SUEZ WATER TECHNOLOGIES & SOLUTIONS

Product Cybersecurity Appendix

This Appendix governs whenever a Supplier Processes Suez Data or has access to a Suez Information System in connection with the relevant agreement, contract, statement of work, task order, purchase order or other document governing the provision of services and/or deliverables by Supplier to Suez (Contract Document). In the event of any inconsistency or conflict between this Appendix and the Contract Document with respect to a subject covered by this Appendix, the provision requiring the higher level of protection for Suez Data shall prevail. The requirements in this Appendix are in addition to any confidentiality obligations between Suez and the Supplier under the Contract Document. Suez or the applicable Suez Affiliate owning any of the Suez Data being accessed pursuant to the Contract Document may enforce the terms of this Appendix.

Part A: Definitions

Any words following the terms "including," "include," "e.g.," "for example" or any similar expression are for illustration purposes only.

(i) Controlled Data is technical or government information with distribution and/or handling requirements proscribed by law, including but not limited to controlled unclassified information and license required export controlled data. Controlled Data shall be subject to the controls below for Suez Restricted Data.

(ii) Highly Privileged Accounts, or HPAs, are accounts with system level administrative or super-user access to devices, applications or databases, administration of accounts and passwords on a system, or ability to override system or application controls.

(iii) Mobile Devices means tablets, smartphones and similar devices running mobile operating systems. Laptops are not considered Mobile Devices.

(iv) Personal Data includes any information that relates to an identified or identifiable natural person (Data Subject), as defined under applicable law. Legal entities are Data Subjects where required by law.

(v) Process(ing) means to perform any operation or set of operations upon Suez Data, whether or not by automatic means, including but not limited to, collecting, recording, organizing, storing, adapting or altering, retrieving, accessing, consulting, using, disclosing by transmission, disseminating, or otherwise making available, aligning or combining, blocking, erasing, or destroying.

(vi) Security Incident is any event in which Suez Data is or is suspected to have been lost, stolen, improperly altered, improperly destroyed, used for a purpose not permitted under the Contract Document or this Appendix, or accessed by any person other than Supplier Personnel pursuant to the Contract Document or this Appendix.

(vii) Security Notices are any written communications, notices, filings, press releases, or reports related to any Security Incident.

(viii) Sensitive Personal Data is a category of Personal Data considered to be especially sensitive and includes medical records and other personal health information, including protected health information (PHI), as defined in and subject to the U.S. Health Insurance Portability and Accountability Act of 1996; personal bank account and payment card information and other financial account information; customer bank account and payment card information; national identifiers; and special data categories of data under applicable data protection law (such as race, nationality, political opinions, trade union membership, home life, and sexual orientation). Sensitive Personal Data shall be subject to the controls specified below for Suez Restricted Data.

(ix) Suez means Suez S.A. or a Suez S.A. affiliate signing the Contract Document with Supplier.

(x) Suez Data is any Suez Confidential Information as defined in the Contract Document Processed in connection with performance of the Contract Document. Personal Data, Sensitive Personal Data, Controlled Data and Suez Restricted Data are Suez Data.

(xi) Suez Information System(s) means any systems and/or computers managed by Suez, which includes laptops and network devices.

(xii) Suez Restricted Data is information that Suez identifies as 'restricted data' in the Contract Document, or that Suez identifies as "Restricted," "Highly Confidential," or similar at the time of disclosure.

(xiii) Supplier is the entity that is providing goods or services to Suez pursuant to the Contract Document.

(xiv) Supplier Information System(s) means any Supplier systems and/or computers used to Process Suez Data pursuant to the Contract Document, which includes laptops and network devices.

(xv) *Supplier Personnel* means all persons or entities providing services and/or deliverables under the Contract Document, including Supplier's employees, permitted affiliates, suppliers, contractors, subcontractors and agents, as well as anyone directly or indirectly employed or retained by any of them.

Parts B-E and H-J apply to all Suppliers that Process any Suez Data.

Part B: Collecting, Processing and Sharing Suez Data

Supplier shall implement appropriate organizational, technical, and physical measures and controls to ensure the security and confidentiality of Suez Data and to prevent accidental, unauthorized or unlawful destruction, alteration, unauthorized disclosure or access, modification or loss; misuse; or unlawful Processing of Suez Data. Supplier is responsible for compliance with this Appendix by all Supplier Personnel.

Organizational security controls:

1. Supplier and Supplier Personnel shall Process Suez Data, and access and use Suez Information Systems, only on a need-to-know basis and to the extent necessary to perform services under the Contract Document or as otherwise instructed by Suez in writing.

5. Other than approved Security Notices, or to law enforcement or as otherwise required by law, Supplier may not make or permit any public statements concerning Suez's involvement with a Security Incident to any third-party without explicit written authorization of Suez's Legal Department.

Part D: Audits

Supplier responsibilities:

1. Supplier must conduct periodic security risk assessments of Supplier Information Systems to identify critical information assets, assess threats, and determine potential vulnerabilities.
2. Upon request, Supplier must provide Suez an executive summary of any audits and assessments conducted on Supplier Information Systems, including the scope of the audit and/or assessment and any vulnerabilities and corrective actions.
3. Supplier must use commercially reasonable efforts to remediate within thirty (30) days any items rated as high or critical (or similar rating) in any audits or assessments of Supplier Information Systems.
4. Supplier agrees to cooperate fully with Suez or its designee during audits (below) and shall provide access to facilities, appropriate resources, and supporting documentation and complete security assessment questionnaires as requested.

Suez audit rights:

5. Suez reserves the right to conduct an audit, upon 30 days advance notice, of Supplier's compliance with the requirements in this Appendix, including but not limited to: (i) review of Supplier's applicable policies, processes, and procedures, (ii) review of the results of Supplier's most recent vulnerability assessment and accompanying remediation plans, and (iii) on-site assessments during regular business hours of Supplier's physical security arrangements and Supplier Information Systems. Suez reserves the right to conduct an Applications Vulnerability Assessment if Supplier's vulnerability assessments do not meet or exceed Suez application security requirements. This right shall survive termination or expiration of the Contract Document so long as Supplier Processes Suez Data.
6. Subject to the confidentiality provisions of the Contract Document, Suez or its representative may review, audit, monitor, intercept, access and, disclose any information provided by Supplier that is Processed or stored on Suez Information Systems or on Suez Mobile Devices accessing the Suez network.

Part E: Regulatory Requirements

In the event Supplier Processes Suez Data that is subject to additional regulatory requirements, or in a manner subject to additional regulatory requirements, Supplier agrees to cooperate with Suez for Suez's compliance with such requirements. Such cooperation may include, without limitation, execution of additional agreements required by applicable law (e.g., EU Standard Contractual Clauses, U.S. Protected Health Information Agreement), implementation of additional security controls required by applicable law, completion of regulatory filings applicable to Supplier, and participation in regulatory audits, subject to the terms of Part D above.

Part F applies to any Supplier that Processes Personal Data (including Sensitive Personal Data)

Part F: Personal Data

1. Supplier shall comply with all laws applicable to Supplier's activities concerning Personal Data governed by this Appendix, including those concerning notice and consent, onward transfer to a third party, and international transfer, and shall act only on Suez's written instruction concerning any such transfers. Supplier must receive approval from Suez prior to (i) moving Personal Data from its Suez-approved hosting jurisdiction to a different hosting jurisdiction; or (ii) provisioning remote access to such Personal Data from any location other than the hosting jurisdiction or other Suez-approved jurisdiction.
2. Any computers, devices or media (e.g., laptop computers, phones/PDAs, USB drives, back-up tapes) containing Personal Data must be encrypted at rest. Encryption also must be employed when transferring Personal Data over public networks/Internet. Supplier must maintain cryptographic and hashing algorithm types, strength, and key management processes consistent with industry practices.
3. Unless and except to the extent expressly provided in the Contract Document, Supplier must seek and obtain Suez's prior written approval regarding the scope of any Personal Data to be collected directly by Supplier, as well as any notices to be provided and any consent language to be used when collecting such information from a Data Subject. In the case of Personal Data collected directly from Data Subjects by Supplier, Supplier shall comply with applicable data privacy laws and regulations, including those concerning notice, consent, access and correction/deletion.

Part G applies to Suppliers that Process Sensitive Personal Data, Controlled Data, and/or Suez Restricted Data. The requirements of this Part G are in addition to requirements of Parts A through F above. References to Suez Restricted Data in this Part G shall be deemed to also refer to Sensitive Personal Data and/or Controlled Data as the context requires.

Part G: Protecting Suez Restricted Data, Controlled Data, and Sensitive Personal Data

1. Supplier must have a formal information security program with clearly defined information security roles, responsibilities and accountability.
2. Supplier must perform or have an independent third party perform vulnerability assessments on Supplier Information Systems annually and remediate as required in Part D.3.
3. Any Supplier Personnel accessing Supplier's internal or hosted network remotely must be authenticated using two-factor authentication method and such transmissions must be encrypted at a level consistent with industry standards.
4. Supplier must implement a device hardening and configuration standard.
5. Supplier must implement appropriate data loss prevention (DLP) controls (e.g., disabling of USB ports, DLP software, URL/Web filtering) to detect and prevent unauthorized removal of Suez Restricted Data from Supplier Information Systems.