybersecurity emergency, when called by the Company either during the crisis or during the post-crisis recovery phases.	19	1%

Non-Disclosure Agreement

This Non-Disclosure Agreement (the "Agreement") is made on the _____ day of _____ 20___ between Kuwait National Petroleum Company having its Head Office located at Al-Ahmadi city, P.O. Box 70, Safat 13001, State of Kuwait ("**KNPC**") and _____, having its principal office located at _____ ("**Receiving Party**") for the purpose of preventing the unauthorized disclosure of KNPC's Confidential Information (hereinafter defined).

1. **"KNPC's Confidential Information"** shall mean all information disclosed by KNPC to the Receiving Party for carrying out the Purpose (hereinafter defined) whether or not reduced to or designated in writing or in electronic form including, without limitation, ideas, patents, inventions, technology, processes, formulations, methods, plans, trade secrets, licenses, know-how, drawings, products, programs, strategies, forecasts, financial data, discoveries, techniques, specifications, designs, employee data, identity of vendors, suppliers, customers, contractors, consultants, and licensees.

2. "**Purpose**" shall mean the purpose for which KNPC's Confidential Information is disclosed to the Receiving Party, namely, Contract No. XX/XXXX, TITLE…….. (FILL IN THE PURPOSE).

3. **Exclusions from KNPC's Confidential Information**: Receiving Party's obligations under this Agreement do not extend to information that is: (a) publicly known at the time of disclosure or subsequently becomes publicly known through no fault of the Receiving Party; (b) independently developed by the Receiving Party prior to disclosure by KNPC; (c) disclosed through legitimate means to the Receiving Party by a third party who did not obtain such KNPC's Confidential Information, directly or indirectly, from KNPC under an obligation of secrecy or confidentiality; or (d) is disclosed by Receiving Party with KNPC' s prior written approval.

   An individual feature of the Disclosing Party's Confidential Information shall not be considered within the above exceptions merely because the feature is embraced by more general information within the exceptions. A combination of features of the Receiving Party's Confidential Information shall not be considered within the above exceptions unless the combination itself and its principle of operation are within the exceptions.

4. **Obligations of Receiving Party**: Receiving Party shall hold and maintain KNPC's Confidential Information in strictest confidence for the sole and

exclusive benefit of KNPC. Receiving Party or any other entity or person acting through it shall not use KNPC's Confidential Information outside the requirements of the Purpose. Receiving Party shall restrict access to KNPC's Confidential Information solely to those employees of the Receiving Party who reasonably require KNPC's Confidential Information to carry out the Purpose and shall require those persons to sign nondisclosure restrictions at least as protective as those in this Agreement. Receiving Party shall not, without prior written approval of KNPC, use for Receiving Party 's own benefit, publish, copy, or otherwise disclose to others, or permit the use by others for their benefit or to the detriment of KNPC, any KNPC 's Confidential Information. Receiving Party shall return to KNPC any and all records, notes, and other written, printed, or tangible materials in its possession pertaining to KNPC 's Confidential Information immediately upon completion of the Purpose or when KNPC requests in writing its return.

5. **Compelled Disclosure**: If Receiving Party is required by applicable law or valid legal order by an applicable court or government authority to disclose any KNPC Confidential Information other than as permitted in this Agreement, then Receiving Party shall (a) provide prompt written notice to KNPC, so that KNPC may timely seek a protective order or other remedy; and (b) upon request, provide reasonable assistance to KNPC at no cost to support efforts to contest or limit the scope of such disclosure requirement. If, thereafter, Receiving Party remains legally compelled to make such disclosure, then Receiving Party shall (a) only disclose that portion of KNPC Confidential Information as is necessary to comply with such law, court order, or government requirement; (b) only disclose such KNPC Confidential Information to the entities such law, court order, or government authority requires; and (c) use reasonable efforts to ensure that such KNPC Confidential Information is afforded any permissible confidential treatment.

6. **Duration**: The nondisclosure provisions this Agreement shall survive the termination of this Agreement and Receiving Party's obligation to hold KNPC's Confidential Information in confidence shall remain in effect.

7. **Relationships**: Nothing contained in this Agreement shall be deemed by the parties or any third party as constituting for any purpose any relationship of principal and agent, employer and employee, partnership or joint venture between KNPC and Receiving Party.

8. **Representations & Warranties**: KNPC makes no express or implied representation or warranties with respect to KNPC's Confidential Information disclosed hereunder including any representation or warranties as to the

accuracy, reliability, completeness, or fitness for a particular purpose. It is further understood and agreed that neither KNPC nor its representatives shall have any responsibility to the Receiving Party or to any other person or entity resulting from the use of any KNPC's Confidential Information so furnished or otherwise provided.

9. **Grant of License**: KNPC's Confidential Information shall remain the sole property of KNPC and the furnishing of any KNPC's Confidential Information hereunder shall not be construed as the granting of a license under any patent, patent application, copyright, copyright registration, trademarks, trade secret, or other proprietary right by KNPC to any person or entity or as implying any right or obligation other than that is specifically stated herein.

10. **Conflict of Interest**: Conflict of interest relating to this Agreement is strictly prohibited and occurrence of any such conflict or anticipated conflict, whether existing prior to or during the period of this Agreement shall immediately be notified to KNPC. In the event of any conflict of interest, anticipated or otherwise, the Receiving Party shall not seek the KNPC's Confidential Information required, or if already obtained, immediately cease using the same and return the same to KNPC. Conflict of interest includes, among others, a situation, actual or anticipated, in which the Receiving Party or any entity or person acting in concert with it is in a position to use the KNPC's Confidential Information outside the requirements of the Purpose to the prejudice or detriment of the business or best interests of KNPC.

11. **Applicable Law**: This Agreement and all matters collateral hereto shall be governed by the laws of the State of Kuwait and the parties hereto submit to the exclusive jurisdiction of the courts of Kuwait.

12. **Severability**: If a court finds any provision of this Agreement invalid or unenforceable, the remainder of this Agreement shall be interpreted so as best to reflect the intent of the parties.

13. **Entire Agreement**: This Agreement expresses the complete understanding of the parties with respect to the subject matter and supersedes all prior proposals, agreements, representations, and understandings. No amendment to this Agreement shall be valid unless reduced to writing and signed by both parties.

14. **Waiver**: The failure to exercise any right provided in this Agreement shall not be a waiver of prior or subsequent rights. This Agreement and each party's obligations shall be binding on the representatives, assigns and successors of such party.

In Witness Whereof, the parties hereto have caused this Agreement to be duly executed through their authorized representatives on the date first above written.

On behalf of:	**On behalf of:**
KNPC	**Receiving party**
Name: *(*See Note below)*	Name:
Title:	Title:
Date: / /	Date: / /
Signature: _____	Signature: _____

**Note : Company's Superintendent of Contract will sign this NDA on KNPC's behalf*