PURCHASE ORDER MASTER SERVICES AGREEMENT

This PURCHASE ORDER MASTER SERVICES AGREEMENT ("Agreement") applies to every purchase, sale, shipment and delivery of certain products or services (as defined as "Services" or "Work" below) that Darden Corporation or its affiliates ("Company") requests from the supplier listed in the Purchase Order that references this Agreement ("Vendor") unless there is a separate fully executed master agreement for the Services between Company and Vendor. This Agreement may be amended or modified from time to time by Company, at its sole option, and such amendments or modifications will apply to any Purchase Order Vendor fills after thirty (30) days from the effective date of the modification or change.

WHEREAS, Vendor provides services and deliverables as defined herein; and

WHEREAS, Company desires to purchase such services from Vendor.

NOW, THEREFORE, and for mutual consideration given and received, the parties agree that the following terms and conditions shall apply:

1. Scope. Services or work ("Services" or "Work") as used in this Agreement shall mean Vendor's products, services or work as described in the applicable Purchase Order or statement of work ("Statement of Work" or "SOW") agreed upon in writing by the Parties, which, by this reference shall be incorporated herein. For the Term, such Services are hereby offered for sale by Vendor and may be purchased by Company in accordance with and subject to the terms and conditions of this Agreement.

2. Term. This Agreement will be binding on the Effective Date and will continue for a period of twelve (12) months thereafter ("Initial Term") unless earlier terminated as set forth herein. Thereafter, this Agreement shall be automatically renewed for successive twelve (12) month periods on the anniversary of the Effective Date (each a "Renewal Term") unless earlier terminated as set forth herein. Either party may terminate this Agreement at the end of the Initial Term or any Renewal Term by providing ninety (90) days written notice prior to the end of any such period. The Initial Term, each Renewal Term and any Transition Period shall collectively be referred to as the "Term."

3. Termination.

   a. Termination for Convenience. Company may, at any time during the Term, upon thirty (30) days' prior written notice, terminate this Agreement or any SOW, in whole or in part, by written notice to Vendor. In such case, Company's liability shall be limited to payment of the amount due for actual Services provided and, if applicable, deliverables provided through the date of termination.

   b. Termination for Cause. Either party may provide written notice of termination to the other party in the event of a material breach of this Agreement. The breaching party shall have thirty (30) days from receipt of such notice to cure the breach. If the breach is not cured within this thirty (30) day period, this Agreement shall automatically terminate upon the expiration of the notice period without further action required by either party.

   c. Effect of Termination. In the event of termination or non-renewal of this Agreement, (i) Company's liability shall be limited to payment of the amount due for actual Services provided and, if applicable, Deliverables provided through the date of termination; (ii)

Vendor agrees to provide Company with all Deliverables (including, without limitation, each Deliverable and/or any working documents related to a Deliverable and/or any partially completed Deliverables), in whole or in part or in process as of the effective date of such termination,(iii) except as otherwise set forth in this Agreement, Vendor agrees to return all Company Information, Company Data, Company Confidential Information and Company Proprietary Information in Vendor's possession; (v) except as otherwise set forth herein, Company agrees to return all Vendor IP (not otherwise licensed to Company, as set forth herein) and Vendor Confidential Information in Company's possession as set forth in Section 23, Confidentiality.

d. Transition Assistance. If requested by Company upon expiration, notice of termination, or non-renewal of this Agreement, Vendor shall provide to Company continued Services (as are already being provided to Company, and under the same terms and conditions in effect at time of notice of termination or non-renewal pursuant to this Agreement), for a period not to exceed six (6) months ("Transition Period") following the effective date of termination or non-renewal, such time period to be set by the Company. If requested by Company, Vendor shall provide transition services under the terms of this Agreement as modified by this provision, in order to facilitate the orderly transfer by Company from use of Vendor's Services to alternate services (collectively "Transition Services"). Such Transition Services shall be provided to Company at the rates set forth in the applicable SOW in place upon the effective date of termination for the duration of the Transition Period and shall be provided without interruption of the Services. Regardless of whether Company agrees to retain Vendor to provide Transition Services, the quality, promptness, and level of Services shall not be changed following notice of termination through the effective date of termination or during the Transition Period, unless mutually agreed to by the parties.

e. Company Data File. During the Term, upon request by Company, Vendor will provide a complete and secure (i.e., encrypted and appropriately authenticated) download or export file of Company Data, Company Confidential Information, and Company Proprietary Information in XML format including all schema and transformation definitions and/or delimited text files with documented, detailed schema definitions along with attachments in their native format at no additional charge. During the Term, Vendor will be available to answer questions about data schema, transformations, and other elements required to fully understand and utilize Company's data file at no additional charge. If Company requests such items in a non-standard format or additional downloads or exports, there may be an additional charge to Company for such services.

4. Price and Taxes.

a. Price. In full compensation for the Services provided under this Agreement (including any pre-approved, reasonable expenses Vendor may incur), Company shall either pay Vendor a set rate for Services actually rendered or shall pay Vendor based on a fixed fee, as set forth in each applicable SOW to this Agreement. All amounts payable by Company pursuant to the terms of this Section 4 shall be exclusive of taxes and shall remain unchanged for the Initial Term and the first and second Renewal Terms of this Agreement. Thereafter, Vendor may increase the rates upon sixty (60) days' written notice prior to the end of the second Renewal Term or any Renewal Term thereafter; provided, however, that such increase shall not exceed three percent (3%) over the rates in effect in the immediately preceding Renewal Term. The new rates shall be effective as of the first day of the Renewal Term following such notice.

b. Taxes.

i. Notwithstanding anything to the contrary contained in any other clause in this Agreement, rates, charges or fees specified in this Agreement are exclusive of all transaction taxes.

ii. Company shall bear all transaction taxes on the services (or goods) provided hereunder (e.g., sales, use, value added, goods and services). Vendor shall state applicable transaction taxes on its invoices or otherwise provide a tax-compliant invoice and remit all collected taxes to the appropriate taxing authority. Vendor shall not charge transaction taxes if Company, to the satisfaction of Vendor, timely provides an applicable exemption certificate acceptable to the taxing authorities. If Company is not invoiced for such taxes and the tax authorities subsequently determine that such taxes are due, Company shall pay such taxes as required by the applicable tax authorities, excluding any interest or penalties where failure to collect and remit such taxes was the result of Vendor's negligence or willful misconduct.

iii. Each party shall bear any and all taxes imposed on it through its entry into this Agreement, without regard to legal requirements relating to the withholding or collection and remittance of taxes to taxing authorities. Vendor agrees that Vendor will provide Company with appropriate withholding certificates or other certificates or documentation, including but not limited to Forms W-9 or W-8 (e.g., Form W-8ECI, Form W-8BEN, Form W-8BEN-E, Form W-8IMY) before any payment is made to Vendor and/or Vendor's US/foreign entity under this Agreement, as required by law and upon subsequent request by Company. Vendor further agrees that Company shall be entitled to withhold from payments due to Vendor under this Agreement any amounts (including amounts Company reasonably determines should have been withheld from previous payments but were erroneously not withheld) that Company believes, in its reasonable discretion, are required to be withheld under applicable law. Vendor further agrees to timely file all required returns, report any income, and pay any applicable taxes incurred as a result of the payments each receives under this Agreement, and timely provide evidence or other certification to Company that such income was reported, including on IRS Form 4669 (or other similar form requested by Company). To the extent required by applicable law, Company agrees to provide Forms 1099, Forms 1042-S, or other appropriate forms to Vendor evidencing the amounts paid to Vendor under the terms of this Agreement and any taxes withheld, along with any original tax receipts or other information required to substantiate a foreign tax credit. Nothing in this Agreement shall be interpreted to require Company to pay any tax on Vendor's behalf or provide a gross-up for tax on any amount paid or payable under this Agreement.

iv. Each party shall bear (a) taxes on its net income, assets, capital, or property or equipment it owns, (b) employee taxes (employer's responsibility for income tax withholding and social security taxes); and (c) real / personal property taxes.

v. The parties shall cooperate (a) to determine, and lawfully reduce, their respective tax liabilities (including by providing resale / exemption certificates, information related to out- of-state/country sales or use of hardware and other reasonably requested information); and (b) in the event of enquiries or audits by a tax authority on inter-party transactions.

vi. Liability on account of taxes not covered herein shall be mutually agreed. Unless otherwise agreed in the above clauses, the party that is liable for payment of any tax upon which interest and penalties are imposed shall bear such interest and penalties.

5. Expenses. Company shall reimburse Vendor for reasonable travel and lodging expenses of Vendor incurred on travel that has been authorized by Company; provided, however, that Company shall not compensate Vendor for any time incurred with such travel. Reasonable travel expenses means the amount per mile allowed by the IRS when private transportation is used, and coach or tourist class rates when commercial air travel is used, unless otherwise authorized by Company. Expense reports and receipts for eligible expenses must be submitted no more than thirty (30) days after the expense is incurred. Unless approved in advance by Company, there shall be no reimbursement for the commuting expense incurred by Vendor's personnel in commuting to Company locations to perform Services or to Company locations from their homes. Vendor shall provide Company with detail of expenses as requested by Company for all reimbursable items as a condition of reimbursement. In all instances, Company shall be afforded the opportunity to review and approve expenses incurred by Vendor prior to reimbursement of the expenses. Notwithstanding the foregoing, for each SOW, in no event will Company reimburse Vendor for expenses that exceed 10% of the fees paid to Vendor pursuant to such SOW.

6. Limit of Expenditure. For fees not fixed in the SOW, expenditures for Services provided under this Agreement shall not exceed the limit set forth in the applicable SOW, unless otherwise expressly approved in writing by Company. Notwithstanding the aforementioned or any other provisions in this Agreement, the total amount payable by Company for the Services shall be determined by applying the stated rate of compensation, if any, to the Services actually performed or Services provided by Vendor, plus expenses as set forth in Section 5. Vendor shall not render Services and Company shall not be required to pay for Services in excess of the amount stipulated in this Agreement, unless Vendor has first secured an amendment to this Agreement signed by an authorized representative of Company for the increase in expenditure.

7. Payment Terms. The parties agree that Vendor will register Vendor’s business in Company’s Vendor Management Portal and use Company’s Procure to Pay system to provide invoices to Company and receive payment information from Company. Vendor will invoice Company through the Company’s Procure to Pay system according to the agreed upon invoicing schedule. Company shall pay all undisputed invoices within sixty (60) days of receipt of Vendor’s invoices through the Company’s invoicing and payment system.

8. Invoicing For Services. Vendor’s invoices shall be issued upon completion of the Services rendered, unless otherwise indicated in an applicable SOW, in which case invoices shall be issued in accordance with the schedule set forth in such SOW. All invoices shall provide a detailed itemization of charges contained therein. The Work shall be delivered free from all claims, liens, and charges whatsoever. In the event Vendor owes money to or is otherwise obligated to Company when the invoice is issued, Company may offset such invoices or the sums due or obligated, making payment to Vendor only for such balance due.

9. Acceptance. Company shall have the right to verify the results of the Services and to accept or reject any such results that are in Company’s judgment non-conforming. In the event Company reviews Service results in which defects or non-conformities are not apparent upon examination prior to acceptance, Company reserves the right to require the rework of such results.

10. Timely Performance. If Vendor has knowledge that anything prevents or threatens to prevent the timely performance of the Services under this Agreement, Vendor shall immediately notify Company thereof and include all relevant information concerning the delay or potential delay.

11. Schedule. Services shall be performed in accordance with the schedule in the applicable SOW.

12. Ownership of Proprietary Information and Licenses.

a. Definitions.

i. "Company Data" means all data and datasets, whether in raw or processed form, that are collected, generated, received, maintained, or stored by or on behalf of the Company in connection with its business operations. Company Data includes, without limitation, customer data, transaction records, usage data, technical data, metadata, and any other information that is subject to data management, processing, or analysis by the Company or its agents.

ii. "Company Information" means any and all information relating to the business, operations, affairs, finances, products, services, customers, suppliers, plans, strategies, or personnel of the Company, whether disclosed orally, in writing, electronically, or by any other means. Company Information includes, but is not limited to, organizational structure, business plans, financial statements, marketing materials, and any other data or documentation that pertains to the Company's business activities.

iii. "Company IP" means all of Company's information, database rights, computer programs, technology, data, platforms, algorithms, software, methods, apparatuses, information or documentation (including without limitation, specifications, designs, plans, drawings, prototypes, diagrams, flow charts or other technical or business information), techniques, processes, materials, systems, plans, models, programs, code, know-how, and, whether or not reduced to practice and whether or not affixed to a tangible medium, Company acquired, developed, owned, or prosecuted intellectual property. Company IP also includes Company Data, Company Information, Company Confidential Information, Company Proprietary Information, and Company Sensitive Information.

iv. "Company Sensitive Information" means all Company Information, together with any other non-public information, data, or material, in any form or medium, that is owned by, pertaining to, or held by the Company and that, if disclosed, accessed, or used without authorization, could reasonably be expected to adversely affect the Company's business interests, operations, reputation, financial standing, or competitive position, including without limitation, personally identifiable information (PII) of employees, customers, or business partners (such as names, contact details, Social Security numbers, financial account numbers, and health-related information).

v. "Deliverables" means all tangible materials, reports, creative(s), and custom designed software, materials, systems, code, programs or documentation (including without limitation, specifications, diagrams, flow charts, designs, plans, drawings, prototypes, or other technical or business information): (A) identified by the parties in the applicable SOW as a Deliverable; and (B) delivered to Company in accordance with this Agreement.

vi. "Developed Information" means all software, computer program, technology, data, platforms, algorithms, processes, methods, apparatuses, techniques, processes, materials, systems, models, programs, code, know-how, information and documentation (including without limitation, specifications, diagrams, flow charts, designs, plans, drawings, prototypes or other technical or business information) developed, created, or otherwise conceived by Vendor in the course of Vendor's performance of this Agreement, whether reduced to practice and whether affixed to a tangible medium, including, without limitation, enhancements, improvements, upgrades, or other modifications.

vii. "Intellectual Property Rights" means current and future worldwide rights under patent law, copyright law, trade secret law, trademark law, trade dress law, moral rights law, and other similar rights.

viii. "Vendor IP" means all Vendor's pre-existing: information, computer programs, technology, data, platforms, algorithms, software, methods, apparatuses, information (including without limitation, specifications, designs, plans, drawings, prototypes or other technical or business information), processes, materials, know-how, and, whether or not reduced to practice and whether affixed to a tangible medium, Vendor acquired, developed, or prosecuted intellectual property.

b. Vendor Ownership. Vendor owns all Intellectual Property Rights to: (i) Vendor IP, including any derivative or modification thereof, and (ii) Developed Information that is a derivative or modification of Vendor IP; excluding any Deliverables ("Vendor Proprietary Information"). Company also acknowledges and agrees that Vendor is in the business of providing computer software consulting, development, and/or programming services and that Vendor shall have the right to provide services to third parties that are the same or similar to the Services provided to Company under this Agreement, subject to the terms and conditions set forth herein. Company shall cooperate with Vendor in preserving Vendor's Intellectual Property Rights in the Vendor IP to the extent included in the Deliverables owned by Company and all documentation and other information and materials pertaining to the same. Additionally, Vendor has the exclusive right to create enhancements, updates, upgrades, adaptations, arrangements, and translations of the Vendor IP in all countries of the world, including the United States.

c. Company Ownership. Company owns all Intellectual Property Rights to: (i) Company IP, including any derivative or modification thereof, (ii) Deliverables, including any derivative or modification thereof; provided, Company has paid, in full, all undisputed invoices for Services related to such Deliverables set forth in the applicable SOW; and (iii) Developed Information that is a derivative or modification of Company IP or Deliverables ("Company Proprietary Information"). Company shall own all right, title and interest in said Deliverables or Company Proprietary Information in perpetuity and said Delivered Information are deemed to be a "Work For Hire" as set forth in the United States Copyright Act of 1976 or if for any reason held not to be a work made for hire, Vendor hereby assigns all of its right, title, and interest in the Deliverables or Company Proprietary Information to Company. Vendor hereby waives any so-called "moral rights of authors" and all other similar rights however denominated throughout the world.

d. License Grant. To the extent that any Vendor IP is intangible and embedded within any of the Deliverables, Vendor hereby grants Company a royalty-free, fully paid-up, worldwide, perpetual, irrevocable, nonexclusive license to use such Vendor IP solely in connection

with the Deliverables; provided, however, the Vendor IP shall be subject to any use restrictions specified in the applicable SOW and Vendor may revoke any use of the Vendor IP that is outside the license grant as set forth herein. Vendor has the right, title, and/or license to grant all such licenses necessary for Company to own and/or use the Deliverables as set forth herein.

e. Exclusion from Use of Vendor IP. Nothing contained in this Agreement shall be construed to grant Company the right to use or exploit any Vendor IP in any manner other than as embodied in or used with a Deliverable.

f. Filing for IP Rights. Vendor shall use commercially reasonable efforts to cooperate fully with Company, and shall cause each of its affiliates and subcontractors (who have rendered Services and are associated with the Intellectual Property Rights of the Deliverable as set forth herein), if any, to cooperate within reason, at the expense of Company, in the preparation, prosecution, and protection of all such Intellectual Property Rights of the Deliverable(s) or Company Proprietary Information, to execute any documents necessary to perfect the transfer of such title, and shall use commercially reasonable efforts to cooperate fully with Company, at Company's expense, in any claims, legal actions and proceedings concerning the Intellectual Property Rights in and to the Deliverable(s) or Company Proprietary Information.

g. No License Grant. Except as expressly set forth herein, no license is granted by either party to the other with respect to any technical or business information, or with respect to rights in any patents, trademarks, copyrights, or other Intellectual Property Rights.

h. Notwithstanding anything to the contrary in this Agreement, both parties shall be free to use and employ their general skills, know-how and expertise, and to use, disclose, and employ any generalized and non-protectable ideas, concepts, methods, techniques, or skills gained or learned during the course of this Agreement ("General Skills"); but shall not be free to use and employ, in whole or in part, the other party's Deliverables, Developed Information, Confidential Information, Proprietary Information, or intellectual property rights, outside the scope and Term of this Agreement.

13. Vendor Access Security.

a. Access. Vendor may be provided with access to Company's computing environment, systems, and/or Company Data as part of this Agreement. During the period(s) of this Agreement that Vendor is granted such access, Vendor shall employ data, network security and privacy practices and procedures consistent with the current state and federal laws. These practices must be acceptable to the Company and in alignment with industry standards, including, as appropriate, without limitation, encryption, firewalls, and vulnerability scans. In addition, Vendor shall follow the process set forth in Section 14 below for notifying Company in the event of any breach of security or privacy with respect to Company's computing environment, systems, or Company Data.

b. Security Questionnaire. Vendor agrees to respond to Company's security questionnaire, which is consistent with the then current national standards as well as current industry standards and cybersecurity practices. Upon a satisfactory security compliance rating of Vendor's responses to the questionnaire as determined by Company in its sole discretion, Company will enable or otherwise grant access as needed during the Term of this Agreement. Thereafter, upon request, Vendor will respond to Company's security

questionnaire within five (5) business days of such request and must receive a satisfactory security compliance rating to maintain access to Company's computing environment and systems. In the event that Vendor does not receive a satisfactory security compliance rating from Company, Vendor's access will be suspended, at Company's sole discretion. In order for Vendor to be provided with such access, Vendor must address any failures and/or vulnerabilities with a plan of action and subsequent scan as proof of remediation to maintain access. If Vendor does not attain a satisfactory security compliance rating within thirty (30) days or mutually agreed upon period after such unsatisfactory security compliance rating, Company may terminate the Agreement and any SOW. An unsatisfactory security compliance rating based on material non-compliance will be considered a breach of the Agreement. In addition, any material delays in the performance of an SOW due to Vendor's unsatisfactory security compliance rating and resulting suspension of access would be a breach by Vendor of the applicable SOW(s).

c. Security Audits and Policies. Vendor shall perform regular security audits, vulnerability assessments, and penetration tests, including the use of bug bounty programs, for its systems and perimeter networks. Vendor shall provide the results of any such audits and tests as requested by Company. Vendor's Security Policy, Disaster Recovery Policy, and Business Interruption Policy shall be provided to Company upon request.

d. In addition to completion of the Company's security questionnaire, in the event that Company Information is being shared with Vendor, Vendor agrees to complete Company's Privacy Impact Assessment. This Privacy Impact Assessment will be used to determine appropriate processes for sharing sensitive information, as well as to ensure adherence to applicable data privacy laws and company policies.

e. Generative AI. "Generative AI Technology" is any machine learning or artificial intelligence tool that produces or creates content (including, but not limited to, text, imagery, audio, code, simulations, and video). "Generative AI Content" is any content created, modified, or produced in part or whole by Generative AI Technology that may be delivered (even if only ephemerally) to Company or Company systems or otherwise accessible by Company through the purchase or license of products or services from the Vendor. Vendor shall provide a list to Company of any Generative AI Content applicable to the SOW or ordering document and the Generative AI Technology used to create such Generative AI Content ("Generative AI List"). Vendor shall not make any changes to the Generative AI List without a Change Order to the SOW or applicable ordering document. Vendor shall comply with best practices regarding internal AI governance and controls including, but not limited to, the most current version of the NIST Artificial Intelligence Risk Management Framework or successor to such.

14. Security Incident Notification. Vendor agrees that it has in place and maintains appropriate security measures and safeguards designed to:

a. ensure the security, confidentiality, integrity, and availability of Company's Data, including, without limitation, personally identifiable information;

b. protect against any anticipated threats or hazards to the security and integrity of Company's computing environment and systems when being accessed by Vendor; and

c. protect against any unauthorized use or disclosure of any Company's Data, which includes personally identifiable information, consistent with applicable laws, industry standards

concerning privacy, data protection, confidentiality, information security, or any other actions contrary to this Agreement. In the event Vendor becomes aware of any security or confidentiality breach, threat, or hazard to the security or integrity of Company's computing environment and systems (e.g., information that a ransomware attacker has moved laterally from Vendor's network system into Vendor's customers' network systems) or the unauthorized use or disclosure of any Company Data ("Security Incident"), Vendor shall immediately contact Company's Director of Cybersecurity in writing to Darden Corporation, at 1000 Darden Center Drive, Orlando Florida 32837 and by email (privacy2@darden.com), to inform Company of any such Security Incident that may have or has occurred. Such notice shall summarize in reasonable details the effect on Company, if known, of the Security Incident and the corrective actions taken or to be taken by Vendor. Vendor shall promptly take all corrective actions that it deems reasonably necessary, and shall cooperate fully with Company, to the extent mutually agreed in writing between the parties, in all reasonable and lawful efforts to prevent, mitigate, or rectify such Security Incident.

15. Industry Recognized Independent Security Audits.

a. Vendor shall provide any industry recognized independent security audits, such as, but not limited to, SSAE 18 SOC letters (Type 1 or Type 2), PCI Attestations of Compliance, Penetration Testing Reports, ISO certifications, Bug Bounty program testing and results, or any other independent audit and/or assessment information, as applicable. During the Term, Vendor shall ensure such audits are performed at least annually. After the first audit report provided thirty (30) days after the Effective Date, Vendor shall provide Company with a copy of each updated or newly released report prepared in connection with each such audit within thirty (30) calendar days after it prepares or receives such report from its data center partner. Reports and materials related to audits shall be delivered to ITCompliance@darden.com using a secure method, such as, but not limited to, portal link utilizing username and password, encrypted zip file, or other mutually agreed upon secure method, as appropriate.

   For systems and applications deployed in a hosted, cloud, or managed service model such as, but not limited to, cloud, Infrastructure as a Service, or Software as a Service, or Platform as a Service, the Vendor shall provide independent security reports related to such environments. These reports may include, but not limited to, SOC letters (Type 1 or Type 2) and/or PCI compliance for the environments that host software, tools, or services related to the fulfillment of the Agreement between Company and Vendor. These reports will be used in combination with, and not in lieu of, security reports for the application and/or service provided by the Vendor that is hosted in such environments.

   Vendor shall appropriately encrypt Company Data transmitted over public networks and on removable media. If available for the application or service, Vendor will provide encryption at rest and in motion for Company Data in accordance with the standards set forth by the National Institute of Standards and Technology.

b. Prohibition of Jeopardizing Functionalities. Vendor shall not include any functionality (e.g. "backdoor") in its hardware and/or software applicable to the Service that jeopardizes the confidentiality, integrity, or availability of Company's systems or Data or any other actions contrary to the interests of Company in regard to confidentiality, integrity, availability, or compliance. Such jeopardizing functionality includes (i) unwanted collection or distribution of Company Data, (ii) unwanted manipulation or changes of Company Data or process

logic, (iii) unwanted disclosure of Company Data, or (iv) reduction of or interference with functionality.

c. Software Development Standards. To ensure secure software development, Vendor warrants it will, at a minimum, adhere to the current industry standards such as OWASP. Security vulnerabilities constitute defects and will be categorized and promptly resolved by Vendor.

16. Ownership of Company Data. Company shall own (a) all individual customer and transaction data (i) collected by Vendor's system through the Services or Software, (ii) related to or generated from Company's business, or (iii) arising from the Services performed pursuant to an SOW and (b) all data (i) provided to Vendor by Company, (ii) generated by Vendor or a third party on Company's behalf or (iii) on Company's system or under Company's control during the Term of this Agreement. Company hereby grants, and Vendor accepts, a limited, non-transferable, non-exclusive license to copy and use Company Data during the Term solely for the purpose of performing the Services required by this Agreement. Subject to the terms and conditions of this Agreement, Vendor will not provide the Company Data to other third parties nor use the Company Data to solicit or otherwise contact Company's customers. Company Data shall be considered Company Confidential Information.

17. Deliverables. Items, including without limitation, Software, that are deemed Deliverables as listed in the SOW shall be provided to the Company by the Vendor as per the Deliverable schedule identified in the SOW. Company will own all right, title, and interest in and to the Deliverables.

18. Reports. Vendor shall provide written periodic reports relating to the Services provided by the Vendor, the frequency and form of which will be determined by Company.

19. Audit. Vendor shall (i) keep adequate and accurate records for a period of seven (7) years from creation, of all amounts paid by or charged to Company, and (ii) maintain in compliance with this Agreement the processes and procedures related to the performance of this Agreement. Company, or its designee, at Company's expense, may upon at least five (5) business days prior written notice and during Vendor's normal business hours, no more than twice per year, unless Company determines or reasonably suspects that there has been a material violation of this Agreement, audit the records, processes and procedures of Vendor for the purpose of verifying compliance with this Agreement.

20. Independent Contractor. Vendor shall at all times be considered an independent contractor and neither Vendor nor any of Vendor's employees and Assistants performing Services under this Agreement shall be deemed an employee of Company. Accordingly, Vendor shall be responsible for: (a) verification and maintenance of the U.S. employment authorization of Vendor's employees and Assistants performing Services under this Agreement and record keeping obligations evidencing thereof (collectively, "U.S. Employment Authorization Requirements"); and (b) payment of its own labor costs, unemployment, social security, and other payroll taxes, including any contributions required by law, and shall indemnify, defend, and hold harmless Company and its officers, directors, employees, and Assistants, from and against any claims arising from Vendor's failure to do so.

21. Changes. Company may at any time during the performance of Services require additions, deductions, or deviations (all hereinafter referred to as a "Change") from the Work. No Change shall be considered as an addition, alteration, or deduction from the Work, nor shall Vendor be

entitled to any compensation for Work done pursuant to or in contemplation of a Change, unless made pursuant to a written Change Order issued by Company.

22. Warranty and Standard Performance.

a. During the Term of this Agreement, Vendor warrants that (i) it shall perform the Services in good faith and with due professional care, in conformance with applicable professional industry standards; (ii) that all Assistants utilized by Vendor have the knowledge, education, training, skills, and experience in the subject matter they are engaged to address or the tasks they are assigned, including certification where required by third party licensors of Company, to perform the tasks assigned to them; and (iii) all Vendor's employees and Assistants performing Services under this Agreement are legally authorized to perform the work and the Vendor has fully complied with all employment verification laws of the U.S. Vendor warrants that it shall perform the Services in conformance with the documentation, specifications, and instructions as set forth in the applicable SOW. For Services performed not meeting this warranty, Vendor shall re-perform such Services at no cost to Company.

b. Vendor warrants that any software, interfaces, scripts or other code provided or otherwise created by Vendor under this Agreement ("Software") shall be delivered and operable according to the specifications provided by Company and set forth in an SOW. For Software not meeting this warranty, Vendor shall correct any deficiency in the Software (such correction period not to exceed sixty (60) days, unless otherwise agreed to by the parties). If such deficiency cannot be corrected, Vendor shall refund any fees and costs related to such Software. This warranty shall survive for a period of twelve (12) months from delivery of the Software.

c. During the Term of this Agreement, Vendor warrants that no malware, worms, date bombs, or time bombs, the purpose or effect of which is to cause any software or hardware to cease operating, or to damage, interrupt, interfere with, or hinder its operation (collectively, "Malware") shall be coded or introduced by Vendor into any software, including Company software, or any element of Company's computing environment or system, including hardware and software. During performance of the Services, Vendor warrants that it will not use vulnerable libraries, vulnerable configurations, and/or vulnerable code, including, without limitation, common weakness enumerations ("CWE"), vulnerable security configurations, or known vulnerable libraries. If the foregoing warranty is breached, Vendor shall, at no charge to Company and in addition to any other remedies available to Company at law or equity, remove the Malware and/or remediate the vulnerabilities and assist Company in reducing the effects of the Malware and vulnerabilities, and, if the Malware or vulnerabilities cause loss of operational efficiency or loss of data, Vendor shall cooperate to the same extent to mitigate and restore such losses.

d. During the Term of this Agreement, consistent with the Security Measures in Exhibit 1, Vendor warrants that it shall implement and provide industry standard data security protocols, procedures, and measures to prevent, to the extent possible, intrusion by hackers, other unauthorized persons, or unauthorized scripts or services, in the Vendor computing environment or system or Company's computing environment or system. Vendor shall at all times comply with its own security policies and procedures and the system security and environment requirements described in a Statement of Work and this Agreement.

e. Vendor represents and warrants that it currently implements, and will continue to implement during the Term, the Security Measures set forth in Exhibit 1, including: (i) it currently has in place or employs network security, business continuity, and disaster recovery policies and procedures commensurate with industry-wide best practices; (ii) it currently has and will continue to employ sufficient controls, procedures, and systems to securely and reliably maintain the confidentiality of all data stored and used pursuant to this Agreement; and (iii) it will maintain and update the foregoing plans as appropriate during the Term of this Agreement and at all times during which it has personal identifiable information or Company Data in its possession.

f. Vendor warrants that all Deliverables will be provided in accordance with all specifications, drawings, instructions, or documentation as agreed upon by the parties under this Agreement. For Deliverables provided not meeting this warranty, Vendor shall correct any deficient Deliverables (such correction period not to exceed sixty (60) days, unless otherwise agreed to by the parties). If the deficiency in the Deliverable cannot be corrected, Vendor shall refund to Company the fees and costs related to such Deliverable. This warranty shall survive for a period of twelve (12) months from acceptance of the Deliverable.

g. Vendor represents and warrants that it shall adhere to the standards and guidelines for software development and DevSecOps described in "Exhibit 2 – Secrets Management" as such policy may be updated from time to time by Company.

23. Confidentiality.

a. A party (the "Discloser") may disclose to the other party (the "Recipient") information that the Discloser considers to be confidential ("Confidential Information"). Confidential Information shall include, but is not limited to, any information not generally shared by Discloser to the public, the Services and any Deliverables, pricing, and all data, trade secrets, business information and other information, relating to the Discloser, its business, customers, suppliers, vendors, competitors or otherwise, whether in tangible or intangible form and however conveyed or made accessible to Recipient, during the Term of this Agreement. Recipient shall use the same degree of care to protect the confidentiality of Discloser's Confidential Information that Recipient uses to protect its own Confidential Information of a like nature, but in no event less than reasonable care. The Recipient may disclose Discloser's Confidential Information to its third-party providers solely to the extent necessary for the business purposes pursuant to this Agreement, as applicable.

b. Except as it relates to personally identifiable information, for which exceptions (i) – (iv) below shall not apply, a party's Confidential Information shall not include information that: (i) is or becomes publicly available through no act or omission of Recipient; (ii) was in the Recipient's lawful possession prior to the disclosure and was not obtained by Recipient either directly or indirectly from the Discloser; (iii) is lawfully disclosed to the Recipient by a third party without restriction on Recipient's disclosure, and where Recipient was not aware that the information was the confidential information of Discloser; or (iv) can be demonstrated by the Recipient (and supported by competent written records) to have been developed independently by the Recipient or its employees, agents and contractors, without use of, reference to, or access to Discloser's Confidential Information. The Recipient may disclose Confidential Information pursuant to a subpoena or other legal or administrative demand for disclosure; provided, however, that the Recipient has given the

Discloser prompt notice of such demand for disclosure to the extent permitted by applicable law and the Recipient reasonably cooperates with the Discloser's efforts at Discloser's expense to secure an appropriate protective order.

c. In the event the Vendor obtains Company's employee(s)' or customers' personally identifiable information, Vendor acknowledges and agrees that it has in place and maintains appropriate security measures and safeguards to prevent the disclosure of personally identifiable information, consistent with Applicable Law and the Security Measures set forth in Exhibit 1.

d. For the purposes of this Agreement, each party shall be deemed the owner of its Confidential Information.

e. Upon termination of this Agreement or at any time upon Discloser's request, the Recipient will return the Discloser's Confidential Information (or identified portions thereof as requested) to the Discloser and will then remove and destroy all of the Discloser's electronic Confidential Information from Recipient's servers and systems, and any and all copies of such information, in whatever format, within a reasonable time period not to exceed thirty (30) days after such termination and certify in writing that such removal and destruction has occurred within such time period, provided that: (i) the Recipient shall not be obligated to delete or destroy such information stored on backup media for disaster recovery purposes (which shall be deleted through the Recipient's normal backup media recycling plan); (ii) Recipient shall not be obligated to develop new technology or incur unreasonable expenses to delete or destroy electronic information that is not readily accessible through the available functionality of the applicable system; and (iii) Recipient shall be allowed to retain such copies of the Confidential Information as are necessary to meet any legal or regulatory requirements or for accounting purposes. Any such information that is retained for any of the foregoing reasons shall remain subject to the confidentiality obligations set forth in this Agreement indefinitely.

f. The parties acknowledge that disclosure of any Confidential Information may give rise to irreparable injury to the Discloser, which injury may be inadequately compensated in damages. Therefore, the Discloser may seek injunctive relief against the Recipient's breach or threatened breach of this Section (Confidentiality) as well as any other legal remedies that are available.

24. Compliance with Laws. Vendor shall comply at its own expense with all applicable laws, ordinances, regulations and codes, including, but not limited to (i) all U.S. Employment Authorization Requirements and (ii) the identification and procurement of required permits, certificates, licenses, insurance, approvals and inspections in performance under this Agreement and shall indemnify, defend and hold harmless Company and its officers, directors, employees and Assistants, from and against any claims arising from Vendor's failure to so comply and, further, shall provide Company with evidence of such compliance as may be requested by Company from time to time during the Term.

a. Vendor will ensure that any personal information ("PI") that is included in Company Data, or Company Sensitive Information is protected against misuse and loss, and from unauthorized access, modification or disclosure, by (i) complying with the Security Measures set forth in Exhibit 1; (ii) complying with all privacy laws and other applicable laws with respect to such PI and its collection; (iii) not using the Company Information other than necessary to perform pursuant to this Agreement or the applicable SOW; (iv)

not process or maintain the PI outside the United States; (v) not disclose the PI to any third party; (vi) disclose PI to its employees only a need to know basis; and (vii) deliver to Company and/or destroy all copies of the PI upon request by Company.

b. Vendor will inform Company in writing and by email (privacy2@darden.com) as soon as reasonably practicable if Vendor receives any communication from (or on behalf of) any individual to whom the PI relates, concerning any request that Vendor provide access to such PI or any complaint in relation to that PI. Vendor must take no other action in relation to any such communications (including making any response to the individual concerned) until Vendor consults with Company (except to the extent that such action is required by law) and receives direction from Company regarding the timing, content and procedure of any possible communication and Company's consent for Vendor to do the same, so long as Company provides such direction in a reasonable timeframe after Vendor' notification.

c. Vendor will comply with all Americans with Disabilities Act ("ADA") requirements relating to online software, including, without limitation, using ADA accessible web design, having universal web site accessibility and making the Services and Software compatible with software accessibility programs.

25. Use of Marks. Vendor does not have the right to publicize or advertise in any manner the Services Vendor is providing to Company or Vendor's relationship with Company. Vendor will have no right or authority to use, display, license, refer to, or in any way benefit from Company's Marks in any manner. Vendor will not indicate, and Company grants no permission for Vendor to indicate, in any manner whatsoever that Vendor or the Services are endorsed or sponsored by Company or any of its affiliates, subsidiaries or parent.

Vendor does not own any interest whatsoever in the Marks. Vendor will refrain from making any claims or asserting any right or interest in the Marks. "Marks" means any semblance of any trade name, trademark, service mark, insignia, symbol, logo, or any other designation or drawing of the Company, or its affiliates, subsidiaries or parent. Vendor shall remove or destroy any Marks prior to any use or disposition of any material rejected or not purchased by Company.

26. Indemnity. Vendor agrees to indemnify, defend, and hold harmless Company, its affiliates and their customers, officers, directors, employees, agents, successors and assigns (all referred to in this clause as "Company") from and against any losses, damages, claims, liabilities, fines, penalties, and expenses (including reasonable attorney's fees) that arise out of or result from: (1) injuries or death to persons or damage to property, including theft, in any way arising out of or caused or alleged to have been caused by the Services performed by, or material provided by Vendor or any persons furnished by Vendor; (2) assertions under Workers' Compensation or similar acts made by persons furnished by Vendor and/or (3) Vendor's gross negligence and/or willful misconduct in its performance pursuant to this Agreement. Vendor shall not be liable for such indemnification resulting from (1) or (2) above if and to the extent such damages are determined by a court of competent jurisdiction to have been caused by the gross negligence of Company. For purposes of this Section, "similar acts" includes any claim brought by Vendor's employee(s) that would be considered a workers' compensation claim if brought against Company by one of Company's own employees. At Company's sole option, Vendor will defend any of the foregoing claims at its sole cost including but limited to all losses and expenses associated therewith with counsel of its choosing provided such counsel is reasonably acceptable to Company. Company also has the right to retain counsel of its own choosing at Vendor's cost. At no time will Vendor have the right to settle any claim without the prior approval of Company.

27. Indemnity: Infringement. Vendor shall indemnify, defend, and hold harmless Company, its affiliates and their customers, vendors, and suppliers and their respective officers, directors, employees, successors, and assigns (all referred to in this clause as "Company") from and against any losses, damages, liabilities, fines, penalties, and expenses (including reasonable attorneys' fees) that arise out of or result from any and all claims (1) of infringement or violation of any patent, copyright, trademark, or trade secret right, or other intellectual property right, privacy right, or any other proprietary or personal interest, and (2) related to the existence of this Agreement or performance under or in contemplation of it (each, a "Claim"). Following notice of a Claim or any facts that may give rise to such Claim, Vendor may, in its sole discretion and expense, (a) procure for Company the right to continue to use the Software, Services, or Hardware ("Solution"), (b) replace the Solution with non-infringing Solution that are materially equivalent in functionality to the Solution or (c) modify the Solution that is the subject of the infringement claim so that it has materially equivalent functionality and is no longer infringing. Further, Vendor agrees to indemnify, defend, and hold harmless Company from any taxes, fines or penalties imposed by any governmental authority as a result of Vendor's violation of any applicable law in its performance of obligations pursuant to this Agreement. Company shall timely notify Vendor of any assertion against it of any Claim and shall cooperate in good faith with Vendor in the defense of any such Claim at Vendor's expense. Vendor, in addition to its indemnity obligations set forth herein, shall immediately refund to Company any amounts paid for the Solution.

28. Insurance. Vendor shall maintain and cause Vendor's subcontractors, if any, to maintain during the term of this Agreement: (1) Workers' Compensation insurance as prescribed by the law of the state in which the Work or Services are performed; (2) employer's liability insurance with limits of at least $1,000,000.00 for each occurrence; (3) automobile liability insurance if the use of motor vehicles is required, with limits of at least $1,000,000.00 combined single limit for bodily injury and property damage per occurrence; (4) Commercial General Liability ("CGL") insurance, including Blanket Contractual Liability and Broad Form Property Damage, with limits of at least $1,000,000.00 combined single limit for bodily injury and property damage per occurrence; (5) Professional Liability insurance in the amount of $1,000,000.00; and (6) cybersecurity insurance (covering costs arising from data destruction and/or theft, extortion demands, hacking, denial of service attacks, crisis management activity related to data breaches, and legal claims for defamation and privacy violations), with limits of at least $2,500,000.00 for each occurrence.

All Vendor CGL, automobile liability insurance and cybersecurity insurance shall designate Company, its affiliates, and their directors, officers, agents, and employees (all hereinafter referred to in this clause as "Company") as additional insured. All such insurance must be primary and non-contributory and required to respond and pay prior to any other insurance or self-insurance available. Any other coverage available to Company shall apply on an excess basis. Vendor agrees that Vendor, Vendor's insurer(s) and anyone claiming by, through, under or on Vendor's behalf shall have no claim, right of action or right of subrogation against Company and its customers based on any loss or liability insured against under the foregoing insurance. Vendor and Vendor's subcontractors shall furnish prior to the start of Work certificates or adequate proof of the foregoing insurance, including, if specifically requested by Company, endorsements and policies. Company shall be notified in writing at least thirty (30) days prior to cancellation of or any change in the policy. Insurance companies providing coverage under this Agreement must be rated by A.M. Best with at least an "A" rating.

29. Notices. Except as otherwise provided herein, all notices, requests, consents, and approvals under this Agreement will be in writing and will be deemed to have been properly given if transmitted electronically via email provided that a delivery receipt is obtained by the Party

sending the notice to the email address set forth in the Agreement, Purchase Order, or at such other email address as any of the Parties hereto from time to time may have designated by written notice to the other Party.

30. Assignment. Vendor shall not assign, directly or indirectly, voluntarily or by operation of law, any of its rights or obligations under this Agreement without the prior written consent of Company, and any such attempted transfer shall be null and void. Notwithstanding the preceding sentence, Vendor may, upon prior written notice to Company, assign this Agreement in connection with a merger, acquisition, sale or other transfer of all or part of its business, or in connection with an internal corporate reorganization, change of control or other similar arrangement; provided, however, Company will have the option to immediately terminate this Agreement and any SOW without liability to Vendor. Company may freely assign this Agreement. This Agreement shall be binding and inure to the benefit of the Parties and their successors and permitted assigns.

31. Force Majeure. Neither party shall be held responsible for any delay or failure in performance of any part of this Agreement to the extent such delay or failure is caused by fire, flood, strike, civil, governmental or military authority, act of God, or other similar causes beyond its reasonable control and without the fault or negligence of the delayed or nonperforming party or its subcontractors.

32. Survival of Obligations. The obligations of the parties under this Agreement, which by their nature would continue beyond the termination, cancellation, or expiration of this Agreement, shall survive termination, cancellation, or expiration of this Agreement.

33. Waiver. The failure of either party at any time to enforce any right or remedy available to it under this Agreement or otherwise with respect to any breach or failure by the other party shall not be construed to be a waiver of such right or remedy with respect to any other breach or failure by the other party.

34. Choice of Law. This Agreement and all transactions under it shall be governed by the laws of the State of Florida excluding its choice of laws rules.

35. Alternate Dispute Resolution. Before submitting any claim, controversy or dispute arising out of this Agreement to litigation or other legal proceedings (except actions seeking extraordinary relief, i.e., specific performance or an injunction), the complaining party will provide written notice to the other of the claim, controversy or dispute, and each will, as promptly as practical, appoint one or more senior executives with authority to settle such claim, controversy or dispute who will meet with each other in good faith for the purpose of resolving the claim, controversy or dispute. If a dispute arises related to this Agreement, or its breach, and the parties have not been successful in resolving such dispute through negotiation, the parties agree to attempt to resolve the dispute through mediation by submitting the dispute to a sole mediator selected by the parties or, at any time at the option of a party, to mediation by the American Arbitration Association ("AAA"). Any such mediation will be held in Orange County, Florida. Each party shall bear its own expenses and an equal share of the expenses of the mediator and the fees of the AAA. All defenses based on passage of time shall be suspended pending the termination of the mediation. If the claim, controversy or dispute is not resolved by mediation in accordance with this Section within 60 days following the selection of a mediator in accordance with the foregoing, either Company or Vendor may elect to pursue available remedies with respect to the claim, controversy or dispute in accordance with this Agreement. In the event a legal action is brought by one party against the other party after unsuccessful mediation to enforce or interpret any term, provision or covenant of this Agreement, the prevailing party in such action shall be entitled to recover the

reasonable costs of such action, including, without limitation, court costs, reasonable attorneys' fees and discovery costs, from the non-prevailing party. Nothing in this clause shall be construed to preclude any party from seeking injunctive relief in order to protect its rights pending mediation.

36. Severability. If any of the provisions of this Agreement shall be invalid or unenforceable, such invalidity or unenforceability shall not invalidate or render unenforceable this entire Agreement, but rather this entire Agreement shall be construed as if not containing the particular invalid or unenforceable provision or provisions, and the rights and obligations of the parties shall be construed and enforced accordingly.

37. Conflict Of Interest. Vendor agrees to refrain from (i) giving commissions, payments, gifts, kickbacks, lavish or extensive entertainment, or other things of value to any employee or agent of Company in connection with this Agreement; or (ii) allowing employee's family members or partners outside of Company (including without limitation, in-laws, life partners, business partners and the like) to be involved in the decision making process or to be an influencer in connection with this Agreement. Vendor shall not engage in any behavior or encourage action by Company's employees that is contrary to (a) Company's policies regarding conflicts of interest (www.darden.com/corporate/), (b) public policy, or (c) any applicable local, state, federal, or international law, regulation, ordinance, standard, or guideline. In the event that Vendor takes any action contrary to Company's interests under this Agreement, or in furtherance of Company's employee's prohibited behavior (including but not limited to the examples above), Vendor shall promptly notify Company, and Company may, at its option, terminate this Agreement without any further obligation to Vendor.

38. Systems Access and Equipment Bailment. Vendor may be provided access to Company's computer or electronic systems ("System Access"). System Access applies to all types of computer or electronic systems (or any substitute therefor) including, but not limited to, any third-party computer or electronic systems, e-mail, intranet, internet, extranet, and telephone voicemail to which Vendor may be given access. Vendor shall be responsible for all of Vendor's actions relating to such system including use of any logon IDs, passwords, or other authentication methods provided to Vendor. All Vendor connectivity or attempted connectivity to Company computing systems shall be only through Company's security gateways or Company's firewalls. Vendor shall not access, and shall not permit unauthorized persons or entities within its control to access, Company's computing systems without Company's express written authorization and any such actual or attempted access shall be consistent with any such authorization. To the greatest extent possible, Vendor shall restrict System Access to Company's network and computer systems to the least degree of access required for performance of any Services. Vendor shall use System Access exclusively for the performance of Services. If Company provides any equipment (including, without limitation, hardware, software and stored data) to Vendor, Vendor shall keep and safeguard such equipment as a bailee and use such equipment only to perform the Services.

39. Assistants. From time to time, Vendor may, subject to the terms and conditions set forth in this Agreement, engage employees, independent contractors, consultants, volunteer assistants or other persons or entities (collectively, "Assistants") to aid Vendor in performing Vendor's duties under this Agreement. Neither Company nor any of its subsidiaries, affiliates or related companies has any relationship with or to such Assistants and such Assistants are not employees, agents, consultants, representatives, assistants or independent contractors of Company, its subsidiaries, affiliates, or related companies. Vendor shall be fully and solely responsible for the supervision of such Assistants, compliance by such Assistants with U.S. Employment Authorization Requirements and for all work performed by such Assistants and any

third-party subcontractors approved by Company as provided in this Agreement. In the event that any Assistant performing Services is found to be unacceptable to Company for cause or without cause, including, but not limited to, demonstration that he or she is not qualified to perform such Services, Company shall notify Vendor of such fact and Vendor shall immediately remove said Assistant from performing Services and, promptly provide a qualified replacement. In addition, Vendor shall not remove any Assistant providing Services under agreement without the prior written consent of Company. Vendor shall ensure that all Assistants comply with the terms of this Agreement, including but not limited to the Confidentiality obligations hereunder, and Vendor will be responsible for any violation of this Agreement by its Assistants.

40. Authorization Verification Requirements.

a. Company requires that Vendor, and its Assistants, comply with immigration laws that require verification of employment authorization, including, but not limited to, labor and employment laws such as the Immigration Reform and Control Act of 1986, as amended, and the Illegal Immigrant Reform and Immigrant Responsibility Act of 1996, as amended.
b. In order to ensure to Company that Vendor is in compliance with the law, Company requests and requires the following:
    i. Adopted Plan of Compliance
        1) By signing this Agreement, Vendor attests that it has adopted a plan of compliance that is in effect as of the Effective Date of this Agreement. Vendor assures that its compliance plan includes, but is not limited to:
            (a) timely, proper completion of I-9 forms and verification of employment authorization;
            (b) timely reverification of I-9 forms for employees with expiring employment authorization;
            (c) proper training of personnel who will prepare I-9 forms; and
            (d) periodic audits of I-9 forms.

        2) In addition to the above conditions for the compliance plan, by signing this Agreement Vendor confirms that the following requirements will apply for its Assistants working on Company projects:
            (a) All Assistants must maintain on their person a valid government-issued identification card; and
            (b) Copies of I-9s and supporting documentation for each Vendor and Assistant working on Company projects will be maintained by Vendor.

    ii. Certification of Compliance
        1) By signing this Agreement, Vendor attests that:
            (a) it has had a qualified legal or human resources professional review the I-9 forms, and supporting documentation, for all employees and Assistants of Vendor who will work on any Company project and/or on any Company facilities;
            (b) the identity and employment authorization documentation of each Assistant appear to be valid and genuine on their face;
            (c) Vendor is in compliance with the immigration employment verification requirements set forth in the immigration laws referenced above; and
            (d) Vendor will impose these same requirements of an adopted plan of compliance and a certificate of compliance on its subcontractors, if any, who work on any Company project and/or on any Company facility(ies).

iii. Third Party Audit

By signing this agreement, Vendor agrees that, at Company's sole discretion, Company may require Vendor to submit to and cooperate fully with a third-party audit of the I-9 forms and related documents at Company's expense. Additionally, Company requires that Vendor reserve for Company the right to audit Vendor's subcontractors, as well.

41. Export Control Regulations and Deemed Exports.

a. Vendor will not directly or indirectly transmit, by way of transshipment, export, reexport, diversion or otherwise, any Work Product or Confidential Information of Company to any destination or location outside the United States except as authorized by Company and in accordance with the U.S. export control laws and regulations.
b. Vendor acknowledges that the export control laws may apply to the disclosure or release of certain technology and software to a foreign national located in the United States, and that Vendor will not release to any unprotected foreign national any Work Product or Confidential Information of Company except as authorized by Company and in accordance with U.S. export control laws and regulations.
c. In order to comply with U.S. export control laws and regulations, Vendor agrees that it will not assign any unprotected foreign national to work on Company projects unless Vendor has: (i) identified the unprotected foreign national to Company (ii) provided Company with all information necessary for Company to make an export licensing determination; and, (iii) has received from Company permission to assign such unprotected foreign national to Company's work. "Unprotected foreign national" shall mean a person who is not a protected individual under the Immigration and Naturalization Act ("INA") (8 U.S.C. sec. 1324b(a)(3)). Protected individuals generally include U.S. citizens, U.S. nationals, lawful permanent residents, lawful temporary residents, refugees and asylees. Possession of a valid work visa does not necessarily confer protected individual status on an individual.

42. Entire Agreement. This Agreement and any SOW attached hereto contain the entire agreement between the parties hereto with respect to the subject matter hereof, and no understandings relative to the contents of this Agreement exist between the parties other than as expressed herein. Any proposal, purchase order, document or transaction record utilized by Vendor shall be for administrative convenience only, and any terms therein which conflict with this Agreement shall be deemed null and void during the entirety of the relationship. No representation or statement not contained in this Agreement shall be binding upon the parties as a warranty or otherwise, nor shall this Agreement or any SOW be modified or amended except by a writing signed by Vendor and Company.

Exhibit 1: Security Measures

1. Asset Management
   1.1 Vendor maintains an inventory of IT assets supporting the Services including internal and external systems.

2. Governance
   2.1 Vendor maintains an Information Security Program (ISP) based on industry best practices and recognized frameworks.
   2.2 Vendor's Security & Compliance Director and Information Security Committee are responsible for information security.
   2.3 Vendor requires contractors and employees to sign a Confidentiality Agreement and Acceptable Use Policy on hire.

3. Risk Management
   3.1 Vendor maintains risk management processes to identify, assess and manage risks to Company Data and IT systems supporting the Services. Vendor will promptly report material risks which may affect Company Data or the Services to the Company.
   3.2 Vendor conducts an information security risk assessment at least once annually and manages risks to Company Data and IT systems supporting the Services in accordance with documented risk management procedures.
   3.3 Vendor conducts vulnerability scans against infrastructure and applications in accordance with their risk to Company, to help identify vulnerabilities and promptly remediates any security vulnerabilities and misconfiguration.
   3.4 Vendor conducts penetration testing of its external network at least one time per year using independent testing professionals and promptly remediates identified vulnerabilities.
   3.5 Vendor conducts penetration testing of its applications at least annually and promptly remediates all critical and/or high findings, confirmed by a re-test within sixty (60) days.

4. Awareness and Training
   4.1 Vendor ensures that Personnel complete information security awareness training and are made aware of their responsibilities with regards to information security and the handling of Company Data.
   4.2 Vendor provides Personnel with clear instructions and awareness for using Company Data and IT systems, including, but not limited to, the following requirements:
      a) Keep Confidential Information and IT equipment secure at all times, including when travelling or working out of the office or from home;
      b) Keep User ids, passwords and PINs for IT systems and devices, confidential and protect them from unauthorized access;
      c) Do not connect untrusted removable media devices to IT systems or laptops;
      d) Keep devices used to access Company Data and IT systems up-to-date with security updates;
      e) Interacting with Company Data in accordance with Vendor's classification and documented handling procedures;
      f) Only share Company Data with authorized individuals on a need-to-know basis;
      g) Encrypt Company Data when emailing or sharing externally;
      h) Check before sending emails containing Company Data that all the recipients are authorized to receive the Company Data;
      i) Be aware of phishing and do not click on links in emails or documents or provide any Company Data over the phone without verifying the caller;
      j) Do not use personal instant messaging services or personal email accounts to conduct Company business or to share or receive Company Data;
      k) Be discreet when discussing Company Data so you cannot be overheard and do not share Company Data online, including using the social media, external social networks, instant messaging or blogging sites;

l) Maintain a clear desk and a clear screen so that Company Data cannot be viewed or accessed by unauthorized individuals;
m) Do not leave Company Data unattended or on voicemails;
n) Securely dispose of paper and other media using correct procedures; and
o) Report security events and non-compliance with security policies promptly and without delay.

5. Access Control

5.1 Vendor restricts physical and logical access to IT systems supporting the Services to only the minimum levels of access and privileges required to perform a function or role.
5.2 New access to Company network, systems, and data are approved and documented.
5.3 Vendor assigns Users a unique ID; shared accounts are prohibited.
5.4 Vendor implements identity and access management processes to control access and authenticate Users prior to granting access.
5.5 Vendor uses Multi-Factor Authentication for remote User virtual private network access to Company network systems.
5.6 Vendor revokes access for Users no longer working on the Services or those that no longer require access.
5.7 Vendor reviews User accounts and their privileges on a regular basis, to verify that access to IT systems supporting the Services is correct.
5.8 Vendor enforces the use of password complexity, minimum length of ten (10) characters, password changes over Company determined intervals, and lockout after six (6) unsuccessful login attempts.
5.9 Vendor ensures that remote access to IT systems and networks supporting the Services is restricted to only authorized individuals using secure entry-points and approved devices.

6. Data Security

6.1 Vendor maintains procedures and controls to protect the security of Company Data (to the extent such Company Data or the environment under which it is stored is under Supplier's direct control) at every stage of its lifecycle from creation through processing, storage and disposal.
6.2 Vendor enforces full-disk encryption on portable devices accessing Company Data.
6.3 Vendor encrypts Company Data in transit.
6.4 Vendor maintains the security of systems and employee laptops using standardized builds that include a hardened operating system, malware protection, and host-based security software.
6.5 Configuration changes are limited to authorized individuals, in accordance with documented change management procedures and using approved systems and tools.
6.6 On request, Vendor will securely delete Company Data from IT systems in accordance with current industry standards such as NIST 800-88 or an equivalent.

7. Application Security

7.1 Vendor only uses Company Data for testing as necessary to deliver the Services to Company as prescribed in the applicable agreement.

8. Security Monitoring & Detection

8.1 Vendor's security department is responsible for security monitoring and detection activities. At a minimum, Vendor shall ensure effective monitoring of privileged user activities and security events including but not limited to login attempts, hostnames/IP addresses connections, date and time of connections. Vendor shall ensure that the systems used to perform the Service are under continuous monitoring with current up-to-date solutions including but not limited to SIEM, IDS/IPS and Firewalls. Vendor shall provide all logs related to all monitoring activities in a mutually agreed format, time and date interval and through a secure transfer method.
8.2 Vendor maintains content filtering technologies to monitor connections to the internet.

8.3 Vendor monitors CERT notifications that may affect any element of its IT systems and patch systems in accordance with a documented procedure that prioritizes the remediation of vulnerabilities based on risk.

8.4 Minimum Requirements on Data Backup and Recovery:
Vendor shall use appropriate backup solutions and other measures to ensure that recovery time objective of four (4) hours and recovery point objective of two (2) hours are met and (if applicable) emergency service levels are complied with.
Vendor shall have an effective, documented and regularly reviewed process in place used to inform Customer in case of a disaster affecting the Service; including defined response times, modes of communication and interfaces.

9. Incident Response

9.1 Vendor maintains security incident response plans to manage response to security events, and these are evaluated on at least an annual basis.

9.2 Vendor will consult with Company prior to conducting forensic investigation following an incident affecting Company Data or the environment under which it is stored (to the extent the same is under Vendor's direct control) and conduct investigations in accordance with legal requirements for preserving evidence. Vendor will keep Company apprised of the forensic investigations and remediation.

9.3 Vendor will contain and mitigate incidents in accordance with documented incident management procedures and response plans.

9.4 Vendor will mitigate newly identified vulnerabilities. Any vulnerabilities that cannot be fixed, that could have a material impact on the security of Company Data will be reported to Company.

9.5 Vendor will conduct post incident reviews to identify root-causes and identify actions required to minimize the risk of similar incidents re-occurring. Response strategies and plans will be updated in response to any lessons learned.

10. Third Party Risk Management

10.1 Vendor's security department maintains a third-party risk management program to ensure that third parties maintain security controls at least as stringent as Vendor's security controls and continually assess the third party on a regular basis in accordance with its risk level as defined by Vendor.

10.2 Third parties are obligated, by contractual agreement, to maintain security controls at least as stringent as Vendor's security policies dictate.

10.3 Third parties are obligated, by contract, to securely delete data at the end of contract.

Exhibit 2: Secrets Management

1 Secrets Management

1.1 Purpose and Scope

Vendor shall adhere to these standards and guidelines for software development and DevSecOps efforts in this Exhibit 1 as is amended by Company from time to time.

Document Scope:

This Exhibit 1 outlines requirements Vendor agrees to follow for Secrets Management as it relates to Vendor's software development, deployment, and runtime related to the Services performed by Vendor pursuant to the Agreement. The scope of this Exhibit 1 does not include identity and access management, secure coding practices, PCI/PII/SOX standards, or governance for users and devices, which may be covered in different sections of this Agreement.

2 Guidance and Standards

2.1 Definition of Secrets

Secrets are digital credentials for authentication or authorization as it pertains to building, configuring, deploying, operating, integrating, or monitoring software. Secrets include, but are not limited to:

- API keys
- Azure DevOps Personal Access Tokens
- Cryptographic keys and hashes
- Database connection strings and credentials
- Digital certificates
- OAuth, JSESSIONID, JWT, SMSESSION or other session tokens
- SSH keys
- Storage account keys
- Usernames and passwords for individuals, service principals, or service accounts
- Any other piece of data that may be used to provide authentication or authorization to secured assets or processes

Secrets Management refers to the policies and procedures for handling Secrets.

2.2 Secrets Management Scope

The practices and guidelines defined within this Exhibit 1 apply to the following contexts, irrespective of the operational state of any application or process:

- Development of custom applications and their components and features
- Modification and extension of third-party applications
- Development of tools and utilities
- PowerShell, Bash, or other scripts for any purposes
- DevSecOps implementations including Classic or YAML CI/CD pipelines and associated scripts
- Configuration and property files
- Documentation files & publications
- Digital capture of information via screenshot or video capture
- Audio recordings
- Vendor's use of Company's systems or that of its third-party licensors where the context is applicable.

These practices and guidelines are relevant and applicable regardless of the general accessibility of any qualifying artifact, physical location, or other compensating factors.

2.3 Requirements:

2.3.1 Keeping Secrets Safe at Generation/Creation

- Vendor shall generate Secrets of sufficient type, length, and complexity according to established Company Cybersecurity standards and with approved tooling.
- Vendor shall scope Secrets to a unique resource in a unique environment. For instance, a database shall not use the same password for Stage and Production instances.
- Vendor shall ensure that Secrets are stored in approved Secret/password managers.
- Vendor shall not share Secrets with other users unless such sharing is necessary and on a need-to-know basis where such users are subject to the applicable confidentiality requirements and terms of use.
- Vendor, when involved in Secrets creation, shall create those Secrets through an automated process, where feasible. Automatically generating credentials removes one of the key weaknesses of Secret Management: human-generated credentials tend to be easier to crack than computer-generated ones.
- Vendor shall change Secrets already in use on a regular schedule. This is often specified and required by different standards, such as PCI DSS which mandates a maximum 90-day rotation cycle. It can take the form of automatically regenerating a new Secret on a schedule, or of prompting for manual creation.
- Vendor shall implement Secrets in a way that makes it easy to revoke and regenerate them as needed.

2.3.2 Keeping Secrets Safe with Users

- Vendor shall not share credentials with other users unless such sharing is necessary and on a need-to-know basis only where such users are subject to the applicable confidentiality requirements and terms of use and furthermore only if these Secrets are associated with a service account and not a personal identity.
- Vendor and Vendor's users shall authenticate to services using the Vendor's own identity or a token or key that represents their identity where feasible.
- Vendor and Vendor's users shall not send Secrets over email or other insecure channels where messages could be saved or forwarded.
- Vendor and Vendor's users shall use Company approved passwords/Secret managers.
- Vendor and Vendor's users shall use Company approved key stores for digital certificates.
- Vendor shall not permit developers and non-administrative personnel to access or maintain production Secrets.
- Vendor and Vendor's users shall use the principle of least privilege: developers shall have Secrets with the minimum scope needed to perform their duties.
- Vendor shall ensure that developers and users of all types receive adequate warnings regarding the risks of trusting public websites and tools and shall instruct these users not to do so. This instruction shall include an admonishment to never paste code into a website that contains a Secret. Specifically, Vendor and Vendor's users, when needing to use an online tool to format, convert, or review code, must remove any Secrets before pasting the code into the website.
- Vendor shall instruct and coach Vendor's users that Secrets of all types are sensitive. A Secret used for functional test automation that is compromised can be detrimental, for example.
- Vendor shall encourage Vendor's users to help identify hardcoded Secrets that need to be prioritized for removal, or to identify weak, unneeded, or stale Secrets that need to be revoked or regenerated.

2.3.3 Keeping Secrets Safe During Development

- Vendor shall not hardcode Secrets or commit Secrets to source code or documentation of any type.
- If Vendor finds existing Secrets, the Vendor shall remove the Secrets from source code as a priority. The Secrets shall also be removed from the source code history which is easily retrievable. Refer to guides such as Removing sensitive data from a repository - GitHub Docs to scrub Secrets from source control history.

- Vendor shall promptly notify Company Cybersecurity of any potential breaches or leaks without undue delay in order to take proper measures, which may include revoking or rotating Secrets that were committed to source control. In the event any other section of the Agreement including, but not limited to, appendices or schedules has specific breach notification terms, those terms shall control in relation to the context and subject matter of such.
- Vendor shall implement enforced code reviews / peer reviews for all coding changes to ensure Secrets are neither being committed to source code or documentation, nor implemented in pipelines without being protected.
- Vendor shall not log Secrets in audit or error logs. Vendor shall implement the correct type of Secret given the nature of the integration or software implementation and shall consult the Architecture Review Board and Cybersecurity for security best practices that Vendor must implement.

2.3.4 Keeping Secrets Safe During Deployment

Whenever feasible, Vendor shall externalize application configuration, including Secrets, from the binaries that are deployed. These needed configurations shall be injected/configured during deployment time through release automation or maintained separately and securely within each individual environment.
Vendor shall deploy application artifacts through Azure DevOps release pipelines or other approved platforms through automated means, where feasible, to reduce access to Secrets by individuals. Secrets shall be retrieved from an approved Secret manager such as Azure Key Vault or with password-protected Azure Pipeline variables.
Vendor shall ensure that only authorized designees maintain the password protected pipeline variables for production Secrets.

2.3.5 Keeping Secrets Safe in Transit

Vendor shall use approved application integration technologies and secured protocols (e.g., HTTPS, SFTP, etc.) to keep Secrets safe in transit and shall consult the Architecture Review Board for best practices and solution proposals that Vendor must implement.

2.3.6 Keeping Secrets Safe at Runtime

Vendor shall not hardcode Secrets in source control, configuration, or documentation files in Applications. Instead, the application shall pick up Secrets at runtime from an approved source designated by Company which may include one or more of the following:

- Azure Key Vault or other approved Secret managers/vaults.
- Environment variables. Only administrators shall have access to remote into production servers and view/edit Secrets in environment variables.
- Encrypted files, secured directories, and/or password-protected key stores that only administrators and the application identity have access to. These shall be maintained outside of the source code.

The application shall run under an established identity so it can authenticate to the source of Secrets at runtime. The Secrets shall be easy to revoke and regenerate at runtime.

2.3.7 Keeping Secrets Safe with SAST & DAST

Vendor shall integrate applications in scope for Veracode Static Application Security Testing (SAST) with Veracode before development begins. Specific procedures shall include the following:

- Create initial build pipelines for continuous integration and ensure Veracode scans are automated.
- Have builds triggered upon code commit or pull request, or at least nightly.
- Use this to shift left and find Secrets in source code as soon as new code changes are made.

Vendor shall have a recurring schedule (at least monthly) configured in the Veracode website for applications in scope for Veracode Dynamic Application Security Testing (DAST)
Ongoing usage of SAST and DAST for scoped applications helps find Secrets that were not caught during development.

2.3.8 Azure DevOps Personal Access Tokens

Vendor shall authenticate to Azure DevOps with identity services rather than cryptographic keys or tokens, where feasible. Azure DevOps also enforces Multifactor Authentication in this manner.
Whenever feasible, Vendor shall not manage keys or tokens alongside application code, since this is difficult and often leads to mistakes (for example, accidentally publishing Secrets to public code repositories or to a broader internal audience than necessary).
When Personal Access Tokens (PATs) are required, Vendor shall follow the recommendations below:

- Tokens shall never be created with full access and shall always be scoped to the minimum needed permissions/scopes.
- Tokens shall only be scoped to one Azure DevOps organization.
- Tokens shall not manage permissions on Azure resources.
- Tokens shall have an aggressive expiration date.
- Tokens shall be treated like passwords and kept secret.
- Tokens shall not be persisted in source code, scripts, or documentation.
- Tokens shall be persisted in approved password/Secret managers, in password-protected pipeline variables, or in approved vaults such as Azure Key Vault.
- Tokens shall not be shared between users. A token is tied to that user's identity and the access they have in Azure DevOps. For instance, an administrator with access to multiple or all projects in Azure DevOps shall not share a token with a developer who shall only have access to a fixed set of projects.
- Developers, Administrators, DevSecOps engineers, etc. shall revoke their own tokens when no longer needed.

Administrators shall audit tokens on a recurring basis and revoke tokens that do not meet the above criteria or that exhibit anomalous behavior or may have been compromised.