**Annual Grid Protection Alliance, Inc., (GPA) Product Maintenance**

With an annual product maintenance agreement, GPA agrees to:

* Provide support for all instances of the products specified in the associated quote including test, acceptance, and production.
* Provide notice of significant bug fixes and new product releases.
* Provide support for the application of patches or the migration to new versions of the product.
* Make GPA staff available for consultation and problem resolution.
* Provide access to a private, problem‐reporting web site (separate from GPA's public, open‐source problem reporting) to open maintenance tasks and allow tracking of these tasks to completion.
* Establish a process to escalate problem resolution, should it be necessary.
* Grant the maintenance contract owner a priority voice in establishing a ranking list for new features to be included in subsequent product releases.
* Provide the maintenance contract owner with two free registrations to the annual GPA User’s Forum, during the term of the maintenance agreement.

**Business Day Support (10 hours x 5 days)**

* GPA personnel will be available for e‐mail and telephone support during normal GPA business hours which are Monday through Friday, 8:00 a.m. until 6:00 p.m., eastern time, with the exclusion of six holidays ‐‐ New Year’s Day, Memorial Day, Fourth of July, Labor Day, Thanksgiving, and Christmas.
* During GPA business hours, GPA on‐call staff will respond immediately, whenever possible; but, in any event, GPA staff will reply within 30 minutes by telephone call or e‐mail to acknowledge receipt of a support request and initiation of work on the issue.
* A 24‐hours x 7‐days support telephone number will be provided for hours outside of those covered by the 10‐hours x 5‐days maintenance services. GPA will endeavor to provide this after‐business‐hours support (subject to the availability of GPA personnel) at 150 percent of GPA’s standard consulting rates with a 4‐hour minimum charge.

**Round‐the‐Clock Support (24 hours x 7 days)**

* Includes all GPA Business Day Support services.
* Additionally, GPA personnel will be available 24 hours x 7 days x 365 days via a direct mobile number and will respond within 15 minutes. Problem investigation will begin immediately.

©Grid Protection Alliance, Inc. 2022

COMPANY’S ACCEPTANCE OF THIS AGREEMENT IS EXPRESSLY SUBJECT TO COMPANY’S “APS ADDENDUM TO SUPPLIER’S HOSTING OR SOFTWARE AS A SERVICE AGREEMENT” WHICH IS ATTACHED TO THIS AGREEMENT.

**APS ADDENDUM TO SUPPLIER’S HOSTING OR SOFTWARE AS A SERVICE AGREEMENT**

**1. PARTIES.**

This Addendum (the “Addendum”) to the Grid Protection Alliance, Inc. Annual Product Maintenance is between Grid Protection Alliance, Inc. with offices at 1100 Market Street, Suite 906B, Chattanooga, TN 37402-2707 (“Supplier”) and Arizona Public Service Company(“Company”), having its principal place of business at 400 North 5th Street, Phoenix, AZ 85004, acting on its own behalf and for the benefit of Pinnacle West Capital Corporation (“PNW”).

**2. ACCEPTANCE AND PRECEDENCE.**

This Addendum is attached to and made part of Supplier’s Hosting or Software as a Service Agreement with Company, which, for purposes of this Addendum, includes any and all support and maintenance agreements related to such Software (collectively, the "Agreement"). Company's acceptance of the Agreement is expressly conditioned upon Supplier's acceptance of this Addendum. This Addendum will supplement the Agreement and have precedence and control over any conflicting or ambiguous terms and conditions in the Agreement.

**3. DEFINITIONS.**

The following definitions are applicable to this Addendum.

"Applicable Law" means all applicable laws, statutes, ordinances, rules and regulations of any governmental authority (including, without limitation, city, county, state, federal, and tribal governmental authorities), including, without limitation, all privacy, data protection, and cybersecurity laws, statutes, ordinances, rules and regulations.

“Availability” or “Available” means the accessibility to a resource in a timely manner, whether Supplier Personnel or other aspect of the Services.

“CIP Assets” means those critical electronic and information technology assets (“CIP Physical Assets”) and information (“CIP Information”) identified by Company pursuant to the NERC Critical Infrastructure Protection (“CIP”) standards.

"Claim" means any claim, action, dispute, demand, or right of action, whether in law or in equity, of every kind and character.

“Company Cyber Assets” means any Company networks, systems, computers, digital devices, or digital equipment, including CIP Physical Assets and industrial control systems.

“Company Property” means Company’s tools, equipment, data, facilities or Company Cyber Assets.

“Confidential Information” means all nonpublic information that Supplier receives about Company or any third-party contractor including, without limitation, customer and employee information, Intellectual Property, CIP Information, Covered Information, Restricted Information, and all other information concerning the business and affairs of Company. Any reproduction of Confidential Information is Confidential Information to the same extent as any original.

“Covered Information” means any CEII and BCSI, and any information created using CEII or BCSI (such as an analytical report). Covered Information is a type of Confidential Information.

“Crisis” means an extraordinary event affecting Supplier that requires emergency response measures to be taken, including any event that may result in the Services or Software becoming unavailable on the Facilities for a significant amount of time.

“Deliverables” has the meaning described in the scope of work or any Order. Deliverables also means all materials or information, whether in tangible or electronic form, and Goods that are delivered by Supplier to Company or installed as part of the Services, including: Software in source, object or executable code form, and all upgrades and updates thereof; Documentation; Developed Material, Supplier Material; hardware; files; databases; webpages; web sites; prototypes; samples; systems; and the contents of any of the foregoing.

"Developed Material" means all Software and Documentation that is developed by Supplier pursuant to the Agreement.

“Documentation” means documentation relevant to Company’s use, installation, and maintenance of the Deliverables and Services including, without limitation, specifications, reports, manuals, drawings, plans, designs, Software, instructions, and other information specified in the scope of work or any Order.

“End User” means any person or entity that Company authorizes to receive and use the Services.

“Error” means any error in the code of any Software which prevents such Software from operating in accordance with the relevant Documentation.

“Facilities” means the hardware, application software, operating system software, firmware, networks, communication devices and lines and all other equipment, software, devices and related materials provided by or used by Supplier to host the Software and provide the Services. Unless otherwise indicated, the Facilities will be construed to include the Software.

“Incident” means an unplanned interruption or reduction in quality of Services or Deliverables.

“Indemnitee” means the indemnified party and its officers, directors, employees, agents, advisors, representatives, affiliates, successors, and assigns.

"Intellectual Property" means any United States and foreign: (A) patents and patent applications, inventions and improvements thereto; (B) trademarks, service marks, trade names, trade dress, logos, business and product names, slogans, and registrations and applications for registration thereof; (C) copyrights and registrations thereof; (D) trade secrets and confidential or proprietary information including, without limitation, processes, methods, designs, formulae, know-how, and models; and tangible embodiments of any of (A) through (D) in any form or medium.

“Licensed Materials” means all engineering, testing and design documentation, schematics, source code, and other materials necessary for Company or its representatives to exercise the Intellectual Property license.

"Losses" means all liabilities, losses, damages, fines, penalties, costs, and expenses, of any kind or nature, whether or not covered by insurance, inclusive of reasonable attorneys’ fees and expenses incurred in the investigation, defense, or enforcement of a party’s rights under this Agreement.

“On Premises Equipment” means Facilities provided by Supplier to Company or End Users of the Services for receiving, managing, maintaining, or using the Services.

"Order" means a purchase order issued by Company to Supplier as part of the Agreement.

“Participant” means entities participating with Company as owners, co-owners, co-leaseholders, or tenant in common in Company’s facilities related to this Agreement or any Order, and each additional entity who may acquire an ownership or leasehold interest in those facilities or any other facility owned in whole or part or operated by Company.

“Personally Identifiable Information” or “PII” means any information that permits the identity of an individual to be directly or indirectly inferred or that is linked or linkable to an individual.

“Problem” means the underlying cause of one or more Incidents.

“Restricted Information” means information or data that is provided by Company to Supplier or is otherwise acquired by Supplier in the course of providing the Services and that is: (A) PII, financial information, medical or health-related information, or energy usage information pertaining to Company’s current, past, or potential customers, employees, or contractors (but not including the contact information of Company’s designated representative for Supplier contact purposes under this Agreement) (collectively also referred to as “Restricted Personal Information”); or (B) passwords, symmetric encryption keys, the private half of a public key encryption pair, operational or monitoring or diagnostic information pertaining to Company’s business operations, CEII, BCSI, CIP Information, Safeguards Information, confidential financial information, or capabilities to disable a security feature applied to protect Restricted Information, networks, or a computing environment (collectively also referred to as “Restricted Personal Information”). Restricted Information is a type of Confidential Information.

“Safeguards Information” means information not otherwise classified as national security information or restricted data that specifically identifies Palo Verde Generating Station‘s (PVGS): (A) detailed control accounting procedures for the physical protection of special nuclear material, (B) detailed security measures including security plans, procedures, and equipment for the physical protection of byproduct and special nuclear material, (C) security measures for the physical protection and location of certain plant equipment vital to the safety of production or utilization of facilities and (D) any information that could reasonably be expected to have a significant adverse effect by significantly increasing the likelihood of sabotage or diversion or theft of source, byproduct and special nuclear material.

"Security Incident" means any circumstance when: (A) Supplier knows or reasonably believes that PII, Confidential Information, or Restricted Information (as applicable) hosted or stored by Supplier has been disclosed; (B) Supplier knows or reasonably believes that an act or omission or the transmission of a computer virus has compromised or may reasonably compromise the cybersecurity of products or services provided to Company by Supplier or the cybersecurity of physical, technical, administrative, or organizational safeguards protecting Supplier's systems or Company Property used to monitor, store, or host PII, Confidential Information, or Restricted Information (as applicable); or (C) Supplier receives any complaint, notice, or communication which relates directly or indirectly to (i) Supplier’s handling of PII, Confidential Information, or Restricted Information (as applicable), ii) Supplier's compliance with the data safeguards in this Agreement or Applicable Law in connection with PII, Confidential Information, or Restricted Information (as applicable) or (iii) the cybersecurity of products or services provided to Company by Supplier or the cybersecurity of Supplier’s systems that could impact Company Property, including, but not limited to, Company Cyber Assets.

"Services" means all services that Supplier will perform under the Agreement.

“SaaS Services” or “Software as a Service” means those services and functionality provided by Software that are hosted on a computer network or systems owned or controlled by Supplier. SaaS Services are a subset of Services.

“Software” means each version of a computer program to be provided or developed by Supplier to perform the Services, including the object code and source code, scripts, routines, macros, and all upgrades, Documentation, work-arounds, error-corrections, patches, and bug fixes. Software also means the modifications and enhancements to the Software and new computer programs, including application program interfaces, developed from time to time by Supplier for the use of Company. Additionally, Software includes the operating platform on which the applications operate.

“Supplier Material” means all Software and Documentation to be provided by Supplier to Company pursuant to this Agreement and any Order and that was generated, developed, or prepared by Supplier or third parties prior to this Agreement or outside the scope of this Agreement or any Order. All Supplier Material will be listed in the Order(s). Software or Documentation not listed in such Order(s) as Supplier Material will be Developed Material.

"Supplier Personnel" means any person working for or on behalf of Supplier, including its officers, directors, employees, agents, and representatives, as well as Supplier’s subcontractors and their officers, directors, employees, agents, and representatives.

“Support Services” means (i) with respect to an Incident, the implementation/provision of a fix or a workaround that results in the Deliverables or Services conforming to and performing in accordance with the applicable specifications in the Agreement and (ii) with respect to a Problem, implementation/provision of a permanent fix that prevents any further Incidents as a result of the Problem. Support Services are a subset of Services.

**4.** **APPENDICES.**

This Addendum includes all documents attached hereto or incorporated by reference, including:

|  |  |
| --- | --- |
| Appendix A | Service Level Agreement |
| Appendix B | Exit Plan |
| Appendix C | Disaster Recovery Plan |
| Appendix D | Insurance |
| Appendix E | Company Access and Security Checks |
| Appendix F | Supplier Personnel Acknowledgement |
| Appendix G | Cybersecurity |
| Appendix H | Data Security and Privacy |

**5. SAAS ACTIVATION, INSTALLATION, PERFORMANCE AND LICENSE GRANT.**

5.1 Audit. Company may from time to time conduct audits and reviews of the Facilities on Supplier's premises with respect to the Services upon the earlier of (a) the date such audit or review is required by a state or federal regulatory agency, commission, or Company’s third party auditor, or (b) ten (10) business days' prior written notice.

5.2 Activation, Installation and Performance. Unless otherwise stated in the Services Agreement, construction, maintenance and operation of the Facilities, and activation, installation, and performance of the Deliverables and Services are and will be the responsibility of Supplier.

5.3 Grant of License On-Premises Equipment. Supplier hereby grants Company and its respective End Users a nonexclusive, paid-up, worldwide license to install, access and use the On-Premises Equipment to receive, manage, maintain, and use the Services.

**6. COMPANY ACCESS AND SECURITY CHECKS.**

Supplier Personnel who require unescorted physical access or remote cyber access to Company Property will comply with the terms and conditions set forth in Appendix E (Company Access and Security Checks). Prior to receiving access to Company Property, Supplier will require all Supplier Personnel to execute and submit to Company a “Supplier Personnel Acknowledgement” in the form of Appendix F (Supplier Personnel Acknowledgement).

**7. SUBCONTRACTORS.**

Supplier will not subcontract any part of the Deliverables or Services without Company's prior written approval. The Agreement will not create any contractual relationship between Company and any subcontractor of Supplier, nor obligate Company to pay or ensure that payment is made to any subcontractor of Supplier. Supplier will promptly pay all amounts owed to its subcontractors in connection with the Agreement. Supplier will be responsible for its subcontractor’s compliance with the Agreement.

**8. TESTING AND ACCEPTANCE.**

8.1. Testing. The Deliverables will be subject to the testing set forth in the Order. In addition, Company or its designated representative may inspect the Deliverables at any time and any place designated by Company. Company may elect to reject the Deliverables for failing an applicable test without waiving any other available remedy. Company will have no duty to discover any flaws or defects of any kind in the Deliverables or in any materials or supplies incorporated in or used in connection with the Services. Company's inspection or lack of inspection, payment, or acceptance will not relieve Supplier of its responsibilities under this Agreement.

8.2. Right to Reject. If Company determines that all or any part of the Services or Deliverables do not conform to the Order, instructions, drawings or descriptions or other requirements of the Agreement, Company reserves the right to reject such Services or Deliverables and cancel all or any unperformed part of the Agreement. Supplier will, at the Company’s option, (a) promptly perform corrective action including reperforming the Services or correcting the nonconforming or defective Deliverables, at Supplier’s sole expense, or (b) refund or credit the price of all Services and Deliverables rejected or cancelled by Company.

8.3 Initial Acceptance Test. Following successful completion of the implementation of the SaaS Service, Supplier will make the SaaS Service accessible to Company for acceptance testing and Company will conduct an acceptance test of such SaaS Service for a thirty (30) day period (the "Initial Acceptance Test"), to determine if the SaaS Service performs substantially in accordance with (i) the Documentation, and (ii) other selected test criteria as are identified in an Order to the Agreement (including any statement of work or specifications) ((i) and (ii) are collectively the "Acceptance Test Criteria"). Company will notify Supplier in writing within ten (10) calendar days after expiration of the Initial Acceptance Test period of either its acceptance or rejection of the applicable SaaS Service. If Company rejects the SaaS Service, Company may: (i) immediately terminate the Agreement and receive a refund of all amounts paid for the rejected SaaS Service without any further obligation or liability of any kind; or (ii) require Supplier to correct the deficiencies disclosed by the Acceptance Test Criteria and repeat such Acceptance Test until successfully completed, reserving the right to terminate as aforesaid. Notwithstanding anything to the contrary herein, no more than 50% of the initial installment of fees will be due upon completion of the Initial Acceptance Test.

**9.** **COMPLIANCE WITH LAW.**

9.1 Applicable Law; Export Control. Supplier will comply with Applicable Law. Each party is responsible for its compliance with all United States export control and economic sanctions laws, as set forth below.

(A) Prohibited Parties. Supplier represents and warrants that Supplier: (i) is not, directly or indirectly, acting for or on behalf of any person, group, entity or nation named pursuant to any law, order, rule or regulation enforced or administered by any department of the United States government as a “Restricted Party” or other sanctioned or blocked person, group, entity, territory or country; and (ii) is not directly or indirectly engaging, instigating or facilitating this transaction on behalf of any such person, group, entity, territory or country. A “Restricted Party” is any company or individual on the Department of Treasury Office of Foreign Assets Control list of Specially Designated Nationals and Blocked Persons or List of Foreign Sanctions Evaders, on the Denied Persons List, the Entity List, or the Unverified List maintained by the U.S. Department of Commerce’s Bureau of Industry and Security or on any other list maintained by any governmental agency restricting the export of any items to or other transactions with specific individuals, companies or other entities.

(B) Compliance with Trade Control Laws. Supplier and Company will comply with all applicable U.S. and non-U.S. export control and economic sanctions laws and regulations relating to its respective business, facilities, contractors and personnel, including but not limited to the U.S. Department of Energy’s Part 810 Regulations, the U.S. Department of State’s International Traffic in Arms Regulations (22 CFR Parts 120 et seq.), the U.S. Department of Commerce’s Export Administration Regulations (15 CFR Parts 730 et seq.), the Nuclear Regulatory Commission’s Part 110 Regulations (10 CFR Part 110), and the U.S. Department of Treasury’s economic sanctions programs (collectively referred to as “Trade Control Laws”).

(C) Export Control Limitations on Facility, Computer, and Network Access. Supplier will not assign any Non-U.S. Person (as defined below) employees, consultant, contractors, or subcontractors to work at or visit Company Property, or to access Company data, computers, or networks without first notifying and receiving written pre-authorization from Company and unless permitted or otherwise authorized by the U.S. government.

(D) Deliveries to Supplier. Supplier will not export, re-export or retransfer any hardware, software (including object code and source code), technology and services received from Company to Non-U.S. Persons (as hereafter defined), or to non-U.S. countries, without first obtaining any required authorizations or in a manner that is inconsistent with applicable Trade Control Laws. A “U.S. Person” means a citizen of the United States, a lawful permanent resident alien of the United States “a "Green Card" holder), an asylee, a refugee, or other protected individual under the Immigration and Naturalization Act. A “Non-U.S. Person” is anyone who is not a U.S. Person.

(E) Deliveries to Company. Prior to providing Company with any hardware, software (including object code and source code), technology and services that are (i) subject to the Export Administration Regulations (15 CFR Parts 730-774) and controlled at a level other than EAR99/Anti-Terrorism (AT), (ii) subject to the Department of State’s International Traffic in Arms Regulations (22 CFR Parts 120 et seq.), or (iii) other applicable Trade Control Laws, Supplier will provide written notice to Company specifying the nature of the controls and any relevant export classification information, including the Export Control Classification Number (“ECCN”) or applicable export classification.

9.2 Licensing. Supplier must have all permits, licenses, registrations, and other authorizations necessary to provide the Deliverables and perform the Services in accordance with Applicable Law (including applicable Trade Control Laws), and Supplier will provide copies of any such documentation to Company upon request.

**10. SUPPLIER REPRESENTATIONS AND WARRANTIES.**

10.1 In addition to the warranties provided in the Agreement, Supplier warrants and represents the following:

10.1.1. Supplier Representation. Supplier represents that Supplier and Supplier Personnel are fully qualified and competent to provide the Deliverables and perform the Services, as applicable.

10.1.2 Title Warranty. Supplier warrants title to the Deliverables is free and clear of defects and encumbrances.

10.1.3 Services Warranty. Supplier warrants that the Services will be: (A) performed and completed in a thorough and workmanlike manner; (B) performed in accordance with all requirements of the Agreement; and (C) of the standard and quality generally recognized and accepted within its industry or profession.

10.1.4 Availability. Supplier represents and warrants, that the Services, Software and Facilities will be fully available to Company and its End Users not less than the Availability Service Level as defined and set forth in the Service Level Agreements in Addendum- Appendix A (“Service Level Agreements”). Supplier will make every reasonable effort to ensure that routine scheduled system maintenance will be performed during times that are believed to have the least impact on Company's daily use of the Services, Software and Facilities.

10.1.5 Services Not to be Withheld. Supplier represents, warrants, and agrees that during the term of the Agreement it will not withhold Services under the Agreement (including, without limitation, implementation, termination transition assistance services) or access to the Facilities for any reason, including, but not limited to, a dispute between the parties arising under the Agreement, another agreement between the parties, or any unrelated dispute between the parties.

10.1.6 Deliverables Warranties. Supplier warrants that all Documentation and Deliverables will be: (A) new and of good quality; (B) free of defects in design except to the extent the Deliverables are manufactured in accordance with detailed designs provided by Company; (C) free from defects in material and workmanship; (D) provided in accordance with all requirements of the Agreement; (E) complete, accurate and may be relied upon by Company; and (F) safe and suitable for the ordinary purposes for which the Deliverables are to be used.

10.1.7 Open Source. Supplier warrants that, except as set forth in the Supplier’s Open Source Software List below, and for so long as the Services are to be provided by Supplier, (a) the Licensed Materials, including any custom Software, do not and will not include “open source software” or any derivative work thereof, and (b) Supplier will not include in any Deliverables or other work product created by Supplier for delivery to Company any “open source” software or any derivative work thereof; provided, however, that Supplier may use or distribute “open source” software if such software is not included in the Software and is not installed and used by Supplier at Company's Site (as in the case of software used only by Supplier in Supplier's own internal systems), or if such software as used by Supplier is not combined, incorporated, merged, or dynamically linked with any proprietary software owned or used by Company (as in the case of development tools or devices that include “open source software” but do not introduce any part of such software into any deliverables, work product, or other Company software). For purposes of the Agreement, “open source” software means any software that is licensed or provided, in whole or in part, pursuant to a license or terms of use that allows users to run, copy, distribute, study, change and improve the software without any obligation of the user to pay fees or royalties, and which contains one or more of the following restrictions: (i) the user may not sublicense, resell or distribute the same software or any derivate work thereof under different terms of use, (ii) the user may not charge license fees for the sublicense, resale or distribution thereof, (iii) the user must release source code to any third party to whom such software or any derivative work thereof is distributed, (iv) the user may not claim copyright or other Intellectual Property rights in any derivative work thereof, or (v) the user is prohibited from discriminating by restricting the persons or purposes for which the software is used. Excluded from the definition of “open source software” is software that is readily available in source code form but is not subject to any restriction on the further use or distribution thereof or any derivative work thereof, including “academic licenses” such as the MIT (aka XII) License, the Berkeley Software Distribution (BSD) license, and the Mozilla license.

|  |
| --- |
| Open Source Software List |
|  |
|  |
|  |
|  |

10.1.8 Compatibility with Future Releases. Supplier warrants that it will provide Company with prior written notice in the event that any upgrades to the Software (i) will not be compatible with existing Software in any material respect, (ii) will degrade the functionality of Software in any material respect, or (iii) will require the acquisition of additional equipment or software to operate.

10.2 Warranty Period. The title warranty has no expiration date. Manufacturers’ warranties expire in accordance with their terms. The other warranties set forth in this Agreement will expire upon the earlier of: (A) twenty-four (24) months after delivery of the Deliverables or completion of the Services; or (B) eighteen (18) months after Company begins the commercial operation of the Deliverables or repaired equipment following installation, start-up, testing, or maintenance. Company’s approval, inspection, or acceptance of, or payment for, the Deliverables or Services will not relieve Supplier of the warranties set forth in this Agreement. Company’s failure to comply with Supplier’s Documentation for the Deliverables or Services does not void Supplier’s warranties, except to the extent that Company’s non-compliance directly causes a defect or deficiency. The expiration dates for all warranties do not apply to Deliverables that contain latent defects.

10.3 Corrective Action. Company will notify Supplier in writing or by any other means reasonable to give Supplier actual notice of breach within a reasonable time frame after Company becomes aware of any breach of warranty. Supplier will, within ten (10) calendar days, provide to Company a written corrective action plan that specifies actions Supplier will take to cure the breach of warranty and minimize any adverse impact to Company. Upon Company’s written approval, Supplier will, at its sole expense: (A) promptly take all necessary corrective actions, including, but not limited to, adjustments, modifications, changes of design, removals, repairs, replacements or installations, and provide all necessary parts, materials, tools, equipment, transportation and labor; (B) cooperate with Company in any investigation relating to the breach of warranty; and (C) perform any tests Company may require to verify that Supplier’s corrective action complies with the Agreement. During Supplier’s performance of corrective action, Company may continue using any Deliverables, Services, and Company Property, in its sole discretion. Any corrective action taken by Supplier will be warrantied for twenty-four (24) months from completion and acceptance by Company of the corrective action.

10.4 Company Corrective Action. If Supplier fails to promptly commence corrective action, or if Supplier’s corrective action fails to remedy the breach of warranty, or Supplier’s schedule for cure of any breach of warranty has significant adverse effect on Company’s operations, Company may undertake corrective action, whether by acquiring replacement Deliverables or equipment, performing services itself, or obtaining similar services elsewhere. Corrective action undertaken by Company does not void Supplier's warranties and Supplier will be liable for Company’s direct costs for such corrective action. As a direct result of Supplier’s breach of any warranties in the Agreement, in addition to correcting such warranty breaches, Supplier will also be responsible for the costs and expenses incurred by Company in correcting any other work in progress affected or damaged, and reimbursing Company for any losses or damages to computers, network, information, data or computer programs, which the parties agree are direct damages.

**11. INDEMNIFICATION.**

11.1 Supplier Indemnification. To the fullest extent permitted by law, Supplier will indemnify, defend, and hold harmless Company Indemnitee for, from and against any and all Losses that any Company Indemnitee may incur in connection with any Claim arising out of, or resulting from any of the following:

(a) any harm, injury, or death to any person, or any damage or destruction of any tangible third party property, if caused in whole or in part by (i) the negligence of Supplier or Supplier Personnel, or (ii) a defect in the Deliverables or Services;

(b) any actual or alleged violation of Applicable Law by Supplier, including acts or omissions by Supplier or Supplier Personnel that cause Company to violate Applicable Law;

(c) any actual or alleged infringement or misappropriation of any third party intellectual property rights except to the extent that the Claim is based on Supplier’s manufacture of the Deliverables or performance of the Services in accordance with Company’s detailed designs or specifications; and

(d) a Security Incident.

11.2 Direct Damages. For clarity, to the extent Company is entitled to indemnification from Supplier in connection with a third party claim, any damage awarded to the third party (direct, consequential, or otherwise), will be deemed to be direct damages of the indemnified party, for which the indemnifying party will be liable.

11.3 Indemnification Procedures. Company will give written notice to Supplier after becoming aware of an actual or potential Claim for which Company is entitled to indemnification pursuant to the Agreement. Company’s failure to give such notice does not relieve Supplier of its indemnification obligations, except to the extent that Supplier is materially prejudiced as a result of such failure. Supplier will not settle any Claim or admit liability on behalf of Company without the prior written consent of Company.

11.4 Waiver of Immunity. Supplier’s indemnification obligations are not limited by any right or obligation that Supplier or Supplier Personnel may have under workers’ compensation laws, disability benefit laws, or other employee benefit laws. Supplier hereby waives any immunity or other limitation of liability it may have under such laws.

11.5 Intellectual Property Remedies. In addition to Supplier’s indemnification obligations, if any third party claims that the Deliverables or Services infringe or misappropriate that third party’s Intellectual Property, Supplier, at Supplier’s sole cost and expense, must: (A) secure a license for Company to continue using the Deliverables or Services; (B) replace or modify the Deliverables or Services with a non-infringing equivalent acceptable to Company; or (C) if approved by Company in writing, remove such Deliverables or Services and adjust Company’s payment obligations accordingly (including a full refund if appropriate).

**12. LIMITATION OF LIABILITY.**

Notwithstanding the foregoing or any other terms or conditions to the contrary, no limitation of Supplier's liability and no exclusion of damages will apply with respect to any claims, damages, losses, fines, penalties, costs and expenses, including reasonable attorney’s fees and costs, arising out of or relating to any of the following:

(a) Supplier’s confidentiality or non-disclosure obligations under this Agreement;

(b) Supplier’s obligations to indemnify Company for third party claim claims under this Agreement;

(c) a Security Incident that arises out of or results from Supplier’s non-compliance with Supplier’s

obligations under Section 13 (Cybersecurity; Data Security and Privacy) of this Addendum; and

(d) the failure by Supplier or Supplier Personnel to timely pay any required taxes, assessments, or contributions.

**13. CYBERSECURITY; DATA SECURITY AND PRIVACY.**

Supplier will comply with the terms and conditions set forth in Appendix G (Cybersecurity) and Appendix H (Data Security and Privacy).

**14. SERVICE LEVELS; SUPPORT SERVICES.**

14.1 SaaS Service Levels. Supplier will provide the SaaS Services and Support Services in accordance with the Service Level Agreements.

14.2 Service Level Defaults. It will be deemed a material breach of the Agreement if Supplier will fail: (a) with respect to Severity 1, 2 or 3 Errors, to comply with the time periods set forth in the Service Level Agreements two (2) times during any ninety (90) day period; or (b) to correct, or provide a work around (as described in the Service Level Agreements) for a Severity 1 or 2 Error within seventy-two (72) hours after Company's original notice thereof (each, a “SaaS Service Level Default”).

Upon the occurrence of a SaaS Service Level Default, in addition to (and not in lieu of) any other rights and remedies available to Company under the Agreement or at law or in equity.

(a) Company will receive a monetary credit of *[designation of credit percentage]* % of the fees (the “SaaS Service Level Credits”) for each SaaS Service Level Default. The application of SaaS Service Level Credits will not relieve Supplier of its obligation to continue its efforts in correcting such SaaS Service Level Defaults. Once a SaaS Service Level Default has occurred, for each additional *[designation of time period by number of days or hours]* period thereafter during which the relevant Error is not corrected, Company will receive an additional SaaS Service Level Credit. The provision of SaaS Service Level Credits is without prejudice to other rights and remedies that Company may have under the Agreement or at law or in equity. Supplier will calculate any amount that Company is entitled to as SaaS Service Level Credits upon notice by Company of SaaS Service Level Defaults. Supplier will credit all SaaS Service Level Credits towards the next invoice; and

(b) Notwithstanding the cure time period set forth in the Agreement, Company may, in its sole discretion, immediately terminate the relevant Agreement or Order and receive a refund of all fees paid by Company to Supplier thereunder (prorated from the date of the occurrence of the Service Level Default).

14.3 Additional Remedies for Service Level Failures. Supplier's failure to meet the Service Level Agreements for resolution of any [Severity Level 1 Errors or Severity Level 2 Errors /[OTHER SEVERITY LEVEL ERRORS]], or any combination of such Errors, within the applicable resolution time set out in the Service Level Table [in any [RELEVANT PERIOD]/FREQUENCY in any [RELEVANT PERIOD]] will constitute a material breach of the Agreement. Without limiting the Company's right to receive SaaS Service Credits, the Company may, at its option:

(a) use any previous version or release of the Software in which such Severity Level 1 or Severity Level 2 Error does not occur or can be worked around if the then-current Software exhibits an un-resolved Severity Level 1 Error or un-resolved Severity Level 2 Error, and Supplier will perform all Support Services for such previous version or release until the Supplier resolves such Severity Level 1 Error or Severity Level 2 Error for the then-current Software; and

(b) obtain such other remedies as may be available to it under the Agreement or otherwise at law or in equity, including the right to terminate the applicable Agreement or Order for material breach in accordance with the termination section of the Agreement.

**15. INSURANCE.**

Supplier and its subcontractors at every tier will maintain in full force and effect the minimum insurance limits and terms set forth in Appendix D (Insurance). Such policies will extend to damages and expenses under the Agreement, as well as any monetary judgment or award, including consequential damages that are insurable by law.

**16. DISASTER RECOVERY**.

Supplier shall have a disaster recovery procedure as it relates to Company Data, attached as Appendix C hereto (such outline and summary plus all of Supplier's supporting detailed documentation and plans as contemplated by the provisions of this Section 16, the “Disaster Recovery Plan”). The Disaster Recovery Plan for all Services shall: (a) be designed to continue all Supplier business operations that are critical to the overall operation and functionality of the Services and Software notwithstanding the occurrence of a Crisis; (b) specify procedures and frequency of testing; and (c) shall be, and shall be maintained consistent with, then-current generally accepted industry standards. The Disaster Recovery Plan shall provide, among other things, a mechanism for the redundancy or back-up of business operations designed to keep the Services from becoming unavailable for a significant amount of time due to a Crisis and to permit the related business operations of Company to be re-instituted in a time period that permits the ongoing operation and functionality of Company's business to which the Services relate.

**17. THIRD PARTY BENEFICIARIES.**

17.1 Except as specifically provided for herein, the Agreement does not create any rights exercisable by any third party. If the Deliverables or Services provided by Supplier pertain to any facility that is co-owned or co-leased by Company and any Participant(s), the following provisions apply:

(a) When entering into the Agreement on behalf of a Participant, Company is acting as the Participant’s agent. All benefits, rights, and remedies of Company under the Agreement, including those pertaining to indemnity, insurance, and ownership, will also inure to the benefit of the Participant.

(b) If Company is acting as agent of Participant in entering into the Agreement, then Company and Participants will retain legal title to the Deliverables or Services provided under the Agreement.

**18. TERMINATION.**

18.1 Cure Period or Renewal. In addition to the termination rights specified in the Agreement, the Agreement will not be subject to termination by Supplier due to a breach by Company unless Company has received written notice specifying the breach and a reasonable period of time to correct the breach, if correctable, or to provide Supplier other acceptable remedies. Company may, without penalty or charge, terminate this Agreement in whole or in part, at or before the effective date of any price increase of the Deliverables or Services or any renewal of the Agreement.

18.2 Termination for Convenience. Company may terminate the Agreement or any Order hereunder at any time upon written notice to Supplier. Notwithstanding anything to the contrary in the Agreement or any Order, in the event of any termination under this section, Company will only be liable to make any payments which are due hereunder to Supplier for work performed in accordance with the terms and conditions herein up to the date of such termination.

**19. EXIT PLAN AND TRANSITION.**

19.1 Exit Plan. In the event of any termination of the Agreement, the parties will prepare and carry out an Exit Plan on the terms set forth in Appendix B-Exit Plan.

19.2 Transition. In the event of any termination of the Agreement, the parties will cooperate to prepare and timely carry out a transition plan. Company will be entitled to continued provision of the Services and Software by Supplier for a period of time determined by Company, not to exceed two (2) months, required for Company to wind down its current use of the Services and/or Software or to make a transition to alternate services providers or facilities.

**20. GENERAL.**

20.1 Remedies. All rights and remedies of the parties are cumulative, and not exclusive. Each party acknowledges that a breach of certain of its obligations under the Agreements and each party's confidentiality obligations set forth in the Agreements) other than any payment obligations hereunder, may result in irreparable and continuing damage to the other party for which monetary damages may not be sufficient, and agrees that the other party will be entitled to seek, in addition to its other rights and remedies hereunder or at law, injunctive or all other equitable relief, and such further relief as may be proper from a court of competent jurisdiction.

20.2 Use of Company’s Name. Neither Supplier nor Supplier Personnel will use Company’s name, trademarks, facility names, or photographs of Company property in any marketing materials, customer lists, or other public documents or publicly accessible locations, without Company’s prior written consent, which may be withheld by Company in its sole discretion.

20.3 License of Intellectual Property; 365(n). The Software is “intellectual property” as defined in 11 U.S.C. §101(35A) which has been licensed hereunder in a contemporaneous exchange for value and the Agreement will be governed by 11 U.S.C. §365(n), as the same may be amended or supplemented from time to time, if Supplier files for bankruptcy.

20.4 UCITA Not Applicable. The Agreement and the transactions contemplated herein is not and will never be subject to the Uniform Computer Information Transactions Act (prepared by the National Conference of Commissioners on Uniform State Laws) as currently enacted by any jurisdiction or as may be codified or amended from time to time by any jurisdiction. Company's rights under the Agreement may be exercised by and for the benefit of Company, and, as applicable, its End Users, and their respective affiliates.

20.5 Assignment. Supplier will not assign its rights or delegate its duties under this Agreement without the prior written consent of Company, which Company may withhold in its sole discretion. Any assignment or delegation by Supplier in breach of this provision is void.

20.6 Survival. Termination or expiration of this Agreement will not relieve either party of any obligation that expressly or by implication survives termination or expiration, including but not limited to: Insurance, Indemnification, Limitation of Liability, and Supplier’s Warranties.

**APS ADDENDUM TO SUPPLIER’S HOSTING OR SOFTWARE AS A SERVICE AGREEMENT**

**APPENDIX A- SERVICE LEVEL AGREEMENT**

This Service Level Agreement (“SLA”) is an attachment to the Addendum executed between Supplier and Company and is hereby incorporated therein by this reference. All capitalized terms used but not otherwise defined herein will have the meanings given them in the Agreement or the Addendum.

1. **DEFINITIONS.**

"Company Authorized Support Personnel" means those Company personnel that Company has designated or authorized to support the SaaS Services.

“Excused Downtime Minutes” means minutes that the SaaS Service are not available due to circumstances reasonably outside of Supplier’s control, including but not limited to downtime resulting from (a) any Company provided content or programming errors; (b) system administration, commands or file transfers performed by Company or its users; (c) work or activities performed at Company’s request; (d) untimely Company response time to incidents that require Company participation for source identification and/or issue resolution; (e) outages that occur between the Scheduled Downtime and any alternative Company chosen maintenance downtime, if the outage reasonably could have been prevented by following the Scheduled Downtime; (f) failure of non-Supplier managed Company or user hardware or software; or (g) periods of Scheduled Downtime.

“Maintenance Services” means all activities Supplier deems reasonably necessary, to continue providing the Supplier’s Software to Company as a Service in accordance with the Agreement, including but not limited to code changes, system configuration changes, etc. Maintenance Services are a subset of Services.

“Outage” means the number of minutes that the Software is unavailable to Company during a given period.

“Required Monthly Availability” means the total number of minutes in the applicable month, minus the Excused Downtime Minutes for that month.

“Scheduled Downtime” means the total number of minutes in the calendar quarter during which the. Service is not Available due to scheduled or announced Service, Software, or system maintenance.

“System Availability Percentage” means the percentage derived from the following calculation: Required Monthly Availability minus the aggregate of all Outage minutes in the applicable month divided by the Required Monthly Availability.

1. **SUPPORT RESPONSE SLA’S.**

For all issues reported to the Supplier customer support department (“Supplier Support”), Supplier will provide support services on a 24 x 7 x 365 basis, in accordance with the response required for the applicable Severity level assigned by Company. Issues are classified under five severity levels as shown in Table 1. Once a case is created, Supplier will respond as explained in Table 2 within a timeframe shown in Table 3. Supplier’s ability to replicate and resolve issues will depend on accurate and detailed information supplied by Company. Supplier will meet the following response times.

**Table 1: Supplier Issue Severity Definitions**

|  |  |  |
| --- | --- | --- |
| **Business Impact** | **Description** | **Definition** |
| Fatal‑S1 (Severity 1) | Production system down | Critical business operations (as determined by Company) halted and users are unable to complete daily operations. Only valid for production systems |
| Critical‑S2 (Severity 2) | Severe functionality loss | Key business functions cannot be performed as determined by Company and Supplier |
| Important‑S3 (Severity 3) | Limited functionality | Issue limits minor business operations |
| Minor‑S4 (Severity 4) | FAQ or documentation Problem | Issue has minimal impact on business |
| Enhancement‑S5 (Severity 5) | Feature enhancement | Company feedback regarding improvement to existing functionality |

**Table 2: Supplier Issue Response Types**

|  |  |
| --- | --- |
| **Response** | **Definition** |
| Acknowledge | Acknowledgement of issue and assignment of issue tracking number (Response) |
| Follow‑Up | Time interval between status updates (Based upon new information only and excludes the initial Company call) |
| Escalation | Length of time to notify proper contacts for resolution (Starts at time of Supplier Acknowledgement) |

**Table 3: Supplier Issue Response Times**

|  |  |  |  |
| --- | --- | --- | --- |
| **Business Impact** | **Acknowledge\*** | **Follow‑Up\*** | **Escalation\*** |
| Fatal‑Sl (Severity 1) | 15 minutes | 1 Hour | 1 Hour – Engineer & Support Management is Notified |
| Critical‑S2 (Severity 2) | 1 Hour | 4 hours | 2 Hours – Engineer & Support Management is Notified |
| Important‑S3 (Severity 3) | 24 Hours | Company Request | Scheduled Patch Release or acceptable workaround |
| Minor‑S4 (Severity 4) | 48 Hours | Company Request | Determined by Supplier |
| Enhancement‑S5 (Severity 5) | 1 Week | Company Request | Determined by Supplier |

**Table 4: Supplier Issue Correction Times**

|  |  |
| --- | --- |
| **SEVERITY LEVEL** | **CORRECTION TIME** |
| Severity 1 | Four (4) hours |
| Severity 2 | Eight (8) hours |
| Severity 3 | Seventy-two (72) hours |
| Severity 4 | Two (2) weeks |
| Severity 5 | Thirty (30) days |

\* Note: Initial call is not considered Follow‑Up. Follow-Up is based on new information to be supplied to the requestor.

For the purposes of this Appendix A, a “work-around” means a temporary work-around, patch or bypass supplied by Supplier in order to temporarily correct the issue; provided, however, that: (a) the Software’s functionality, compatibility or use is not adversely affected; and (b) the work-around is not unduly burdensome to Company. Notwithstanding the availability of a work-around, Supplier will continue to work to fix the issue and, in any event, provide Company with the applicable permanent correction within: (i) ten (10) days for a Severity 1 or 2 issue; or (ii) three (3) weeks for a Severity 3, 4, or 5 issue.

**3. SUPPORT REQUESTS.**

Supplier Support is available to Company Authorized Support Personnel. Company will keep Supplier advised from time to time of its Company Authorized Support Personnel.

**4. SUPPORT METHODOLOGY.**

A ticket will be opened in the Supplier Issue Tracking System. In all communications between the parties, both Supplier and Company Authorized Support Personnel will identify issues by the Supplier ticket number. Supplier will communicate status updates (“Follow-Ups”) to the original requestor via email or telephone or both, as appropriate. Company may also access Supplier’s customer relationship management system (also known as “CRM”) to track Problem tickets online.

**5. MAINTENANCE.**

5.1 Scheduled Maintenance. Supplier will be responsible for notifying Company Authorized Support Personnel of Supplier’s regularly Scheduled Downtime and exceptions. For exceptions to Scheduled Downtime, Supplier will notify Company at least ten (10) days in advance. This provision applies to the production environment only. At Supplier’s discretion, Supplier may perform maintenance (scheduled or unscheduled) at any time on the staging, testing, and configuration environment.

5.2 Unscheduled Emergency Maintenance. Supplier Support will notify Company of any emergency maintenance downtime on the production environment as soon as possible

5.3 Maintenance Services. Supplier reserves the right to perform Maintenance Services on the Software.

**6. ESCALATION POLICY.**

In the event Company, in its sole discretion, determines an issue or Problem merits additional attention by Supplier Support, or if any response, Follow Up or correction time is not met as set forth herein, Company Authorized Support Personnel may escalate the issue by requesting to speak directly with a Supplier Support Manager.

**7. SAAS AVAILABILITY SLA.**

System Availability Percentage. While Supplier strives for 100% uptime, Supplier will ensure the SaaS Services are available at least 99.99% of the Required Monthly Availability for the Service (“SaaS Availability SLA”). At Company’s request, the parties will engage in an annual review of industry standards and practices to determine if an improved percentage is appropriate.

**8. METRICS AND REPORTS.**

8.1 At minimum, Supplier will provide the following metrics and reports to Company monthly:

(a) Required Monthly Availability Percentage Report

(b) Significant Events Reports will include, but not be limited to:

* Outage Minutes
* Problem description(s)
* Problem resolution(s)

(c) Monthly Performance Report including, but not limited to:

* + - Average and peak time for messages to be received and transmitted during a one-hour period
    - Message count during a one-hour period
    - Cycle time reports on problems and how quick they are acknowledged and closed per table 2 above
    - Failed message counts per 24-hour period

**9. SERVICE LEVEL REVIEWS.**

9.1 Supplier will initiate and schedule quarterly service level reviews with Company covering the following matters:

(a) SaaS Services performance to the SaaS Availability SLA

(b) Major issues and their resolution

(c) Upcoming revisions, changes to Supplier Support Services, and strategic planning

(END APPENDIX A SERVICE LEVEL AGREEMENTTO APS ADDENDUM TO SUPPLIER’S HOSTING OR SOFTWARE AS A SERVICE AGREEMENT)

**APS ADDENDUM TO SUPPLIER’S HOSTING OR SOFTWARE AS A SERVICE AGREEMENT**

**APPENDIX B - EXIT PLAN**

1. Definitions.

For purposes of this Exit Plan, the following terms will have the meanings set out below:

“Replacement Services” means any services which are substantially similar to the Services and which Company or one of its affiliates procures in substitution for the Services following the termination of the Agreement, whether those services are provided internally and/or by any third party.

Replacement Supplier” means any third-party service provider of Replacement Services appointed by Company or one of its affiliates from time to time.

“Termination Assistance Fees” means the charges payable by the Company for the Termination Services as will be set out in the Exit Plan.

“Termination Period” means the period of twelve (12) months (which may be reduced at the Company's discretion by giving Supplier sixty (60) days' written notice) commencing on the date of service of any notice of termination of the Agreement.

“Termination Services” means the termination transition services to be provided under the Exit Plan. In addition, Services under the Agreement will be provided in accordance with the terms of the Agreement during the Termination Period.

2. For the Termination Period, Supplier will provide all reasonable and necessary transition assistance to Company and its affiliates to allow, as chosen by Company, the orderly transfer and replacement of the Services by Company or a Replacement Supplier, or their respective representatives. Such transition may entail the substitution of websites, communication networks, software, servers, and reports, and/or the termination or modification of the Services in whole or in part. Supplier and Company will cooperate with each other in the production of the Exit Plan in accordance with this attachment to complete the Exit Plan in a timely manner.

3. As soon as reasonably practicable after any notice of termination is served in accordance with the Agreement, the parties will:

1. Agree upon a date (which will be no later than thirty (30) calendar days after the date of such meeting) for the joint production and circulation of a first draft of the Exit Plan; and
2. Appoint a senior management individual of each of the parties, each of whom will act as a point of contact for the Termination Period and to deal with all matters relating to termination of both the Services and/or any license relating to the Licensed Materials granted under the Agreement.

4. The Exit Plan will:

1. Address the scope of the Termination Services, Termination Assistance Fees and the service levels applying to the Termination Services. Unless otherwise agreed by the parties, each party will continue to meet its respective obligations under the Agreement during the Termination Period. Supplier acknowledges that it is important to Company to effect an orderly transition in-house or to a Replacement Supplier of the Replacement Services and, in this respect, it is also important that there is no degradation in the provision of the Services; and
2. Describe the process by which the parties will return or cease to use each other's Confidential Information; and
3. Address the project management of the Termination Services and identify relevant individuals who will manage the provision and implementation of the Termination Services.

5. Upon request by Company during the Termination Period, Supplier will provide to Company any reasonable documentation describing, explaining or which would otherwise assist Company in inviting third party service providers to supply the same or similar software and/or services (or any part of the same) and negotiating alternate arrangements with those third parties with regard to the provision of Replacement Services.

6. Supplier will provide or make available to Company detailed information, data, and records reasonably necessary for the provision of services similar to the Services and/or any software which may be used by Company or a Replacement Supplier in lieu of the Software post termination of the Agreement.

7. The parties will agree upon any other reasonably necessary provisions to facilitate a smooth and orderly transition from Supplier to Company or the Company's nominated Replacement Supplier.

(END APPENDIX B EXIT PLAN TO APS ADDENDUM TO SUPPLIER’S HOSTING OR SOFTWARE AS A SERVICE AGREEMENT)

**APS ADDENDUM TO SUPPLIER’S HOSTING OR SOFTWARE AS A SERVICE AGREEMENT**

**APPENDIX C- SUPPLIER’S DISASTER RECOVERY PLAN**

TO ATTACH SUPPLIER’S DISASTER RECOVERY PLAN]

(END APPENDIX C DISASTER RECOVERY PLAN TO APS ADDENDUM TO SUPPLIER’S HOSTING OR SOFTWARE AS A SERVICE AGREEMENT)

**APPENDIX D INSURANCE**

1. **INSURANCE TERM AND COVERAGE.**
   1. Until all obligations under the Agreement are satisfied (unless otherwise stated herein), Supplier and Supplier subcontractors at every tier will, at their sole expense, provide and maintain, at a minimum, the following insurance coverages and limits, using forms and insurers acceptable to Company.
2. **MANDATORY INSURANCE.**
   1. Supplier will provide:
      1. Commercial General Liability (CGL). CGL insurance with limits of $1,000,000 per occurrence and $2,000,000 for general and products-completed operations (aggregate). Coverage on an “occurrence” basis using Insurance Services Office (ISO) Form CG 00 01 or equivalent, including coverage for premises operations, independent contractors, products-completed operations, personal and advertising injury and liability assumed under the Agreement. Products-completed operations coverage to be maintained for at least three (3) years past acceptance, cancellation or termination of the Agreement.
      2. Workers’ Compensation and Employer’s Liability. Workers’ Compensation insurance with statutory limits and Employer’s Liability insurance with limits of not less than $1,000,000 per accident and per employee for bodily injury or disease.
      3. Commercial Automobile Liability. Commercial Automobile Liability insurance with limits of not less than $1,000,000 per accident covering all of Supplier’s owned, hired, or non- owned vehicles used in connection with the Agreement.
      4. Umbrella/Excess Liability. Umbrella or Excess Liability insurance with limits of not less than $10,000,000 per occurrence and in aggregate greater than the underlying CGL, Employer’s Liability, and Commercial Automobile Liability limits above. All umbrella or excess liability policies must follow the form of the underlying policies and expressly provide that the Umbrella or Excess Liability policy drops down over a reduced or exhausted aggregate limit of the underlying insurance.
3. **PROVISIONAL INSURANCE.**
   1. If, at any time during the term of the Agreement, Supplier’s scope includes any of the following activities, Supplier will provide the corresponding insurance coverage. Coverage may be provided by endorsement to an existing insurance policy as long as terms, conditions, provisions and definitions of such endorsement meet the terms, conditions and limits outlined below:
      1. Professional Liability/Errors and Omissions. If Supplier’s obligations under the Agreement include performing professional services including, but not limited to, engineering work, design, architectural work, legal, financial, accounting, consulting, or medical services, then Supplier will provide Professional Liability/Errors and Omissions insurance with limits of not less than $5,000,000 per claim and $10,000,000 in the aggregate. Such insurance must cover liabilities for financial loss resulting or arising from negligent acts, errors, or omissions in rendering Services or in connection with the Agreement. Continuous coverage must be maintained during the term of the Agreement and for three (3) years (either as a policy in force or extended reporting period) after completion, cancellation or termination of the Agreement.

* + 1. Data Protection/Cyber Liability Insurance. Supplier will provide Data Protection/ Cyber Liability Insurance if: (A) any Deliverables or Services procured by Company contain any Software; (B) Supplier will store, process, or host Confidential Information in performance of the Services; (C) Supplier will remotely access Company Property; (D) Supplier will connect any electronic device, asset, or equipment to any Company Property; (E) Supplier will electronically handle, remotely access, exchange, transmit, monitor, or store any Restricted Information or Supplier’s system or network will be used to store, process, or host Restricted Information including data hosting services or computing services as part of the Services Supplier may provide under this Agreement; or (F) Supplier’s Services under the Agreement are subject to the Payment Card Industry Data Security Standard (“PCI DSS”), Supplier will provide such Data Protection/Cyber Liability insurance with limits not less than $10,000,000 per claim and in the aggregate covering liabilities resulting or arising from acts, errors, or omissions in rendering Goods or Services or in connection with the Agreement. Coverage must include, but not be limited to: damages, including fines and penalties, Supplier is obligated to pay Company or any third party associated with a Security Incident or associated with loss of Confidential Information; costs resulting from a PCI DSS assessment; costs to notify individuals whose PII or Restricted Information was lost or compromised; costs to provide credit monitoring and credit restoration services to individuals whose PII or Restricted Information was lost or compromised regardless of cause (including, without limitation, Supplier negligence or gross negligence and unlawful third party acts) and costs resulting from cyber extortion demands.

Such policy must provide coverage for wrongful acts, claims, and lawsuits anywhere in the world and must be kept in force during the term of the Agreement and for three (3) years after completion, cancellation, or termination of the Agreement.

Supplier, at its discretion, may cover the above Data Protection/Cyber Liability Insurance requirements under a Professional Liability policy so long as the terms, conditions, provisions, and definitions of such policy do not restrict, negate, or limit the insurance required as set forth in this section.

1. **INSURANCE POLICY PROVISIONS AND CONDITIONS.**
   1. Additional Insured. Except for Workers’ Compensation, Professional Liability/Errors and Omissions, and Data Protection insurance, all the policies required by this Agreement must be endorsed to include Company and Company Indemnitees as additional insureds. For any claims related to the Agreement, Supplier’s insurance or self-insurance coverage will be the primary insurance and any insurance or self-insurance carried by Company or any Company Indemnitee will be excess and will not contribute. Company will be entitled to coverage consistent with the broadest utilized ISO coverage endorsements at the time the Agreement is executed, without exception. Additional insured coverage under any CGL policy or Contractors Pollution Liability policy must include ongoing and completed operations coverage.
   2. Waiver of Subrogation. Supplier and subcontractors of every tier will waive, and require its insurers to waive, any and all recovery rights they may have against Company or any Company Indemnitee.
   3. Separation of Insureds. All policies, except for Workers’ Compensation, Professional Liability/Errors and Omissions, and Data Protection insurance, will apply separately to each insured against whom claim is made or suit is brought, subject to the policy limit of liability, and will not contain any cross suits exclusion.
   4. Insurer Ratings. All policies must be provided by licensed and admitted insurers, or eligible surplus lines carriers, with a rating of no less than A-:VII from A.M. Best.
   5. Self-Insurance and Retentions. Self-insurance and retentions: (1) are the sole responsibility of Supplier; and (2) must provide Company and Company Indemnities all benefits that would otherwise be available and provided under an insurance policy, including, but not limited to, the defense of claims. Upon Company’s request, Supplier will present evidence acceptable to Company of its ability to be self-insured and the financial ability to respond to stated self-insured retentions related to the Agreement.
   6. Evidence of Insurance. Company reserves the right to request a certificate or endorsement for any insurance policy required in the Agreement. In the event of a claim, if requested, a copy of the responsive policy must be provided to Company within five (5) calendar days.
   7. Acceptance of Evidence. In no event does Company’s failure to receive or identify deficiencies in insurance documentation serve as waiver of Supplier’s obligation to obtain and maintain the required insurance coverages and limits. Acceptance of documents by Company does not constitute approval or agreement that the insurance requirements have been met, or that the insurance policies identified in the certificates are in compliance with the insurance requirements of the Agreement.
   8. Maintenance of Insurance. Supplier’s failure to provide satisfactory evidence of insurance will be deemed a material breach of the Agreement. Supplier’s lack of insurance does not negate Supplier’s obligations under the Agreement. Furthermore, Company may deny access to any Site for so long as Supplier does not sufficiently prove the existence of the required insurance coverages.
   9. Claims. Supplier will promptly make a full written report to Company of all accidents or claims for damage arising from or in connection with: (i) the Agreement or any Order; (ii) the discharge of Supplier's duties under the Agreement or any Order; or (iii) the presence of Supplier or Supplier Personnel on Company Property. Supplier will cooperate fully with Company and with any insurance carrier in the investigation and defense of all such accidents and claims and such obligation will survive the termination or expiration of the Agreement.
   10. Notice of Cancellation. Supplier will provide Company with written notice of any cancellation of any required insurance policies within ten (10) calendar days of receipt of notice from Supplier’s insurance carrier or broker.
   11. Provision of Policies. Neither the content of any insurance policy, nor certificate, nor Company's approval thereof, will relieve Supplier of any of its obligations in the Agreement.
   12. No Representation. Company does not represent that the coverage types or amounts of insurance required in this Agreement are adequate to protect Supplier against all potential losses that Supplier may incur, nor will the types or amounts of insurance be construed to limit, release, or waive any obligations or liabilities of Supplier to Company or other parties.
   13. Special Circumstances. With Supplier’s written consent, which shall not be unreasonably withheld, Company reserves the right to modify these requirements, including limits based on the nature of the risk, prior experience, insurer, coverage, or other special circumstances.

(END OF APPENDIX D)

**APPENDIX E – COMPANY ACCESS AND SECURITY CHECKS**

1. **ACCESS.**
   1. Supplier Personnel Access. Supplier will review and verify Supplier Personnel’s need for unescorted physical access or electronic access, including Interactive Remote Access (“IRA”), to Company Confidential Information and Company Property at least once every six (6) months during the term of the Agreement. Supplier will retain evidence of such reviews for two (2) years from the date of each review.
   2. Access to Company Cyber Assets. Supplier and Supplier Personnel will not access or connect to Company Cyber Assets without Company’s prior written authorization, which Company may revoke at any time and for any reason in the exercise of its sole discretion. The scope of such authorization may be limited by Company, and Supplier and Supplier Personnel must comply at all times with that authorization, in addition to the requirements set forth in the Agreement.
   3. Access Control Policy. Supplier will maintain policies and procedures to address the security of remote and onsite access to Company Information and Company Property, including systems and networks (an “Access Control Policy”), that is consistent with the personnel management requirements of the current revision of NIST Special Publication 800-53, AC-2, PE-2, PS-4, and PS-5, as applicable, and the requirements of this Appendix E.
   4. Required Notification and Revocation. Supplier will immediately notify Company Leader, as identified in Company’s vendor management system, in writing, and orally, no later than four (4) hours after any of the events identified in subsections (A) through (G) below so that Company can revoke unescorted physical access and electronic access, including IRA, for such Supplier Personnel.
2. Any Supplier Personnel no longer requires access to Company Confidential Information or Company Property to furnish the Deliverables, Goods, or Services provided by Supplier;
3. Any Supplier Personnel is terminated or suspended or his or her employment is otherwise ended;
4. Supplier reasonably believes any Supplier Personnel poses a threat to a safe working environment, including to employees, customers, Company Confidential Information or Company Property;
5. There are any material adverse changes to any Supplier Personnel’s background history that conflict with such Supplier Personnel’s background report or record, including, without limitation, any information not previously known or reported in such report or record;
6. Any Supplier Personnel loses his or her U.S. work authorization;
7. Supplier’s provision of the Deliverables, Goods, or Services is either completed or terminated.
8. Any Supplier Personnel no longer requires unescorted physical access or electronic access, including IRA, to CIP Assets, or no longer meets the requirements for unescorted physical access or electronic access, including IRA, as set forth in Section 2.4 (Additional Requirements for Supplier Personnel CIP Assets Access).
   1. Access Revocation. Supplier will return to Company any Company Property including, but not limited to, Company photo ID badge, keys, parking pass, documents, laptop or other Company device in the possession of such Supplier Personnel no later than one day after the events identified in subsections (A) through (G) of Section 1.4 (Required Notification).
9. **SECURITY CHECKS.**
   1. Affected Supplier Personnel. Supplier will conduct Security Checks (as defined in Section 2.2 (Security Checks)) of all Supplier Personnel who require: (A) unescorted physical access to any Company Property (“Affected Supplier Personnel Category 1”); (B) a user name and password to access any Company Property; or (C) access to Company Property containing Confidential Information. Supplier Personnel meeting any of the requirements in subsections (B) and (C) above are individually and collectively referred to herein as, “Affected Supplier Personnel Category 2.” Affected Supplier Personnel Category 1 and Affected Supplier Personnel Category 2 are individually and collectively referred to herein as “Affected Supplier Personnel.”
   2. Security Checks. “Security Checks” means: (A) drug screening and background checks (consisting of a criminal history and employment history screening) conducted in accordance with the then-current “Company Access Request” (CAR) form located at <https://www.aps.com/en/About/Our-Company/Doing-Business-with-Us>; and (B) completion of the CAR form (attesting that the drug screening and background checks for each Affected Supplier Personnel have been satisfactorily completed). CAR forms for Affected Supplier Personnel must be submitted by Supplier to Company.
   3. Timing of Security Checks. Security Checks must be completed prior to any Affected Supplier Personnel's performance of the Services under any of the conditions described in clauses (A) through (C) in Section 2.1 (Affected Supplier Personnel), and Supplier will only allow those Supplier Personnel who successfully pass the Security Checks to perform the Services under any of the conditions described in clauses (A) through (C) in Section 2.1 (Affected Supplier Personnel).
   4. Additional Requirements for Supplier Personnel CIP Assets Access. If Affected Supplier Personnel require access to CIP Assets, then Affected Supplier Personnel will be subjected to additional Security Checks conducted by the Company as provided below.
      1. Unescorted physical or remote access to CIP Assets requires Supplier Personnel to receive annual Company CIP Assets training (“Company CIP Assets Training”) and be subject to a personnel risk assessment (“PRA”). Company will furnish all Company CIP Assets Training materials to Supplier for those Supplier Personnel that Company determines will require access to CIP Assets. Supplier will ensure that all Supplier Personnel having unescorted physical access or remote cyber access to CIP Assets have taken the Company CIP Assets Training. Supplier will maintain documentation that Company CIP Assets Training is conducted, including the date the Company CIP Asset Training was completed and attendance records. Supplier will retain such records from the current and previous full calendar year (unless directed by Company to retain specific evidence for a longer period of time) and make such records available to Company upon request.
      2. The enhanced background check requirements referenced in this Section 2.4 (Additional Requirements for Supplier Personnel CIP Assets Access) will be completed by Company at its expense. The PRA will comply with the background check requirements set forth in the CIP Reliability Standards and may be repeated at least every seven (7) years or more frequently for cause. The PRA will include an identity verification (e.g., performance of e-Verify or consent-based Social Security Number verification in the United States and review of government issued identification) and will be conducted pursuant to Affected Supplier Personnel consent as provided to Company.

* 1. Drug Screening Requirements. A negative result on a minimum 5-panel specimen drug screening is required of all Supplier Personnel requiring unescorted access to Company Property. Drug screening must be completed through a U.S. Department of Health and Human Services approved laboratory. The guidelines and requirements for drug screening are further detailed in the CAR form located at <https://www.aps.com/en/About/Our-Company/Doing-Business-with-Us>
  2. Costs; Records. With the exception of Section 2.4 (Additional Requirements for Supplier Personnel CIP Assets Access), Supplier is responsible for any costs incurred in conducting Security Checks of Supplier Personnel. Supplier will retain all records related to Security Checks for at least three (3) years after the completion of the Services (or longer if requested by Company), and will make such records available to Company upon request.

(END OF APPENDIX E)

**APPENDIX F – SUPPLIER PERSONNEL ACKNOWLEDGEMENT**

In accordance with my assignment to provide services to Arizona Public Service Company (**"Company"**), pursuant to Agreement No. [MLIS PO Number] between Company and Contracting Party Name (**"Supplier"**), and in light of the related confidential records and information that may be disclosed to me by Company in connection with this assignment (**"Confidential Information"**), I hereby acknowledge the following:

1. I am employed by Supplier, or if applicable Supplier’s subcontractor, and not Company.
2. Supplier (or its subcontractor) and not Company is responsible for paying all of my wages, benefits, and other compensation. Supplier (or its subcontractor) and not Company is responsible for withholding and/or paying all income tax, social security, unemployment compensation, workers’ compensation and other taxes, assessments, and other contributions.
3. I am not entitled to any Company-provided benefits, including, without limitation, vacation, sick leave, holiday pay, medical and dental benefits, outage or other Company incentives and 401k, and specifically disclaim all rights to such benefits.
4. I will familiarize myself with and adhere to all policies and procedures provided to me by Company that are applicable to supplier personnel working at or on Company’s site or equipment, including those pertaining to safe work practices, site work requirements, workplace harassment and maintaining a drug-free workplace.
5. I can be removed from my assignment at Company for any reason at any time, with or without notice, with no liability by Company.
6. I will only disclose, verbally or visually, any Confidential Information to which I may have access to Company and Supplier employees, agents or representatives who have a need to know and are authorized to have access to the Confidential Information, and to take all precautions necessary to prevent the Confidential Information from being disclosed to any third parties, unless expressly instructed in writing to do so by an authorized representative of the Company.
7. I will not use any Confidential Information disclosed to me by or on behalf of Company (including the knowledge gained therefrom) for any purpose other than in connection with my assignment for the Company.
8. I will not copy, reproduce, abstract, remove from the Company's facilities, or distribute, in whole or in part, any Confidential Information, unless expressly instructed in writing to do so by an authorized representative of the Company.
9. I will not use in connection with my assignment to Company any portion of any confidential or proprietary information that I may have acquired from or developed under another assignment or employer or other outside party, unless authorized in writing by such employer or other outside party.
10. For assignments of work concerning activities at the Palo Verde Generating Station, Confidential Information will include all categories of information classification defined in the Nuclear Administrative and Technical Manual, specifically Procedure 84DP-0RM32, Handling of Proprietary, Confidential and Highly Confidential Information, which is available upon request to Company, and will also include "Safeguards Information" and computer programs or related materials. For the purposes of this Appendix F (Supplier Personnel Acknowledgement), “Safeguards Information” means information not otherwise classified as national security information or restricted data that specifically identifies Palo Verde Generating Station‘s (PVGS): (A) detailed control accounting procedures for the physical protection of special nuclear material, (B) detailed security measures including security plans, procedures, and equipment for the physical protection of byproduct and special nuclear material, (C) security measures for the physical protection and location of certain plant equipment vital to the safety of production or utilization of facilities and (D) any information that could reasonably be expected to have a significant adverse effect by significantly increasing the likelihood of sabotage or diversion or theft of source, byproduct and  special nuclear material.
11. This Supplier Personnel Acknowledgement will not prohibit any communications to agencies that are required or allowed under applicable government regulations, including, without limitation, Nuclear Regulatory Commission regulations 10 C.F.R. Section 50.7 “Employee Protection” and 10 C.F.R. part 19.
12. I understand that if I am requested or ordered to disclose Confidential Information by any regulatory authority or by a court of law, or if I am requested by any other third party to disclose Confidential Information, I will promptly notify the authorized representative of the Company to whom I report on this assignment. In addition, I will provide full details of such order or request before I comply with it, so that the Company is afforded the opportunity to participate in the disclosure, for the purpose of resisting it, or otherwise to obtain any continuing protection of the Confidential Information that it considers necessary.
13. I understand that my obligations acknowledged in this Supplier Personnel Acknowledgement supersede any prior Non-Disclosure Agreement signed in connection with an assignment to Company and these obligations remain in effect following completion of the assignment.

Signature:

Printed Name:

(END OF APPENDIX F)

**APPENDIX G – CYBERSECURITY PROVISIONS**

**1. CONNECTION TO COMPANY CYBER ASSETS.**

* 1. Supplier will comply with the Company’s processes for connection to any Company Cyber Assets, including the requirements for verification, attestation, and documentation prior to any such connection.

1. **SUPPLIER CYBERSECURITY POLICY.**
   1. Supplier will provide to Company the Supplier’s cybersecurity policy, which must be consistent with the current revision of the National Institute of Standards and Technology (“NIST”) Special Publications 800-53 or 800-82, as applicable. Supplier will comply with and maintain that cybersecurity policy at all times. Any changes to Supplier’s cybersecurity policy that are inconsistent with the security requirements of NIST Special Publications 800-53 or 800-82, as applicable, are subject to review and approval by Company prior to implementation by Supplier.
2. **SECURITY INCIDENT NOTIFICATION AND MANAGEMENT.**
   1. Response Plan. Supplier will maintain policies and procedures to address Security Incidents (a “Response Plan”) including efforts taken to mitigate the harmful effects of Security Incidents, to address and remedy the occurrence, and to prevent the recurrence of Security Incidents. Supplier will provide the Response Plan to Company. The Response Plan must follow best practices that are, at a minimum, consistent with the current revision of the NIST Special Publication 800-61, and relevant sections of 800-53 or 800-82, as applicable.
   2. Notice of Security Incident. Notwithstanding any other notice requirements of the Agreement, Supplier will notify Company via email at acdc@aps.com immediately upon the occurrence of a Security Incident involving the Goods, Services or Deliverables or Supplier’s supply chain. Such notice must include the date and time of the Security Incident (or the approximate date and time of the occurrence if the actual date and time of the occurrence is not precisely known) and a detailed summary of the facts and circumstances of the Security Incident, including a description of: (A) why the Security Incident occurred (e.g., a precise description of the reason for the system failure); (B) the amount of Company’s Confidential Information or PII known or reasonably believed to have been Disclosed; (C) the potential security impact and recommended corrective actions specific to the Goods, Services and Deliverables provided by Supplier to Company; and (D ) the measures being taken to address and remedy the occurrence and to prevent the same or a similar event from occurring in the future.

Except as required by Applicable Law, Supplier agrees that it will not inform any third party of any Security Incident without Company's prior written consent. If such disclosure is required by Applicable Law, Supplier will work with Company regarding the content of the disclosure to minimize any potential adverse impact upon Company and its customers, employees and contractors.

* 1. Updates. Supplier will provide written updates to Company regarding the Security Incident. Such updates must identify all new facts or circumstances learned after the initial written notice and must be provided to Company within a reasonable time after learning of those new facts or circumstances.
  2. Implementation of Response Plan. Immediately upon learning of a Security Incident, Supplier will implement its Response Plan and, within twenty-four (24) hours of implementing its Response Plan, Supplier will notify Company of implementation via email at [acdc@aps.com](mailto:acdc@aps.com).
  3. Cooperation. Supplier will, at its sole cost and expense, assist and cooperate with Company in any: (A) investigation; (B) disclosures to affected parties; and (C) remedial measures, as requested by Company in connection with a Security Incident or as required under any Applicable Law. In the event a Security Incident results in the disclosure of Company’s Confidential Information or PII such that notification is required to be made to any person or entity pursuant to Applicable Law (including privacy and consumer protection laws) or pursuant to a request or directive from a governmental authority or Company, then such notification will be provided by Company, except as otherwise required by Applicable Law or as approved by Company in writing. Company will have sole control over the timing and method of providing such notification, and Supplier will pay or reimburse, as applicable, all costs and expenses for such notification.
  4. Prevention of Reoccurrence. Within seven (7) days following Supplier’s notice to Company of a Security Incident, Supplier will provide recommendations to Company via email at [acdc@aps.com](mailto:acdc@aps.com) regarding actions that Company may take to reduce the risks of reoccurrence of the same or a similar Security Incident, including, as appropriate, action plans and mitigating controls that Supplier will coordinate with Company to develop. Further, Supplier will provide guidance and recommendations to Company regarding long-term remediation of any cybersecurity risks posed to Company’s Confidential Information and Company Property, and will further provide any information necessary to assist Company in recovery efforts in response to a Security Incident. Within thirty (30) days of the occurrence of a Security Incident, Supplier will develop and execute a plan to reduce the likelihood of reoccurrence of the same or a similar Security Incident. Such prevention plan must be consistent with Supplier’s Response Plan and the current revision of NIST Special Publications 800-61 and 800-184, as applicable. Supplier will provide the prevention plan to Company.

If the Security Incident arises from a third-party supplier’s software, equipment or services, then if Supplier is permitted to disclose such information, Supplier shall provide updates to Company of such third-party supplier’s plan for the prevention of recurrence of such Security Incident.

* 1. Unrelated Incidents. If: (A) confidential information stored in Supplier’s computer networks is corrupted or destroyed, or is accessed, acquired, compromised, modified, used or Disclosed by any unauthorized person or by any person in an unauthorized manner or for an unauthorized purpose; (B) Supplier knows or reasonably believes that an act or omission has compromised or may reasonably compromise the cybersecurity of the products of services that Supplier provided to an entity other than Company; or (C) Supplier receives a complaint, notice, or communication relating directly or indirectly to (i) Supplier’s handling of confidential information, (ii) Supplier's compliance with Applicable Law in connection with confidential information, or (iii) the cybersecurity of confidential information that Supplier has transmitted (the aforementioned (A), (B) and (C), an “Unrelated Incident”), and the Unrelated Incident has the reasonable potential to either negatively impact the Goods, Deliverables, or Service provided or to be provided to Company, or to harm Company, then Supplier will provide to Company a confidential report describing, to the extent legally permissible, a detailed summary of the facts and circumstances of the Unrelated Incident, including a description of the Unrelated Incident, why it occurred, and the measures being taken to address and remedy the occurrence and to prevent the same or a similar event from occurring in the future.

1. **ACCESS.**
   1. Supplier Personnel Access. Supplier will review and verify Supplier Personnel’s need for unescorted physical access or electronic access, including Interactive Remote Access (“IRA”), to Company Confidential Information and Company Property at least once every six (6) months during the term of the Agreement. Supplier will retain evidence of such reviews for two (2) years from the date of each review.
   2. Access to Company Cyber Assets. Supplier and Supplier Personnel will not access or connect to Company Cyber Assets without Company’s prior written authorization, which Company may revoke at any time and for any reason in the exercise of its sole discretion. The scope of such authorization may be limited by Company, and Supplier and Supplier Personnel must comply at all times with that authorization, in addition to the requirements set forth in the Agreement.
   3. Access Control Policy. Supplier will maintain policies and procedures to address the security of remote and onsite access to Company Information and Company Property, including systems and networks (an “Access Control Policy”), that is consistent with the personnel management requirements of the current revision of NIST Special Publication 800-53, AC-2, PE-2, PS-4, and PS-5, as applicable, and the requirements of this Appendix G (Cybersecurity).
   4. Required Notification and Revocation. Supplier will immediately notify Company Leader, as identified in Company’s vendor management system, in writing, and orally, **no later than 4 hours** after any of the events identified in subsections (A) through (G) below so that Company can revoke unescorted physical access and electronic access, including IRA, for such Supplier Personnel.
2. Any Supplier Personnel no longer requires access to Company Confidential Information or Company Property to furnish the Deliverables, Goods, or Services provided by Supplier;
3. Any Supplier Personnel is terminated or suspended or his or her employment is otherwise ended;
4. Supplier reasonably believes any Supplier Personnel poses a threat to a safe working environment, including to employees, customers, Company Confidential Information or Company Property;
5. There are any material adverse changes to any Supplier Personnel’s background history that conflict with such Supplier Personnel’s background report or record, including, without limitation, any information not previously known or reported in such report or record;
6. Any Supplier Personnel loses his or her U.S. work authorization;
7. Supplier’s provision of the Deliverables, Goods, or Services is either completed or terminated.
8. Any Supplier Personnel no longer requires unescorted physical access or electronic access, including IRA, to CIP Assets, or no longer meets the requirements for unescorted physical access or electronic access, including IRA, as set forth in Appendix E (Company Access and Security Checks).
   1. Access Revocation. Supplier will return to Company any Company Property including, but not limited to, Company photo ID badge, keys, parking pass, documents, laptop or other Company device in the possession of such Supplier Personnel no later than one day after the events identified in subsections (A) through (G) of Section 4.4 (Required Notification and Revocation).
9. **AUTHENTICATION; AUTHORIZATION.**
   1. Supplier will integrate their access and authorization service with the Company’s authentication provider, i.e.; Ping, a single sign-on service, for Company managed access or revocation.
   2. Supplier will document the Deliverables, Goods, and Services levels, methods, and capabilities for authentication and authorization.
   3. Supplier will provide a method for defining user and process accounts, access and security permissions, and applications with roles based access control capability.
   4. Supplier will provide a method for protecting against unauthorized privilege escalation.
   5. Supplier will verify and provide documentation for the Deliverables, Goods, and Services attesting that undocumented or unauthorized logging or control functions are not installed (e.g., key loggers, software to activate cameras and microphones, remote or autonomous command and control capabilities, etc.).
   6. Supplier will document all accounts (including, but not limited to, generic and/or default) and identify those that need to be active for proper operation of the Deliverables, Goods, and Services.
   7. Supplier will change default account settings to Company-specific settings (e.g., length, complexity, history, and configurations) or support Company in these changes. Supplier will not publish changed account information. Supplier will provide new account information to the Company via a protected mechanism.
   8. Prior to delivery of the Deliverables, Goods, and Services to Company, Supplier will remove or disable any accounts that are not needed for normal or maintenance operations of the Deliverables, Goods, and Services.
   9. Supplier will protect credentials, including not storing passwords (user and process) in clear text and not hardcoding passwords into Deliverable software or scripts.
   10. The Deliverables, Goods, and Services may only allow access protocols that encrypt or securely transmit login credentials (e.g., tunneling through Secure Shell Terminal Emulation (SSH) and Transport Layer Security (TLS)).
   11. The Deliverables, Goods, and Services may not allow multiple concurrent logins using the same authentication credentials, allow applications to retain login information between sessions, provide any auto-fill functionality during login, or allow anonymous logins.
   12. Supplier will provide a configurable account password management capability that allows for, but is not limited to, the following:
       * Changes to passwords (including default passwords)
       * Selection of password length
       * Frequency of change
       * Setting of required password complexity
       * Number of login attempts prior to lockout
       * Inactive session logout
       * Screen lock by application
       * Comparison to a library of forbidden strings
       * Derivative use of the user name
       * Denial of repeated or recycled use of the same password
10. **SOFTWARE; SERVICES.**
    1. Supplier will remove all software components that are not required for the operation and/or maintenance of the Deliverables, Goods, and Services. This removal must not impede the primary function of the Deliverables, Goods, and Services. If software that is not required cannot be removed or disabled, Supplier will document a specific explanation and provide risk mitigating recommendations and/or specific technical justification. The software to be removed and/or disabled must include, but not be limited to:
       * Games
       * Device drivers for product components not procured/delivered
       * Messaging services (e.g., email, instant messenger, peer-to-peer file sharing)
       * Software compilers in user workstations and servers
       * Software compilers for programming languages that are not used in the Deliverables, Goods, or Services
       * Unused networking and communications protocols
       * Unused administrative utilities, diagnostics, network management, and system management functions
       * Backups of files, databases, and programs used only during system development
       * All unused data and configuration files
    2. Supplier will provide documentation of software/firmware that supports the Deliverables, Goods, and Services, including scripts and/or macros, run time configuration files and interpreters, databases and tables, and all other included software (identifying versions), revisions, and /or patch levels, as delivered.
    3. Supplier will ensure the Deliverables, Goods, and Services utilize only services and/or ports required for normal operation, emergency operations, or troubleshooting and Supplier will provide documentation listing all ports and authorized services required for normal operation, emergency operation, or troubleshooting.
    4. Supplier will ensure Deliverables, Goods, and Services do not contain any malicious code or limit the capability to execute code which escalates privileges beyond those required for normal or emergency operation of the Deliverables, and, where Goods and Services are being provided, ensure that malicious code or the capability to execute code which escalates privileges beyond those required for normal or emergency operation of a Company Cyber Asset are not introduced to such asset during the provision of the Services.
    5. Supplier will provide summary documentation of the Deliverables, Goods, and Services, security features and security-focused instructions on product maintenance, support, and reconfiguration of default settings.
    6. Upon Company's request, Supplier will return or document the secure disposal of Company's data and Company-owned hardware that is no longer needed by the Supplier (e.g., NIST Special Publication SP 800-80).
    7. Supplier will use trusted and secure channels to ship Deliverables, Goods and Services, such as encrypted digital delivery or U.S. registered mail.
11. **LOGGING; AUDITING.**
    1. Supplier will provide logging capabilities or the ability to support Company's existing logging system. Logging capabilities provided by Supplier must be configurable by Company and support Company's security auditing requirements. As specified by Company, the Deliverables, Goods, and Services must cover the following events, at a minimum (as appropriate to their function):
       * Information requests and server responses
       * Successful and unsuccessful authentication and access attempts
       * Account changes
       * Privileged use
       * Application start-up and shutdown
       * Application failures
       * Major application configuration changes
    2. Supplier will time stamp audit trails and log files.
    3. Supplier will provide confidentiality and integrity security protection of log files.
    4. Supplier will maintain an approach for collecting and storing (e.g., transfer or log forwarding) security log files.
    5. Supplier will provide a list of all log management capabilities that the Deliverables, Goods, and Services are capable of generating and the format of those logs. This list must identify which logs are enabled by default.
12. **MALWARE DETECTION AND PREVENTION.**
    1. Supplier will validate that cybersecurity services (e.g., virus checking, malware detection and host intrusion detection) do not conflict with operation of the Deliverables, Goods, and Services.
    2. Supplier will verify that the addition of security features does not adversely affect connectivity, latency, bandwidth, response time, and throughput specified for performance of the Deliverables, Goods, and Services.
13. **VULNERABILITY MANAGEMENT.**
    1. Supplier will maintain policies and procedures to address the disclosure and remediation by Supplier of Vulnerabilities and material defects related to the Deliverables, Goods, and Services including the following:
14. Prior to the delivery of the Deliverables, Goods, or Services, Supplier will provide summary documentation of publicly disclosed Vulnerabilities and material defects related in the Deliverables, Goods, or Services, the potential impact of such Vulnerabilities and material defects, the status of Supplier’s efforts to mitigate those publicly disclosed Vulnerabilities and material defects, and Supplier’s recommended corrective actions, compensating security controls, mitigations, and/or procedural workarounds;
15. Supplier will provide summary documentation of Vulnerabilities and material defects in the Deliverables, Goods, and Services to Company via email at [acdc@aps.com](mailto:acdc@aps.com) within thirty (30) days after such Vulnerabilities and material defects become known to Supplier. This includes summary documentation on Vulnerabilities that have not been publicly disclosed or have only been identified after the delivery of the Deliverables. Summary documentation must include a description of each Vulnerability and material defect and its potential impact, root cause, and recommended corrective actions, compensating security controls, mitigations, and procedural workarounds;
16. Supplier will disclose the existence of all known methods for bypassing computer authentication in the Deliverables, Goods, and Services, often referred to as backdoors, and will provide written documentation that all such backdoors created by Supplier have been permanently deleted or disabled; and
17. Supplier will maintain a vulnerability detection and remediation program consistent with the current versions of NIST Special Publication 800-53, 4 RA-5, SA-11, and SI-2, as applicable.
    1. Whether or not publicly disclosed by Supplier and notwithstanding any other limitation in the Agreement, following written notice provided to and acknowledged by Supplier, Company may disclose any Vulnerabilities or material defects in the Deliverables, Goods, or Services provided by Supplier to: (A) the Electricity Information Sharing and Analysis Center (E-ISAC), the Industrial Control Systems Cyber Emergency Response Team (ICS- CERT), or any comparable entity; (B) any entity, if so necessary to preserve the reliability of Company Property, as determined by Company in its sole discretion; and (C) any entity, if so required by Applicable Law.
    2. Supplier will communicate security-related technical issues to Company via email at [acdc@aps.com](mailto:acdc@aps.com) within seven (7) days of becoming known to Supplier. This communication is not intended for non- technical contract-related issues.
    3. Supplier will maintain a quality assurance program and validate that all software and firmware included in the Deliverables, Goods, and Services have undergone quality control testing to identify and correct potential cybersecurity weaknesses and Vulnerabilities. This testing must include fuzz testing, static testing, dynamic testing, and penetration testing. Supplier will use positive and appropriate negative tests to verify that the Deliverables, Goods, and Services operate in accordance with requirements and without extra functionality, and will monitor for unexpected or undesirable behavior during such tests. Supplier will provide summary documentation of the results of the testing that includes unresolved Vulnerabilities and recommended mitigation measures.
    4. Supplier will provide a secure process for users to submit problem reports and remediation requests. This process must include tracking history and corrective action status reporting.
    5. Upon the Company’s submission of a problem report to Supplier, Supplier will review the report, provide status updates of problem resolution within fifteen (15) days, and develop an initial action plan for resolution of the problem within thirty (30) days.
    6. Supplier will provide Company with Supplier’s responsible disclosure and threat reporting policies and procedures (e.g., Computer Emergency Response Teams (CERTs)), which must address public disclosure protections implemented by Supplier.
18. **HARDWARE, FIRMWARE, SOFTWARE, AND PATCH INTEGRITY AND AUTHENTICITY.**
    1. Supplier will maintain risk management policies, procedures and processes for supply chain delivery of hardware, software (including patches), and firmware provided to Company. Supplier will provide documentation of its chain-of-custody practices, inventory management program (including the location and protection of spare parts), information protection practices, integrity management program for components provided by sub-suppliers, instructions on making requests for replacement parts, and commitment to ensure that, for the operational life of such item, spare parts are available by Supplier.
    2. Upon request by Company and if such information is not Supplier’s confidential information or otherwise protected by legal privilege, Supplier shall specify how digital delivery for procured products (e.g., software and data) including patches will be validated and monitored to ensure the digital delivery remains as specified. When product features and delivery mechanisms allow, Supplier shall apply encryption technology to protect procured products throughout the delivery process.
    3. If Supplier provides software or patches to Company, Supplier will publish or provide a hash conforming to the Federal Information Processing Standard (FIPS) Security Requirements for Cryptographic Modules (FIPS 140-2) or similar standard information on the software and patches to enable Company to use the hash value as a checksum to independently verify the integrity of the software and patches and avoid downloading the software or patches from Supplier’s website that has been surreptitiously infected with a virus or otherwise corrupted without the knowledge of Supplier.
    4. Supplier shall provide a software bill of materials for procured (including licensed) Goods consisting of a list of components and associated metadata that make up a component.
    5. Supplier will identify the country (or countries) of origin of the Deliverables, Goods, and Services and components (including hardware, software, and firmware). Supplier will identify the countries where the development, manufacturing, maintenance, and service for the Deliverables, Goods, and Services are provided. Supplier will notify Company of any changes in the list of these countries at least one hundred and eighty (180) days prior to initiating a change in the list of countries.
    6. Supplier will use trusted channels to ship the Deliverables, Goods, and Services, such as U.S. registered mail.
    7. Supplier will document the capability for detecting unauthorized access throughout the delivery process.
    8. Supplier will provide chain-of-custody documentation for the Deliverables, Goods, and Services, as determined by Company in its sole discretion, and will require tamper-evident packaging for delivery.
19. **PATCHING GOVERNANCE.**
    1. Prior to the delivery of any Deliverables, Goods, or Services, and prior to any connection of electronic devices, assets or equipment to Company Property, Supplier will provide documentation regarding its patch management and vulnerability management/mitigation programs and update processes (including third-party hardware, software, and firmware) for the Deliverables, Goods, and Services, and any electronic device, asset, or equipment to be connected to Company Property during the provision of the Deliverables, Goods, and Services. Such documentation must include information regarding:
20. The resources and technical capabilities needed to sustain Supplier’s program and process, or recommendation for how the integrity of a patch is to be validated by Company; and
21. Supplier's approach and capability to remediate newly reported zero-day Vulnerabilities.
    1. The current or supported version of the Deliverables, Goods, and Services must not require the use of out-of-date, unsupported, or end-of-life version of third-party components (e.g., Java, Flash, Web browser, etc.).
    2. Supplier will verify and provide documentation that the Deliverables and Goods (including third- party hardware, software, and firmware) and the Services have appropriate updates and patches installed prior to delivery to Company.
    3. Supplier will provide appropriate software and firmware updates to remediate newly discovered Vulnerabilities or weaknesses within thirty (30) days of such discovery. Updates to remediate critical Vulnerabilities must be provided within fourteen (14) days of such discovery. If updates cannot be made available by Supplier within these time periods, Supplier will provide mitigations and/or workarounds to Company within seven (7) days.
    4. When third-party hardware, software (including open-source software), and firmware is provided by Supplier to Company, Supplier will provide appropriate hardware, software, and firmware updates to remediate newly discovered Vulnerabilities or weaknesses within sixty (60) days of such discovery. Updates to remediate critical Vulnerabilities, as determined by the Common Vulnerability Scoring System (CVSS), must be provided within thirty (30) days of such discovery. If such third-party updates cannot be made available by Supplier within these time periods, Supplier will provide mitigations and/or workarounds to Company within fourteen (14) days.
22. **VIRUSES, FIRMWARE AND MALWARE.**
    1. Supplier will use best efforts to investigate whether computer viruses or malware are present in any software or patches before providing such software or patches to Company. To the extent Supplier is providing third-party software or patches, Supplier will use reasonable effort to ensure the third-party investigates whether computer viruses or malware are present in any software or patches prior to providing them to Company or installing them on Company Cyber Assets.
    2. Supplier warrants that it has no knowledge of any computer viruses or malware coded or introduced into any software or patches, and Supplier will not insert any code which would have the effect of disabling or otherwise shutting down all or a portion of such software or damaging information or functionality. To the extent Supplier is providing third-party software or patches, Supplier will use reasonable efforts to ensure the third-party will not insert any code which would have the effect of disabling or otherwise shutting down all or a portion of such software or damaging information or functionality.
    3. If installed files, scripts, firmware, or other Supplier-delivered software solutions are flagged as malicious, infected, or suspicious by an anti-virus vendor through open source solutions like “Virus Total,” Supplier will provide technical proof as to why the “false positive” hit has taken place to ensure their code’s supply chain has not been compromised.
    4. If a virus or other malware is found to have been coded or otherwise introduced as a result of Supplier’s breach of its obligations under the Agreement, Supplier will immediately and at its own cost:
23. Take all necessary remedial actions and provide assistance to Company to eliminate the virus or other malware throughout Company’s systems and networks, regardless of whether such systems or networks are operated by or on behalf of Company;
24. If the virus or other malware causes a loss of operational efficiency or any loss of data where Supplier is obligated under the Agreement to back up such data, take all steps necessary and provide all assistance required by Company and its affiliates to mitigate the loss of or damage to such data and to restore the efficiency of such data; and
25. Where Supplier is not obligated under the Agreement to back up such data, use commercially reasonable efforts to mitigate the loss of or damage to such data and to restore the efficiency of such data.
26. **END OF LIFE OPERATING SYSTEMS.**
    1. The Deliverables, Goods, and Services must not be required to reside on end-of-life operating systems, or any operating system that will go end-of-life within twelve (12) months from the date of installation.
    2. Supplier will support the latest versions of operating systems for Supplier-provided software that is installed within twenty-four (24) months of official public release of an operating system version.
27. **CRYPTOGRAPHIC REQUIREMENTS.**
    1. Supplier will document how its cryptographic system protects the confidentiality, data integrity, authentication, and non-repudiation of devices and data flows in the underlying system, as requested by Company. This documentation must include, but not be limited to, the following:
28. The cryptographic methods (hash functions, symmetric key algorithms, or asymmetric key algorithms) and primitives (e.g., Secure Hash Algorithm (SHA-256), Advanced Encryption Standard (AES-128), RSA, and Digital Signature Algorithm (DSA-2048)) that are implemented in the system, and how these methods are to be applied; and
29. The preoperational and operational phases of key establishment, deployment, ongoing validation, and revocation.
    1. Supplier will use only “approved” cryptographic methods as defined in the FIPS 140- 2 Standard when enabling encryption on its products.
    2. Supplier will provide an automated remote key-establishment (update) method that protects the confidentiality and integrity of the cryptographic keys.
    3. Supplier will ensure that:
30. The system implementation includes the capability for configurable crypto periods (the life span of cryptographic key usage) in accordance with the Suggested Crypto periods for Key Types found in the current revision of NIST 800-57 Part 1, as applicable;
31. The key update method supports remote re-keying of all devices within ninety (90) days as part of normal system operations; and
32. Emergency re-keying of all devices can be remotely performed within thirty (30) days.
    1. Supplier will provide to Company a method for updating cryptographic primitives or algorithms utilized by Supplier.
33. **SECURE DEVELOPMENT PRACTICES.**
    1. Supplier will provide summary documentation of its secure product development life cycle including the standards, practices (including continuous improvement), and development environment (including the use of secure coding practices) used to create or modify Supplier- provided hardware, software, and firmware. The Supplier shall document how the most critical application security weaknesses (including Open Web Application Security Project (OWASP) Top 10 or SANS Top 25 Most Dangerous Software Errors) are addressed in Supplier's system development life cycle.
    2. Supplier will provide summary documentation of its coding reviews, including defect lists and plans to correct identified Vulnerabilities.
    3. Supplier will provide documentation of all input validation testing including, but not limited to, measures for prevention of command injection, structured query language injection, directory traversal, remote file include, cross-site scripting, and buffer overflow.
    4. Supplier will provide a contingency plan for sustaining the security of the Deliverables, Goods, and Services in the event Supplier ceases to operate in the industry (e.g., security-related procedures and products placed in escrow).
34. **REMOTE ACCESS.**
    1. Supplier will coordinate with Company on all remote access to Company’s systems and networks, regardless of interactivity, and will comply with all controls for interactive remote access and system-to-system remote access sessions requested by Company.
    2. If Supplier directly, or through any affiliates, subcontractors, or service providers, connects to Company’s systems or networks, the following protective measures must be maintained by Supplier:
35. Supplier will not access, and will not permit any other person or entity to access, Company's systems or networks without Company's authorization and any such actual or attempted access must be consistent with Company’s authorization;
36. Supplier will maintain processes designed to protect credentials as they travel throughout the network and will ensure that network devices have encryption enabled for network authentication to prevent possible exposure of credentials;
37. If Supplier Personnel use a virtual private network or other device to simultaneously connect machines on any Company system or network to any machines on any Supplier or third-party systems, Supplier will:
    1. Use only a remote access method consistent with Company’s remote access control policies;
    2. Provide to Company the full name, phone number, and email address of each Supplier Personnel who use any such remote access method; and
    3. Ensure that any computer used by Supplier Personnel to remotely access any Company system or network will not simultaneously access the Internet or any other third-party system or network while logged on to Company systems or networks.
    4. Supplier will ensure that Supplier Personnel accessing Company networks are uniquely identified and that accounts are not shared between Supplier Personnel.
38. **RETURN OR DESTRUCTION OF REMOVABLE MEDIA.**
    1. Within fifteen (15) days following expiration or termination of the Agreement, or at any time upon Company’s request, Supplier will return to Company all hardware and removable media provided by Company that contains Company’s Confidential Information. Company’s Confidential Information in such returned hardware and removable media shall not be removed or altered in any way. The hardware must be physically sealed and returned via bonded courier, or as otherwise directed by Company.
    2. If hardware or removable media containing Company’s Confidential Information is owned by Supplier or a third-party, Supplier will provide to Company within fifteen (15) days following expiration or termination of the Agreement, or upon Company’s request, a notarized statement detailing the destruction method used and the data sets involved, the date of destruction, and the entity or individual who performed the destruction. Supplier’s destruction or erasure of Company’s Confidential Information pursuant to this Section 17 (Return or Destruction of Removable Media) must be in compliance with industry best practices (e.g., Department of Defense 5220-22-M Standard, as amended).
    3. Upon the later of (i) completion of the delivery of the Goods and Services to be provided under this Agreement, (ii) the termination of any applicable warranty period under the Agreement or (iii) the termination of this Agreement, Supplier will return to Company all hardware and removable media provided by Company containing Company Information. Company Information in such returned hardware and removable media shall not be removed or altered in any way. The hardware should be physically sealed and returned via a bonded courier or as otherwise reasonably directed by Company. If the hardware or removable media containing Company Information is owned by Supplier or a third-party, a notarized statement detailing the destruction method used and the data sets involved, the date of destruction, and the entity who performed the destruction will be sent to a designated Company security representative within thirty (30) calendar days after the later of (i) completion of the delivery of the Goods and Services to be provided under this Agreement, (ii) the termination of any applicable warranty period under the Agreement or (iii) the termination of this Agreement. Supplier’s destruction or erasure of Company Information pursuant to this Section shall be in compliance with industry standard practices (e.g., Department of Defense 5220-22-M Standard, as may be amended).
39. **AUDIT RIGHTS.**
    1. Company or its third-party designee may, but is not obligated to, perform audits and security tests of Supplier’s information technology or systems environment and procedural controls to determine Supplier’s compliance with the Agreement. Such audits and tests may include coordinated security tests, interviews of relevant Supplier Personnel, review of documentation, and technical inspection of systems and networks as they relate to the receipt, maintenance, use, retention, and authorized destruction of Company’s Confidential Information.
    2. Supplier will provide all information reasonably requested by Company in connection with any audit and will provide reasonable access and assistance to Company upon request.
    3. Supplier will comply, within reasonable timeframes at its own cost and expense, with all reasonable recommendations that result from such inspections, tests, and audits. Company reserves the right to view, upon request, any original security reports that Supplier has undertaken or commissioned to assess Supplier’s own network security. If requested, copies of these reports will be sent via bonded courier to Company. Supplier will notify Company of any such security reports or similar assessments once they have been completed. Any regulators of Company or its affiliates shall have the same rights of audit as described herein upon request.

(END OF APPENDIX G)

**APPENDIX H - DATA SECURITY AND PRIVACY**

1. **RESTRICTED INFORMATION.**
   1. Supplier may, or is otherwise expected to electronically, handle, remotely access, exchange, transmit, monitor, store, process or host Restricted Information or Supplier’s system or network will be used to store, process or host Confidential Information including data hosting services or computing services (i.e. Software as a Service) as part of the Services that Supplier may provide under this Agreement.
   2. Restricted Information, including all copies, derivatives and summaries thereof, is the property of Company. Supplier will use the Confidential Information solely to perform Supplier's obligations under this Agreement. Except as expressly permitted in this Appendix H, Supplier may not sell, assign, lease, disseminate, or otherwise dispose of the Confidential Information or any part thereof to any other person, nor may Supplier commercially exploit any part of the Restricted Information. Supplier may not possess or assert any property interest in or any lien or other right against or to any Confidential Information.
2. **SECURITY CONTROLS.** 
   1. During the period Supplier is processing, handling or storing any Confidential Information, Supplier will (A) maintain commercially reasonable administrative, technical, and physical security controls to protect against destruction, loss, alteration of or unauthorized access to such Confidential Information, including, but not limited to, those set forth below in this Section 2 (Security Controls); and (B) not, without Company’s prior written approval, modify to the detriment of Company or its customers or personnel, or discontinue, any such security controls without comparable or better replacement security controls.
   2. Supplier will maintain an information security program that includes, at minimum, policies, procedures and tools that at all times meet or exceed industry applicable security frameworks and standards (e.g., NIST 800-53, COBIT, ISO 27000 series), and comply with any regulation established by applicable U.S. and/or foreign governmental regulatory agencies, and the written standards required by Company's Information Security Department and provided to Supplier from time to time.
   3. Supplier will routinely scan for and screen viruses and other malicious code from its software and computer equipment. Supplier will provide and use current industry standard anti-virus scanning software that will scan for and screen viruses and other malicious code from all data, files, e-mails, graphics, and images that may otherwise be transferred to Company or its customers’, employees’ or contractors’ computer network or equipment.
   4. Supplier will routinely update all anti-malware software signature and definition files. Supplier will immediately notify Company if it becomes aware of any viruses, malicious code or any other mechanisms that could harm Company or its customers’, employees’ or contractors’ computer network, equipment or data.
   5. Supplier will maintain and use an industry accepted advanced firewall. Supplier’s firewalls must log and audit all connections. Logs from firewalls must be securely stored. Firewalls must be configured to deny-by-default with explicit rules created for only necessary connections.
   6. Supplier will maintain an industry standard Intrusion Detection System (IDS) that will cover its network, and if applicable, host.
   7. Upon request, Supplier will provide Company with its data security policy, including its procedures and requirements for:
3. Server accessibility
4. Password policy
5. Usage policies
6. Authentication procedures
7. Encryption procedures
8. Remote access, including dial-in, usage and procedures
   1. Remote access (dial-in, high speed, or others) to Supplier’s network will be segregated from the rest of the network and will utilize strong, two-factor authentication.
   2. Supplier will limit access to Confidential Information to the least number of authorized Supplier Personnel necessary.
   3. Supplier will control physical and electronic access to Supplier’s servers, and Supplier’s telecom closets must be controlled via cipher or card-swipe type locks.
   4. Supplier will maintain a disaster recovery procedure as it relates to Confidential Information, and, upon Company’s request, provide it to Company for review. Such disaster recovery procedure must address, at a minimum, offsite tapes, backups, and Supplier’s facility.
   5. Supplier will maintain procedures on patching Supplier’s networked systems (servers, operating systems, etc.), and, upon Company’s request, provide such procedures to Company. Supplier will apply critical security patches to all networked systems within thirty (30) days of vendor release of such patches and will retain patching records for a period of not less than one (1) year.
   6. Supplier will segregate all Restricted Information from Supplier’s information or the information of Supplier’s other customers.
9. **PRIVACY AND DATA SECURITY LAWS, SECURITY POLICIES AND PROCEDURES.** 
   1. Supplier acknowledges the sensitivity and confidentiality of personal information which may be contained in Confidential Information and that such information may be subject to Applicable Law.
   2. Supplier will comply with all Applicable Law and contractual requirements relating to the privacy and confidentiality of PII in the performance of its obligations under this Agreement.
   3. Supplier security controls will include policies for the provisioning of access to Confidential Information limited solely to those Supplier Personnel with a business reason or need to perform Supplier’s obligations under this Agreement and the disposal/destruction of any such Confidential Information that are in compliance with Applicable Laws.
   4. If, during the term of the Agreement, Supplier has access to, collects, accesses, uses, stores, processes, disposes of or discloses credit, debit, or other payment cardholder information, Supplier will comply with Payment Card Industry Data Security Standards (“PCI DSS”).
   5. Supplier is responsible for any breach of this Appendix H or violation of Applicable Law by its Supplier Personnel.
10. **SECURITY INCIDENT NOTIFICATION AND MANAGEMENT.**
    1. Response Plan. Supplier will maintain policies and procedures to address Security Incidents (a “Response Plan”) including efforts taken to mitigate the harmful effects of Security Incidents, to address and remedy the occurrence, and to prevent the recurrence of Security Incidents. Upon request, Supplier will provide the Response Plan to Company. The Response Plan must follow best practices that are, at a minimum, consistent with the current revision of the NIST Special Publication 800-61, and relevant sections of 800-53 or 800-82, as applicable.
    2. Notice of Security Incident. Notwithstanding any other notice requirements of the Agreement, Supplier will notify Company via email at acdc@aps.com and via written letter to Company’s designated representative (as specified in the Agreement) immediately upon the occurrence of a Security Incident involving the Goods, Services or Deliverables or Supplier’s supply chain. Such notice must include the date and time of the Security Incident (or the approximate date and time of the occurrence if the actual date and time of the occurrence is not precisely known) and a detailed summary of the facts and circumstances of the Security Incident, including a description of: (A) why the Security Incident occurred (e.g., a precise description of the reason for the system failure); (B) the amount of Confidential Information known or reasonably believed to have been Disclosed; (C) the potential security impact and recommended corrective actions specific to the Goods, Services and Deliverables provided by Supplier to Company; and (D ) the measures being taken to address and remedy the occurrence and to prevent the same or a similar event from occurring in the future.

Except as required by Applicable Law, Supplier will not inform any third party of any Security Incident without Company's prior written consent. If such disclosure is required by Applicable Law, then such notification will be provided by Company, except as otherwise required by Applicable Law or as approved by Company in writing. Company will have sole control over the timing and method of providing such notification to minimize any potential adverse impact upon Company and its customers, employees and contractors, and Supplier will pay or reimburse, as applicable, all costs and expenses for such notification.

* 1. Updates. Supplier will provide written updates to Company regarding the Security Incident. Such updates must identify all new facts or circumstances learned after the initial written notice and must be provided to Company within a reasonable time after learning of those new facts or circumstances.
  2. Implementation of Response Plan. Immediately upon learning of a Security Incident, Supplier will implement its Response Plan and, within twenty-four (24) hours of implementing its Response Plan, Supplier will notify Company of implementation via email at acdc@aps.com and via written letter to Company’s designated representative.
  3. Cooperation. Supplier will, at its sole cost and expense, assist and cooperate with Company in any: (A) investigation; (B) disclosures to affected parties; and (C) remedial measures, as requested by Company in connection with a Security Incident or as required under any Applicable Law.
  4. Prevention of Reoccurrence. Within seven (7) days following Supplier’s notice to Company of a Security Incident, Supplier will provide recommendations to Company via email at acdc@aps.com and via written letter to Company’s designated representative regarding actions that Company may take to reduce the risks of reoccurrence of the same or a similar Security Incident, including, as appropriate, action plans and mitigating controls that Supplier will coordinate with Company to develop. Further, Supplier will provide guidance and recommendations to Company regarding long-term remediation of any cybersecurity risks posed to Confidential Information and Company Property and will further provide any information necessary to assist Company in recovery efforts in response to a Security Incident. Within thirty (30) days of the occurrence of a Security Incident, Supplier will develop and execute a plan to reduce the likelihood of reoccurrence of the same or a similar Security Incident and provide such plan to Company via email at [acdc@aps.com](mailto:acdc@aps.com) and via written letter to Company’s designated representative. Such prevention plan must be consistent with Supplier’s Response Plan and the current revision of NIST Special Publications 800-61 and 800-184, as applicable.
  5. Unrelated Incidents. If: (A) confidential information stored in Supplier’s computer networks is corrupted or destroyed, or is accessed, acquired, compromised, modified, used or Disclosed by any unauthorized person or by any person in an unauthorized manner or for an unauthorized purpose; (B) Supplier knows or reasonably believes that an act or omission has compromised or may reasonably compromise the cybersecurity of the products of services that Supplier provided to an entity other than Company; or (C) Supplier receives a complaint, notice, or communication relating directly or indirectly to (i) Supplier’s handling of confidential information, (ii) Supplier's compliance with Applicable Law in connection with confidential information, or (iii) the cybersecurity of confidential information that Supplier has transmitted (the aforementioned (A), (B) and (C), an “Unrelated Incident”), and the Unrelated Incident has the reasonable potential to either negatively impact the Goods, Deliverables, or Services provided or to be provided by Supplier to Company, or to harm Company, then Supplier will provide to Company a confidential report describing, to the extent legally permissible, a detailed summary of the facts and circumstances of the Unrelated Incident, including a description of the Unrelated Incident, why it occurred, and the measures being taken to address and remedy the occurrence and to prevent the same or a similar event from occurring in the future.

1. **Encryption of Certain Restricted Information.** 
   1. Encryption Methods. Supplier will use methods that meet current industry minimum requirements and that are mutually agreed upon, but in all cases at a minimum of 256-bit encryption, to encrypt all Restricted Information that Supplier electronically transmits or stores.
   2. Encryption Transmissions. Supplier will cooperate with Company in receiving encrypted transmissions from Company.
   3. Mask PII. Supplier will mask all PII used in any testing or non-production environment in accordance with Company’s requirements.
2. **Risk Assessment.**

Upon fifteen (15) days’ notice Company may conduct a risk assessment via questionnaire to determine the data security risks associated with the Services to be performed, and, depending on the results of this assessment, Company may be required by its internal security policies to conduct a site audit or other risk evaluations of Supplier's operations. Supplier will cooperate with Company in such initial assessment, and any subsequent required evaluations in order to permit Company to evaluate the relevant information and security planning of Supplier. If Company determines that Supplier does not comply with the data security requirements contained in this Agreement or this Appendix H, and Supplier is unable to correct such deficiencies after commercially reasonable efforts, then, upon written notice to Supplier and without limiting Company's other remedies hereunder, Company may refuse to proceed with the planned Services and terminate this Agreement and/or any Order or statement of work at no cost to Company.

1. **Security Audits and Reports.** 
   1. Reporting Requirements for Restricted Personal Information. If Supplier will be performing Services requiring storage or processing of Restricted Personal Information at Supplier’s or its Subcontractor’s site, then, at least once annually, Supplier will have an audit of its (and as applicable, its Subcontractors’) operations performed by an independent auditing firm in accordance with the American Institute of Certified Public Accountants (“AICPA”) current version of the Statements of Standards of Attestation Engagements (SSAE),“Reporting on Controls at a Service Organization”. This audit will include (a) an evaluation that tests and validates Supplier's key controls in relation to the safekeeping of Restricted Information (i.e., a SOC report, or other control assessment that is generally-accepted in the United States financial services industry) at each site, and (b) reasonable Company-specific audit criteria provided by Company in such review. The scope of the audit must include the Services that Supplier provides Company hereunder. Upon Company's request, Supplier will provide Company with a copy of its outside auditors' reports. Supplier will allow Company, its independent third party auditors, its governmental regulators, its customers, its customers' independent third party auditors or its customers' governmental regulators to inspect and audit Supplier's facilities, systems and records relating to Supplier's provision of Services hereunder and compliance with this Appendix H and the Applicable Privacy and Data Security Laws. Supplier will promptly remedy any noncompliance identified during an inspection or audit. If Supplier is unable to promptly remedy such findings, Company may terminate this Agreement at no cost to Company upon written notice to Supplier. At Supplier’s request, Company in its sole discretion may waive one or more annual SSAE 16 audit requirements and perform an audit of Supplier’s operations (or have Company’s third part auditors perform the audit) in accordance with this Section 7 (Security Audits and Reports) at Supplier’s cost.
   2. Company may provide Supplier with a document listing the security and information controls with which they require compliance, to be responded to by Supplier at Supplier’s expense.  The document provided by Company may include requirements for (a) Supplier’s key controls in relation to the safekeeping of Restricted Information at each site, and (b) reasonable Company-specific audit criteria provided by Company within a reasonable period after the commencement of Services.  The scope of the request and associated response includes the Services that Supplier provides Company hereunder.  Upon Company’s request, Supplier will provide Company with reasonable evidence to support statements made in Supplier’s response.  Supplier will allow Company or Company’s representative to audit Supplier’s facilities, systems and records directly relating to Supplier’s provisions of Services hereunder and compliance with this Appendix H and Applicable Law, with Company and Supplier each responsible for expenses incurred by their personnel in the fulfillment of this action.  Supplier will promptly remedy any noncompliance identified during an inspection or audit or provide an appropriate mitigation or compensating control, subject to mutual agreement by Company and Supplier. If Supplier is unable to promptly remedy such noncompliance or provide such mutually agreed upon mitigating or compensating control, Company may terminate this Agreement at no cost upon written notice to Supplier.
   3. Supplier will notify Company any time an independent auditing firm is contracted by Supplier to provide independent evaluation of Supplier’s key controls in relation to (a) the safekeeping of Restricted Information or (b) reasonable Company-specific audit criteria previously provided by Company, for facilities within the scope of this project and where Restricted Information provided by Company could reasonably be within the scope of such an audit.  Upon Company’s request, Supplier will provide a technical presentation detailing the audit tests which evaluated Supplier controls relating to the safekeeping of Restricted Information and will specifically address any deficiencies identified in sufficient detail to support assessment of risk.  Upon Company’s request, Supplier will provide a document identifying the Supplier controls related to the protection of Restricted Information that were evaluated by the independent auditing firm along with any findings by the independent auditing firm relevant to the protection of Restricted Information in sufficient detail as to support assessment of risk.  This document must be verified as accurate and representative of the audit by the independent audit firm contracted and will be accompanied by a statement attesting to such accuracy, provided by the independent audit firm.
2. **Recovery of confidential Information.**

If any Confidential Information is lost or damaged due to Supplier’s failure to comply with the provisions of this Appendix H, or Supplier’s negligence or willful misconduct, Supplier will use commercially reasonable efforts to assist Company in replacing or regenerating such lost or damaged data without additional charge or expense to Company. In addition to any other remedies available to Company hereunder, Supplier will be responsible for any regulatory and statutory fines or penalties imposed upon Company as a result of such loss or damage, which the parties agree will be direct damages.

1. **Disposition of Information and Materials.**

Upon Company’s request at any point during the term of this Agreement, but in any event, within fifteen (15) Business days of expiration or termination of this Agreement, Supplier will return to Company (or erase or destroy as described below) all Restricted Information (or components thereof identified to Supplier by Company) and all copies, derivatives, and summaries of the same, pertaining to this Agreement to which Supplier gained access or use during the term of this Agreement. Supplier will comply with Company’s request without regard to any disputes then existing between the parties. Alternatively, with Company’s prior written consent, Supplier may erase or destroy such Restricted Information in accordance with Applicable Laws using means to protect against unauthorized access to or use of the information, and to assure that such information may not be recoverable following its disposal. In any case an officer of the Supplier will certify in writing to Company that all such Restricted Information has been so returned, erased, or destroyed.

1. **retention, data requests, and location.**

10.1 Supplier will comply with Company’s data retention requirements and supply a data dictionary to Company upon Company’s request.

10.2 Supplier understands that Company may be subject to data requests and audits by various regulatory agencies that may require Company to produce, in as little as two hours, Company data or Confidential Information that meets the data or audit request criteria, and Supplier will provide the facilities and other resources needed for Company to access and timely produce such Company data and Confidential Information at no additional cost. Notwithstanding any other provision of this Agreement, Supplier will make all Company data and Confidential Information (complete and unaltered) immediately available at any time to Company, in a format requested by Company, at no additional charge. Supplier will provide, at no additional charge, access and means for Company to identify, delete, preserve, collect and produce Company data and Confidential Information for Company’s record retention, regulatory, business, or legal purposes, as applicable.

10.3 Supplier may not store Company data or Confidential Information outside of the United States, and Supplier must at all times know the location of the Company data and Confidential Information and immediately disclose that location to Company upon request.

(END OF APPENDIX H)

(END TO APS ADDENDUM TO SUPPLIER’S HOSTING OR SOFTWARE AS A SERVICE AGREEMENT)