Cybersecurity and Data Protection Terms and Conditions

Last Modified: December 20, 2023

These Cybersecurity and Data Protection Terms and Conditions (these "**Terms and Conditions**") apply to the contractor or supplier (and its personnel and subcontractors) (collectively, "**Supplier**") to an Aegion Corporation or an Affiliate of Aegion Corporation (collectively, "**Company**") agreement ("**Agreement**") to which these Terms and Conditions are referenced. These Terms and Conditions shall further apply to any Supplier that may store, process, or have access to Company Data or Confidential Information. Company and Supplier are collectively referred to herein as the "**Parties**" and each a "**Party**."

These Terms and Conditions set forth certain of the Supplier's covenants with respect to the protection of Company Data and is supplemental to any Agreement and a part thereof. For the avoidance of doubt, a breach by Supplier of its covenants, representations and other undertakings hereunder shall constitute a breach of and an event of default under the Agreement for which the Company shall have all of its rights and remedies thereunder.

For the avoidance of doubt, compliance with these Terms and Conditions by Supplier shall in no way limit Supplier's liability to the Company, its Affiliates and their respective directors, managers, officers, employees and agents arising from or relating to the disclosure or misuse of Company Data in violation of Applicable Law or the provisions of the Agreement, and these Terms and Conditions shall in no way modify or limit in any way Supplier's obligations and liability thereunder or hereunder. Company and Supplier agree that no information constituting Personally Identifiable Information, as defined below, will be provided under the Agreement or during the course of Supplier and Company's engagement. Any information to be provided under the Agreement or during the course of Supplier and Company's engagement that would constitute Personally Identifiable Information will be Deidentified and/or Aggregated prior to Supplier being provided with the information or provided access to the information. In the event Supplier has been or will be provided with Personally Identifiable Information or access to Personally Identifiable Information, Company and Supplier agree to immediately enter into a new Agreement with terms governing the processing of Personally Identifiable Information.

1. Definitions. For purposes of these Terms and Conditions, the following terms shall have the following meanings:

(a) Affiliate - Affiliate means any entity directly or indirectly controlling, controlled by or under common control with another entity.

(b) Aggregated – Aggregated means a process through which information that relates to a group or category of individuals, from which individual identities have been removed, that is not linked or reasonably linkable to any individual or household, including via a device.

(c) Applicable Law – Applicable Law means any law, regulation, regulatory guidance or other legal or regulatory standard applicable to Supplier, Services provided under the Agreement or Company Data. For the avoidance of doubt, the term Applicable Law includes any changes to any law, regulation, regulatory guidance or other legal or regulatory standard that occurs during the term of the Agreement.

(d) Company Data – Company Data includes all PII and all other Confidential Information of the Company. For the avoidance of doubt, all Company Data constitutes Confidential Information for purposes of the Agreement.

(e) Confidential Information - means all non-public, confidential, or proprietary information of Company or any of its Affiliates, any company managed by Company or any of its Affiliates, or customer of any of the foregoing, any third party which has disclosed such information to Company, or to any of its Affiliates on a confidential basis, whether in oral, written, electronic, or other form or media, and whether or not marked, designated or otherwise identified as "confidential." Confidential Information includes (i) all information that would reasonably be considered non-public, confidential, or proprietary given the nature of the information or the circumstances of its disclosure; (ii) all information which is of value to the aforementioned entities and/or individuals and the disclosure of which could result in competitive or other disadvantage to the aforementioned entities and/or individuals, and (ii) all notes, analyses, compilations, reports, forecasts, studies, samples, data, statistics, summaries, interpretations, and other materials prepared by or for the Supplier or its employees or contractors that contain, are based on, or otherwise reflect or are derived, in whole or in part, from any of the foregoing. Examples of Confidential Information include, without limitation, Company or Affiliates, their respective customers' or such third parties' business or financial affairs, trade secrets, technology, research and development, pricing, product plans, marketing plans, employee and candidate identities, client lists, customer lists, registered representative lists, the types and amounts of products and Services provided hereunder by Supplier to Company, information which is considered sensitive by Company and/or Affiliates because it relates to proprietary data or information important to Company maintaining its competitive advantage in the marketplace and is deemed important to the success of its business by Company's senior executive management or its board of directors, the terms or existence of the Agreement, and all copies, summaries, and compilations of any of the foregoing. Confidential Information also includes business-related information of Company and Affiliates the tampering with which, or unauthorized disclosure, access or use of which, would cause a material adverse impact to the business, operations or security of Company or Affiliates or would violate Applicable Law.

(f) Deidentified – Deidentified means a process through which information is modified such that the information cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular individual, provided that the Supplier:

(i) Has implemented technical safeguards that prohibit reidentification of the individual to whom the information may pertain.

(ii) Has implemented business processes that specifically prohibit reidentification of the information.

(iii) Has implemented business processes to prevent inadvertent release of deidentified information.

(iv) Makes no attempt to reidentify the information.

(g) Encrypted Data – Encrypted Data means data that has been transformed through an industry standard process into a form that results in a low probability of assigning meaning without the use of a protective process or key.

(h) Personally Identifiable Information (PII or Personal Information) - PII means all customer and employee non-public personally identifiable information and is protected by legal and regulatory requirements and is sensitive information and/or could cause harm to customers, employees or the Company and Affiliates if mishandled and disclosed in violation of Applicable Laws or these Terms and Conditions. PII includes non-public personal information covered by Title V of the Gramm-Leach-Bliley Act, HIPAA, and state privacy and information security laws, including the California Consumer Privacy Act and similar laws.

(i) Security Incident – Any actual or reasonably suspected unauthorized acquisition of or access to Company Data including incidents of acquisition or access exceeding properly granted authority. Security Incident includes any event that constitutes a security breach under Applicable Law.

Any other capitalized terms used herein without a definition shall have the meaning assigned to it in the Agreement.

2. Scope of Data Protection Program. The information and security obligations set forth in these Terms and Conditions are based on ISO standards 27001 and 27002 as the same may be updated from time to time and shall apply where any Service provided by Supplier involves any product, service, or system that:

(a) is branded with Company trademarks, logos or includes Company-related Internet domain names;

(b) will access Company Data; or

(c) exists on the same logical and/or physical network as other Supplier products, services or system that have access to sensitive Company Data.

3. Control of Data; Limited License. As between Supplier and Company, all Company Data is and shall remain the exclusive property of Company. Company hereby grants Supplier with a limited license to use Company Data solely for the purposes of performing the Services under the Agreement (or other agreements between the Parties) and these Terms and Conditions. Notwithstanding the foregoing and any other provision in these Terms and Conditions, Supplier shall not possess or assert any lien against or to Company Data.

4. Collection, Sharing and Use of Company Data. Notwithstanding provisions to the contrary in the Agreement or other agreements between the Parties, Supplier may only use Company Data provided under the Agreement for the purpose of providing Services pursuant to the Agreement.

5. Derivative Data.

(a) Any information created using Company Data that identifies or is capable of identifying the Company, its Affiliates, or individuals shall constitute Company Data and (as between Company and Supplier) is owned by Company.

(b) Information created using Company Data may only be used or shared by Supplier to provide Services pursuant to the Agreement.

6. Deletion of PII. Individuals to whom PII relates may have rights to demand deletion of some or all of the PII collected by an entity or the entity's service providers.

(a) Deletion requests received by Company. If Company receives a deletion request from an individual to whom PII relates, Company will notify Supplier regarding the request and the individual making the request. Supplier will comply in a prompt and legally compliant time frame with any direction by Company to delete PII relating to the requesting individual.

(b) Deletion requests received by Supplier or its service providers. If Supplier receives a deletion request from an individual to whom PII relates, Supplier shall notify Company in writing of the deletion request promptly and in no case more than three (3) business days after receipt of the request. Supplier's notification to the Company shall include a copy of the request. Supplier will comply in a prompt and legally compliant time frame with any direction by Company to delete PII relating to the requesting individual.

7. Sale of PII. In no event shall Supplier engage in the sale (as defined under Applicable Law) of PII provided to Supplier.

8. Information Regarding Collection or Sharing of PII. Individuals to whom PII relates may have rights to demand information regarding the collection or sharing of PII collected by an entity or the entity's service providers.

(a) Information requests received by Company. If Company receives an information request from an individual to whom PII relates, Company will notify Supplier regarding the request and the individual making the request. Within 15 business days, Supplier will provide the information requested by Company, which may include the following:

(i) The categories of PII relating to the requesting individual that the Supplier or its service providers collect or share;

(ii) The specific items of PII relating to the requesting individual that the Supplier or its service providers collect or share;

(iii) The sources of any PII relating to the requesting individual that the Supplier or its service providers collect or share;

(iv) The business purpose for which any PII is shared.

(b) Information requests received by Supplier or its service providers. If Supplier receives an information request from an individual to whom PII relates, Supplier shall notify Company in writing of the information request promptly and in no case more than three (3) business days after receipt of the request. Supplier's notification to the Company shall include a copy of the request. Supplier will respond to the individual in a prompt and legally compliant time frame.

9. PII Obtained by Supplier through a Sale. If Supplier will provide PII to the Company, prior to providing such PII Supplier will notify Company regarding data elements that were obtained by the Supplier through a sale (as defined under Applicable Law).

10. Security Policy Management. At all locations where access is provided to Company Data under the Agreement (each a "Supplier Facility"), Supplier will maintain and enforce up-to-date, industry standard written data protection policies and procedures under an established industry security framework. Such policies and procedures must address:

(a) Physical and environmental security

(b) Communications and operations management

(c) Industry standard anti-virus and anti-malware controls

(d) Software patching

(e) Network connection security

(f) Secure software development

(g) Access controls to systems containing or processing Company Data

(h) Systems logging and monitoring for systems containing or processing Company Data

(i) Testing of security controls for systems containing or processing Company Data

(j) Information security incident management

(k) Supplier will not, and will ensure that its personnel do not, break, bypass, or circumvent, or attempt to break, bypass or circumvent, any security system of the Company or any Affiliate, or obtain, or attempt to obtain, access to any Company Data.

11. Human Resource Security Management.

(a) Without limiting its obligations and liabilities hereunder or under the Agreement, Supplier's information security policies and programs shall at

all times include ensuring that its employees, agents, contractors and permitted subcontractors that provide or affect any of the Services are:

(i) provided with adequate training regarding security practices;

(ii) appropriately disciplined for failure to comply or adhere with Supplier's policies and procedures relating to privacy, information security or cybersecurity;

(iii) screened to at least the extent provided hereunder to ensure there are not any current or prior information security-related incidents in their employment history, including incidents relating to fraud, dishonesty or financial crimes, including without limitation identity theft or related events, before they are assigned to perform any Services or related functions; and

(iv) bound by the terms of Supplier's standard non-disclosure agreement.

12. Business Continuity and Disaster Recovery Management. Supplier shall establish and maintain industry-standard business continuity, backup and redundancy, and disaster recovery management practices.

13. Compliance Management. Supplier understands, acknowledges, and agrees that the requirements contained herein are in addition to and do not limit any obligations imposed by Applicable Laws and its obligations under the Agreement while performing Services under the Agreement or any agreement or while provided access to Company Data. In addition to complying with these Terms and Conditions, Supplier agrees to maintain compliance with industry-standard practices for data management and security and all Applicable Laws.

14. Encrypted Data. Supplier will employ industry-standard controls to ensure any Company Data that is Encrypted always remains in an Encrypted state. Such controls shall include industry-standard encryption key management, including storing and transmitting encryption keys separately from the Encrypted data. Supplier will immediately notify Company if any Company Data that was Encrypted ceases at any time to be in an Encrypted state.

15. Deidentified and Aggregated Data. Supplier will employ industry-standard controls to ensure any Company Data that is Deidentifed or Aggregated always remains in that state. Supplier will immediately notify Company if any Company Data that was Deidentifed or Aggregated ceases at any time to be in that state.

16. Audits and Examinations.

(a) Throughout the term of the Agreement, Supplier shall provide to Company at the request of and at no cost to Company, copies of Supplier's third party audits, operational assessments, reports of independent public accountants, annual audited financial statements, and any other documentation agreed upon by the parties necessary that reflects Supplier's regulatory and financial standing and the status of Supplier's

controls for data processing. Unless prohibited by applicable law, Supplier shall promptly advise Company of any actual or contemplated material changes in Supplier's ownership or control.

(b) If, in the reasonable determination of the Company, provided audits relating to the Supplier do not provide sufficient information to determine risks posed by the Supplier or Supplier's compliance with these Terms and Conditions, Company shall have the right to perform or have performed audits of the Supplier. The terms of such audits shall be reasonably agreed between the Parties.

(c) In connection with its obligations hereunder, Supplier shall reasonably cooperate and provide to Company auditors, in a timely manner, all such assistance as they may reasonably require in connection with any audit or examination. Company shall provide Supplier with a reasonable time period to complete the requests of the auditors and examiners. Company shall provide Supplier with a copy of the results from any such audit upon Supplier's request.

17. Third Party Audits. In addition to any other audit and reporting requirements under the Agreement or any other agreement, during the term of the Agreement, if a SOC 1 Report or a SOC 2 Report reveals that the Services provided by Supplier do not cause Supplier's operations to meet the auditor's recommendation, then Supplier shall provide such further services as are necessary to bring its operations into conformance with the auditor's recommendations to such level and degree, at no cost to Company.

18. Regulatory Agency Requirements. The Supplier understands and acknowledges that the Company and Affiliates may be subject to examination by any federal, state or local governmental or quasi-governmental officials with regulatory authority over the Company or such Affiliate. The Supplier agrees to cooperate fully with any examination or inquiry by any such officials or other regulatory body or agency. The Supplier further acknowledges that the Company may be required to engage in ongoing oversight of its relationship with the Supplier, including, but not limited to, reviewing the Supplier's financial condition, compliance with privacy laws and regulations, insurance coverage, and performance under these Terms and Conditions. The Supplier agrees to cooperate with the Company in monitoring the Supplier and its performance under these Terms and Conditions and to provide the Company with updated information in these and other areas, in such form and at such times as the Company may reasonably request.

19. Remediation of Deficiencies. If Company reasonably determines, following any of the foregoing audits of Supplier's security practices with respect to the Services (including in connection with an Company "technology due care assessment" or similar review), that there are any gaps or deficiencies in such Supplier security (e.g., if, with regard to Supplier's security, Company has what is considered a "strong recommendation" under Company's technology review procedures as of the effective date of the Agreement), then the Parties shall work together in good faith to reach a mutual agreement to address such gaps or deficiencies; provided, however, that if the Parties cannot reach such a mutual agreement within thirty (30) days after such determination by Company, Company shall have the right to terminate the

Agreement or any Schedule without the payment of any early termination fee, penalty or other similar charge regardless of any other terms and conditions in the Agreement or any relevant Schedule.

20. Right to Monitor. Company shall have the absolute right, but not the obligation, to monitor access to and the processing of Company Data as part of the Services. Such monitoring, and any comments provided by Company in that regard, do not diminish Supplier's obligations hereunder.

21. Cybersecurity Insurance. Supplier shall at its sole cost and expense procure and maintain through the term of the Agreement or any agreement and for a period of two (2) years following the termination or expiration thereof, industry-standard network risk and cyber liability coverage (including coverage for unauthorized access, failure of security, breach of privacy perils, as well at notification costs and regulatory defense) in the amount prescribed in the Agreement or $1,000,000 per claim, whichever is greater, naming Company as an additional insured with waiver of subrogation. Such policy shall provide coverage for disclosures and/or breaches of Company Data arising out of or relating to Supplier's services. Such policy shall also include coverage for the costs associated with restoring lost or damaged Company Data, sending breach notifications to affected individuals, public relations expenses, fines and penalties. Such policy shall not contain exclusions for the acts or omissions of either Supplier or Company or their respective employees, agents, subcontractors or volunteers, whether intentional or unintentional, resulting in or relating to any use of Company Data not expressly permitted by the Agreement or these Terms and Conditions or any breach of Company Data. Supplier must notify Company at least thirty (30) days prior to the cancellations or modification of such policy.

22. Records Retention and Disposal of Company Data.

(a) Supplier shall provide Company with a complete back-up of all Company Data, in electronic form, as requested by Company.

(b) Supplier is responsible for retaining any and all records related to the Services provided until the last to occur of:

(i) seven (7) years after expiration or termination of the Agreement;

(ii) all pending matters relating to the Agreement (e.g., disputes) are closed; or

(iii) any retention requirements under Applicable Law have elapsed, Supplier shall maintain and provide access upon request to the records, documents and other information required to meet Company's audit rights under these Terms and Conditions. Before destroying or otherwise disposing of such information, Supplier shall provide Company with sixty (60) days prior notice and offer Company the opportunity to recover such information or to request Supplier to deliver such information to Company.

(c) The Supplier shall ensure that it does not retain Company Data for longer than it needs such information to perform its obligations hereunder. The Supplier's disposal policy shall require that such information is reviewed and destroyed on a routine basis, which shall be no less than weekly. As part of its Information Security Program, the Supplier shall take appropriate measures to properly dispose of Company Data, whether such information is in paper, electronic or other form and to prevent identity theft.

23. Liability and Indemnification.

(a) Notwithstanding any provision in the Agreement or other agreements between the Parties, Supplier shall indemnify and hold Company harmless for any violation by the Supplier, or entities or persons performing services on behalf of Supplier relating to the Agreement, of any provision of these Terms and Conditions, including any direct or consequential damages relating to the violation of the provisions of these Terms and Conditions. Supplier further agrees that it assumes all responsibility and risk of loss to Supplier resulting from access to and use of Company Data and Confidential Information. In no event shall any Company entity or its directors, officers, employees or representatives be liable for any claims, liability, damages, losses, costs, or expenses of any kind suffered or incurred by Supplier, in contract, tort, or otherwise, including but not limited to any indirect or consequential damages, loss of profits or revenue, loss of use of Supplier assets, costs of capital and/or financing, down time costs, costs of reduced productivity, loss of or compromise of data, contractual liability to third parties, governmental penalties, loss of opportunity, loss of goodwill, and any other purely economic losses (including economic loss arising as a consequence of property damages) arising under or in connection with these Terms and Conditions, even if Company has been advised of the possibility of such claims, liability, damages, losses, costs, or expenses, and even if Company has been at fault or in breach of contract.

(b) Access to Company Data and Confidential Information is made available to Supplier "as is" and "when available". Company disclaims any and all representations and warranties relating to Company Data and Confidential Information, including any implied warranty of fitness for a particular purpose, quality, functionality, accuracy, currency, completeness, reliability, operability, or performance.

24. General. Without limiting the foregoing, and regardless of the location of Supplier's place of business or the location where the Services are provided, and for the avoidance of all doubt, Supplier covenants and agrees that the provisions of Choice of Law provision of the Agreement also governs these Terms and Conditions and Supplier covenants and agrees to comply with all applicable United States of America federal laws, and all applicable laws of the states of the United States of America, and, in addition laws of other applicable

jurisdictions in connection with the performance of its obligations, including without limitation its obligations to protect Company Data. In the event the applicable Agreement does not contain a Choice of Law provision, these Terms and Conditions shall be governed by the laws of the state of Missouri.