Appendix I
Cybersecurity Requirements

1. This **Exhibit** forms an integral part of the Agreement for the [Project Name] BESS ("Project") between Syrcuit Energy Solutions (the "Buyer" or "Owner") and [Contractor Name] (the "Contractor").

2. **Definitions**. Capitalized terms used herein shall have the meanings set forth in this Section 1. Terms that are capitalized but not otherwise defined in this **Exhibit** shall have the meaning set forth in the Agreement.

"Applicable Privacy Laws" means the relevant data protection and privacy laws to which the parties are subject to and any Applicable Laws, subordinate legislation, regulations, and other legal requirements relating to (a) data protection and data security; (b) the Processing of any Buyer Data, in each case as modified, amended, or replaced from time to time, and (c) Applicable Information Security Standards.

"Applicable Information Security Standards" means industry best practices or frameworks to secure information, computer systems, network, and devices using a defense-in-depth approach, such as and including, but not limited to, ISO/IEC 27001 – Information Security Management Systems – Requirements and ISO/IEC 27002 – Code of Practice for International Security Management, ISO/IEC 27017 – Information Technology-Security Techniques – Code of Practice for Information Security Controls Based on ISO/IEC 27002 for Cloud Services, ISO/IEC 27018 – Information Technology – Security Techniques-Code of Practice for Protection of Personally Identifiable Information (PII) in Public Clouds Acting as PII Processors, the Control Objectives for Information and related Technology (COBIT) standards, the National Institute of Standards and Technology (NIST) Cybersecurity Framework including the NIST SP 800-53 – Security and Privacy Controls for Information Systems and Organizations, the Trust Service Principles and Controls of SOC 2 Type 2 Certification (covering security and availability), and the CIS Critical Security Controls, as best industry practices and frameworks may evolve over time.

"Authorized Employees" means Contractor's employees who have a need to know or otherwise access Buyer Data to enable Contractor to perform its obligations under the Agreement.

"Authorized Persons" means (a) Authorized Employees; and (b) Contractor's agents, contractors, subcontractors, subservice organizations, and service providers, who have a need to know or otherwise access Buyer Data to enable Contractor to perform its obligations under the Agreement, whose security has been reasonably investigated to verify that such security is reasonable and consistent with Contractor's obligations under this **Exhibit**, and who are bound in writing by confidentiality and other obligations sufficient to protect Buyer Data in accordance with the terms and conditions of this **Exhibit**.

"**Metadata**" means data about data, or a set of data that describes and gives information about other data, or all of the contextual, processing, and use information needed to identify and certify the authenticity, integrity, and scope of active or archival electronic information or records, such as file dates (e.g., creation date, date of last data access, date of last data modification, and date of last metadata modification), file format or file type, file location (e.g., directory structure or pathname), file name, file permissions (e.g., who can read the data, who can write to it, and who can run it), and file size.

"**Process**", "**Processes**", "**Processing**" mean any operation or set of operations which is performed upon Buyer Data whether or not by automatic means, such as access, adaptation,

alteration, creation, collection, disclosure, disposal, dissemination or otherwise making available, erasure, processing, receipt, recording, retrieval, storage, structuring, transmission, or use.

"**Buyer Data**" means any information disclosed to, shared with or to which access is provided to Contractor by or at the direction of Buyer in the course of Contractor's performance under the Agreement, including Confidential Information and Customer Information.

"**Buyer Systems**" means any computer, computer application, computer network, equipment, mobile computing device, imaging device, server, software, or storage device controlled, leased, or owned by Buyer or operated by a third-party on behalf of Buyer that Processes Buyer Data in connection with this Agreement, or is connected to or otherwise interacts with Contractor Systems.

"**Security**" means Contractor's administrative, physical, procedural, and technical safeguards and controls, including without limitation, policies, procedures, guidelines, practices, standards, controls, hardware, software, firmware and physical security measures, the function or purpose of which is, in whole or part, to: (a) protect the confidentiality, integrity or availability of Buyer Data, (b) protect the availability of Buyer and Contractor Systems; (c) prevent the unauthorized use of or unauthorized access to Buyer Data, Buyer Systems, and Contractor Systems ; and (d) prevent a Security Breach or malicious infection of Buyer Data, Buyer Systems, and Contractor Systems.

"**Security Breach**" means any actual or reasonably suspected: (a) unauthorized use of, or unauthorized access to, Buyer Data, Buyer Systems, or Contractor Systems; (b) inability to access Buyer Data, Buyer Systems or Contractor Systems due to a malicious use, attack or exploit of such Buyer Data, Buyer Systems, or Contractor Systems; (c) unauthorized access to, disclosure of, theft of or loss of Buyer Data, Buyer Systems, or Contractor Systems; or (d) any act or omission that compromises either the Security of Buyer Data or Contractor Systems, or the administrative, physical, procedural, technical, administrative, or organizational safeguards and controls put in place by Contractor (or any Authorized Persons), or by Buyer should Contractor have access to Buyer's Systems, that relate to the security, confidentiality, or integrity of Buyer Data.

"**Contractor Systems**" means any computer, computer application, computer network, equipment, mobile computing device, imaging device, server, software, or storage device controlled, leased, or owned by Contractor or operated by a third-party on behalf of Contractor that Processes Buyer Data, is used to perform the Work and any related services under the Agreement, or is connected to any Buyer Systems.

"**U.S. Persons**" has the meaning set forth in 22 CFR §120.15.

3. Contractor Representations, Warranties, and Covenants.

3.1. Buyer Data**.** Contractor acknowledges and agrees that, in the course of its engagement by Buyer, Contractor may create, receive, or have access to Buyer Data. Contractor shall comply with the terms and conditions set forth in this **Exhibit** in connection with its Processing of such Buyer Data and be responsible for any unauthorized Processing of Buyer Data under its control or in its possession. Contractor shall be responsible for, and remain liable to, Buyer for the actions and omissions of all Authorized Persons concerning the treatment of Buyer Data as if they were Contractor's own actions and omissions. Buyer Data is deemed to be Confidential Information of Buyer and is not Confidential Information of Contractor.

3.2. Covenants. In recognition of the foregoing, Contractor agrees and covenants that it shall:

(a) keep and maintain all Buyer Data in strict confidence, using such degree of care as is appropriate to avoid unauthorized Processing;

(b) not Process Buyer Data in violation of law;

(c) Process Buyer Data solely and exclusively for the purposes for which the Buyer Data, or access to it, is provided pursuant to the terms and conditions of this **Exhibit** and the Agreement, and not disclose, distribute, rent, sell, share, transfer, use, or otherwise make available Buyer Data for Contractor's own purposes or for the benefit of anyone other than Buyer, in each case, without Buyer's prior written consent;

(d) not, directly or indirectly, disclose Buyer Data to any person other than its Authorized Persons who are U.S. Persons, without Buyer's prior written consent unless and to the extent required by government authorities or as otherwise, to the extent expressly required, by applicable law, in which case, Contractor shall (i) use best efforts and to the extent permitted by applicable law notify Buyer before such disclosure or as soon thereafter as reasonably possible; (ii) be responsible for and remain liable to Buyer for the actions and omissions of such Authorized Persons concerning the treatment of such Buyer Data as if they were Contractor's own actions and omissions; and (iii) require the Authorized Persons who has access to Buyer Data to execute a written agreement agreeing to comply with the terms and conditions of this **Exhibit** relating to the treatment of Buyer Data; and

(e) be responsible for the Security of the Contractor Systems and any Buyer Data on the Contractor Systems.

3.3. Data Ownership and use Limitations. As between Contractor and Buyer, Buyer is the owner of any and all Buyer Data, including Buyer Data provided by Buyer's clients, customers, or users, if applicable, and Contractor shall have no ownership rights or interest in the Buyer Data.

3.4. Vendor Assessment. Contractor shall also provide proof of third-party penetration testing results for their product and/or environments, and proof of Cybersecurity Insurance (e.g., Certificate of Insurance)

3.5. Legal and Compliance. Contractor shall provide terms of service which can be assessed for possible risks. Contractor's service agreement shall include non-disclosure clauses for data stored on their platform and comply with relevant legal standards and licensing requirements for intellectual property (IP) usage. Contractor shall provide clear liability and indemnity clauses to protect against data breaches or service failures. Contractor shall ensure compliance with local data residency laws for cross-border data transfers and provide Service Level Agreements (SLAs) defining availability.

4. Information Security.

4.1. Compliance with Laws**.** Contractor represents and warrants to Buyer that its Processing of Buyer Data does and will comply with all Applicable Privacy Laws, as well as all other applicable regulations and directives.

4.2. Written Information Security Program. Contractor shall implement and maintain a comprehensive written information security program, which is reviewed at least annually, that: (a) contains administrative, physical, procedural, and technical controls to provide for the availability, confidentiality, integrity, and security of Buyer Data, Buyer Systems, and Contractor Systems; (b) protect against hazards or threats and unauthorized access or use of Buyer Data, Buyer Systems,

and Contractor Systems; (c) controls identified risks; (d) addresses access, retention, and transport of Buyer Data, and (e) provides for disciplinary action in the event of its violation.

4.3. Safeguards and Controls. Without limiting Contractor's obligations under Section 3.1, Contractor shall implement and maintain administrative, physical, procedural, and technical safeguards and controls to protect Buyer Data, Buyer Systems, and Contractor Systems from unauthorized access, accidental loss, acquisition, alteration, damage, destruction, disclosure, or misuse that are no less rigorous than the highest Applicable Information Security Standards, and shall ensure that all such safeguards and controls, including the manner in which Buyer Data is created, collected, accessed, received, used, stored, processed, disposed of, and disclosed, comply with Applicable Privacy Laws, as well as the terms and conditions of this **Exhibit**.

4.4. Minimum Safeguards and Controls. The Security that Contractor is required to employ and maintain pursuant to this **Exhibit** shall include, at a minimum, the safeguards and controls listed in Attachment 1, attached hereto, and incorporated herein by reference.

4.5. Critical Infrastructure Protection. Contractor shall submit documentation describing the approach, methodology and design to provide physical and cyber security with its submittal of the Technical Specifications which shall be at least [sixty (60) days] prior to the provision of the Services. The Equipment and the BESS shall be designed with the criteria to meet applicable industry standards and guidelines (at the time of this writing, NERC CIP, or any future standard adopted by the industry in its place that is applicable to the Project) compliance requirements and identify areas that are not consistent with the applicable NERC CIP guidelines and requirements. The cyber-security documentation shall include a block diagram of the control system with all external connections clearly described. Contractor shall provide such additional information as Buyer may reasonably request as part of a security posture assessment.

4.6. Data Security and Privacy. Contractor shall ensure data is encrypted at rest (e.g., AES-256) and in transit (e.g., TLS 1.2 or higher). Contractor shall implement a Robust Security Framework (e.g. Zero Trust Architecture) to secure access to customer data in their systems and provide mechanisms to audit and track how data is used within their infrastructure.

5. Authorized Persons and Employees.

5.1. Authorized Employees. During the term of each Authorized Employee's employment by Contractor, Contractor shall at all times cause such Authorized Employees to abide strictly by Contractor's obligations under this **Exhibit** and Contractor's standard policies and procedures, a copy of which have been provided to Buyer. Contractor further agrees that it shall maintain a disciplinary process to address any unauthorized Processing of Buyer Data by any of Contractor's Authorized Persons. Contractor also agrees to prevent terminated Authorized Persons from Processing Buyer Data, Buyer Systems, and Contractor Systems by promptly terminating their physical and electronic access to such Buyer Data, Buyer Systems, and Contractor Systems.

5.2. Security Liaison. Contractor shall assign an individual working for Contractor that shall act as the security liaison between Buyer and Contractor, oversee compliance with this **Exhibit**, receive notice of Security Breaches within Contractor's organization, coordinate Security Breach incident response and remedial action, and provide notice, reporting, and work within Contractor to undertake other actions and duties as set forth in the Agreement. Contractor shall ensure that such individual is sufficiently experienced, qualified, and trained to be able to fulfill the functions set out in this subsection and any other functions that might reasonably be expected to be carried out by the individual as a security coordinator.

Contractor Security Liaison	[NAME]	[CONTACT INFORMATION]

5.3. Use of Third Parties. Contractor shall not provide any sub-contractor, vendor, or other third party with access to Buyer Data, Buyer Systems, or Contractor Systems unless it has received prior written consent from Buyer, or such access is specifically allowed under the Agreement. In all events, prior to providing any sub- contractor, vendor, or other third party with such access, Contractor shall: (a) conduct investigation of such third party to confirm they are capable of providing the Work and related services pursuant to the terms of this **Exhibit** (and provide Buyer, upon demand, with full documentation of this investigation); (b) conduct a reasonable investigation of such third party's information security to verify that such security is reasonable and consistent with Contractor's obligations under this **Exhibit**; (c) contractually impose upon such third party the contractual duties at least as restrictive as those contained herein as such obligations may be applicable to the services they provide; and (d) contractually secure rights with respect to such third party that enable Contractor's compliance with this **Exhibit**. In all events, Contractor is and shall remain fully responsible for any act, errors, or omission of any third party retained by Contractor with respect to this **Exhibit**.

5.4. U.S. Persons and Location. All obligations under this **Exhibit**, including Processing of the Buyer Data, and access to Buyer System and Contractor System by Contractor and its Authorized Persons, shall be performed solely by U.S. Persons. All Contractor Systems used to perform the Work and related services under the Agreement, including any data hosting, data center, and disaster recovery facilities and systems, shall be located in the USA. Contractor and Authorized Persons with access to Buyer Data shall access, store, process and transmit Buyer Data only on computers located in the USA, unless Contractor has received Buyer's prior written consent. In the event Contractor discovers or reasonably believes that any Buyer Data has been or is being accessed, created, collected, disclosed, disposed, processed**,** received, stored**,** transmitted, or used in any other country other than the USA, or by any individuals who are not U.S. Persons, Contractor shall provide prompt notice to Buyer, and in all events shall provide such notice within 48 hours of such discovery.

6. Security Breach Procedures.

6.1. Security Breach. In the event of a Security Breach, Contractor shall, with full disclosure to the Buyer:

(a) promptly conduct a reasonable investigation of the reasons for and circumstances of such Security Breach;

(b) take all reasonably necessary actions to prevent, contain, and mitigate the impact of such Security Breach, and remediate such Security Breach;

(c) provide notice to Buyer to the designated notice addresses in Section 17.4 of the Agreement and by [telephone at the following number: [TELEPHONE NUMBER]/emailing Customer at [EMAIL ADDRESSES]], with a copy by email to Contractor's primary business contact within Buyer immediately and in any event within 24 hours after Contractor discovers such Security Breach;

(d) promptly, and in no event more than two business days after Contractor confirms a Security Breach, provide a written report to Buyer providing all relevant details concerning such Security Breach;

(e) collect and preserve all evidence concerning the discovery, cause, vulnerability, remedial actions and impact related to such Security Breach, which shall meet reasonable expectations of forensic admissibility; and

(f) document the incident response and remedial actions taken in detail, which shall meet reasonable expectations of forensic admissibility.

6.2. Security Breach Notice. Contractor shall not inform any third party of any Security Breach without first obtaining Buyer's prior written consent, other than to inform a complainant that the matter has been forwarded to Buyer's legal counsel. Further, Contractor agrees that Buyer shall have the sole right to determine: (a) whether notice of the Security Breach is to be provided to any individuals, regulators, law enforcement agencies, consumer reporting agencies, or others as required by law or regulation, or otherwise in Buyer's discretion; and (b) the contents of such notice, whether any type of remediation may be offered to affected persons, and the nature and extent of any such remediation. Contractor hereby authorizes Buyer, in Buyer's sole and absolute discretion, to provide notice of, and reasonably required information and documents concerning, any Security Breach, to third parties, including without limitations individuals or entities that may have been impacted by the breach.

6.3. Security Breach Written Report**.** Upon request by Buyer, Contractor shall promptly provide Buyer with a written report containing information reasonably requested by Buyer relating to any Security Breach. In addition, Contractor shall provide Buyer with summaries of the relevant portions of any security assessment and security control audit reports.

6.4. Cooperation and Reimbursement. Contractor agrees to reasonably cooperate at its own expense with Buyer in any litigation, investigation, or other action deemed necessary by Buyer to protect its rights relating to the access, creation, collection, disclosure, disposal, maintenance, process**,** protection**,** receipt, storage**,** transmission, or use of Buyer Data. Contractor shall reimburse Buyer for all actual reasonable costs incurred by Buyer in responding to, and mitigating damages caused by, any Security Breach, including all costs of notice and/or remediation pursuant to this Section.

7. Oversight of Security Compliance.

7.1. Information Maintenance. Contractor shall collect and record information, and maintain audit trails, logs, planning documents, records, and reports, concerning its Security, its compliance with this **Exhibit**, Applicable Privacy Laws, and Security Breaches, and its Processing of Buyer Data, and the Processing of the Buyer Data on Contractor's Systems.

7.2. Complete and Truthful Statements. Contractor represents, warrants, and covenants that the information provided in response to Buyer’s security assessment questionnaire, software security assessment, and any other information provided with respect to the Security of Contractor Systems is complete, truthful, and accurate.

7.3. Written Information Security Questionnaire. Upon Buyer's request, at no charge to Buyer, to confirm compliance with this **Exhibit**, as well as Applicable Privacy Laws and Applicable

Information Security Standards, Contractor shall accurately, completely, promptly, and truthfully complete a written information security questionnaire provided by Buyer, or a third party on Buyer's behalf, regarding Contractor's business practices and information technology environment in relation to all Buyer Data being handled and/or services being provided by Contractor to Buyer pursuant to the Agreement. Contractor shall fully cooperate with such inquiries. Buyer shall treat the information provided by Contractor in the security questionnaire as Contractor's Confidential Information.

7.4. Review of Security Controls. Upon Buyer's request, at no charge to Buyer, to confirm Contractor's compliance with this Exhibit, as well as any Applicable Privacy Laws, Contractor grants Buyer or, upon Buyer's election, a third party on Buyer's behalf, permission to perform an assessment, audit, examination, or review of all controls and safeguards in Contractor's physical and/or technical environment in relation to all Buyer Data being handled and/or services being provided to Buyer pursuant to the Agreement. Contractor shall fully cooperate with such assessment by providing access to knowledgeable personnel, physical premises, documentation, infrastructure, and application software that accesses, creates, collects, discloses, disposes, processes, receives, stores, transmits, or uses Buyer Data for Buyer pursuant to the Agreement. In addition, Contractor shall provide Buyer with the results of any audit by or on behalf of Contractor that assesses the effectiveness of Contractor's information security program as relevant to the security and confidentiality of Buyer Data shared during the course of the Agreement. Buyer shall treat such audit reports as Contractor's Confidential Information under this **Exhibit**.

7.5. Network Diagram. Upon Buyer's request, Contractor shall provide Buyer with a network diagram that outlines Contractor's information technology network infrastructure and all equipment used in relation to fulfilling its obligations under the Agreement, including, without limitation: (a) connectivity to Buyer and all third parties who may access Contractor's network to the extent the network contains Buyer Data; (b) all network connections, including remote access services and wireless connectivity; (c) all access control measures, access-list-controlled routers, firewall protection (for example, firewalls, packet filters, intrusion detection and prevention services), secure access control methods, secure authentication protocols, and secure access control methods; (d) all backup or redundant servers; and (e) permitted access through each network connection.

7.6. Audits. At least once per year, at no charge to Buyer, Contractor shall conduct site audits of the information technology and information security controls for all Contractor Systems used to perform the Work and related services under the Agreement, including, but not limited to, obtaining a network-level vulnerability assessment performed by a recognized third-party audit firm based on recognized industry best practices.

7.7. SOC 2 Audit. At no charge to Buyer, Contractor shall, at least once each calendar year at no greater than a twelve month interval from the previous audit (such interval, the "**Audit Period**"), obtain a SOC 2 Type 2 audit, report, attestation, and opinion (or a mutually-agreed equivalent audit, report, attestation, and opinion) issued under SSAE 18 (or any successor audit standard promulgated by the AICPA) from an independent, certified public accounting firm of good reputation that evaluates the design and operating effectiveness of controls over Contractor Systems (including infrastructure, software, people, procedures, and data) through or from which the Work and related services are provided, including those of all of Contractor's Authorized Persons, Subcontractors and subservice organizations throughout the entirety of the Audit Period and relating to all Trust Services Principles and Criteria (as defined by the AICPA) (a "**SOC 2**

Audit"). Contractor shall provide any and all reports from the SOC 2 Audit to Buyer within one week of Contractor's receipt thereof. Without limiting the foregoing, each audit report must include a description of any changes made to Contractor Systems during the Audit Period, including any changes in the Authorized Persons, Subcontractors, and subservice organizations used by Contractor, as well as assessments and attestations from Contractor, its Subcontractors, and any subservice organizations with respect to the effectiveness of the controls prior to and after the implementation of any such change.

7.8. Deficiency. If following any audit or security assessment performed by Contractor: (a) the auditor fails to provide attestation with respect to one or more criteria, or (b) Contractor at any time discovers a weakness or deficiency in Contractor's controls (any of the foregoing, a "**Deficiency**"), then Contractor shall notify Buyer and meet with Buyer upon Buyer's request to discuss with Buyer the nature and extent of the Deficiency, and Contractor shall (i) promptly develop a remediation plan with respect to each Deficiency (which shall include deadlines for the completion of the tasks/activities under such remediation plan and such deadlines shall be mutually agreed upon with Buyer), (ii) diligently implement the remediation plan and shall use commercially reasonable efforts to remediate any Deficiencies, and (iii) promptly report to Buyer on the status of remediation efforts as requested by Buyer.

8. Information Management.

8.1. Collection and Preservation of Information. In accordance with Buyer's instructions and requests, and in Buyer's sole discretion Contractor shall collect and preserve any information related to the Agreement (including Buyer Data and Metadata) in the care, custody, or control of Contractor (or a third party on Contractor's behalf), including collection and preservation of information in accordance with any retention schedules and retention obligations that exist as a result of pending or threatened litigation or other legal action. Upon Buyer's request, Contractor shall provide such preserved information in a format requested by Buyer.

8.2. Return or Destruction of Buyer Data. At any time during the term of the Agreement at Buyer's request, or upon the termination or expiration of the Agreement for any reason, Contractor shall, and shall instruct all Authorized Persons to, promptly return to Buyer all copies, whether in written, electronic, or other form or media, of Buyer Data in its possession or the possession of such Authorized Persons, or securely dispose of all such copies such that is rendered indecipherable (including degaussing, deleting, permanently erasing, and shredding, as applicable), unreconstructable, unreadable, and unusable, and certify in writing to Buyer that such Buyer Data has been returned to Buyer or disposed of securely. Contractor shall comply with all directions provided by Buyer with respect to the return or disposal of Buyer Data.

8.3. Authentication. In the event that Buyer is required to authenticate any of the information described in this Section 7, Contractor shall cooperate with Buyer in providing any requested assistance with such authentication, including without limitation testifying (by affidavit, declaration, deposition, in court, or otherwise) as a custodian of records to authenticate the information, establish chain of custody, and/or provide any other requested information and/or assistance.

9. Equitable Relief. Contractor acknowledges that any breach of its covenants or obligations set forth in this Exhibit or Contractor's standard policies and procedures, a copy of which have been provided to Buyer, may cause Buyer irreparable harm for which monetary damages would not be adequate compensation and agrees that, in the event of such breach or threatened breach, Buyer is entitled to seek equitable relief, including a restraining order, injunctive relief, specific

performance, and any other relief that may be available from any court, in addition to any other remedy to which Buyer may be entitled at law or in equity. Such remedies shall not be deemed to be exclusive but shall be in addition to all other remedies available at law or in equity.

10. Material Breach. Contractor's failure to comply with any of the provisions of this Exhibit is a material breach of the Agreement. In such event, Buyer may terminate the Agreement effective immediately upon written notice to the Contractor without further liability or obligation to Contractor.

11. Indemnification. Contractor shall defend, indemnify, and hold harmless Buyer and its affiliates, subsidiaries, and their respective agents, directors, employees, officers, owners, partners, permitted assigns, and successors (each, a "**Buyer Indemnitee**") from and against all actions, awards, costs, damages, deficiencies, expenses , fines, interest, judgments, liabilities, losses, or penalties, of whatever kind, including reasonable attorneys' fees, the cost of enforcing any right to indemnification hereunder, and the cost of pursuing any insurance providers, arising out of or resulting from any claim against any Buyer Indemnitee arising out of or resulting from Contractor's failure to comply with any of its obligations under this **Exhibit**.

12. Miscellaneous.

12.1. Cooperation and Coordination. Contractor agrees to reasonably cooperate and coordinate with Buyer concerning: (a) Buyer's document preparation, enforcement, investigation, monitoring, and notification requirements and reporting concerning Security Breaches and Contractor's and Buyer's compliance with Applicable Privacy Laws; and (b) any other activities or duties set forth under this **Exhibit** for which cooperation between Buyer and Contractor may be reasonably required.

12.2. Contractor's Expense. Contractor's compliance with this **Exhibit**, and any actions required of Contractor herein, shall be at Contractor's sole and exclusive expense and shall be included as part of the price of the Work and related services provided by Contractor and for no additional fee to Buyer, including any Buyer requests authorized herein.

12.3. Survival. Contractor's obligations and Buyer's rights in this **Exhibit** shall continue as long as Contractor, or a third party for or on Contractor's behalf, Processes Buyer Data, including after expiration or termination of the Agreement.

12.4. Precedence. In the event of a conflict between this **Exhibit** and any terms set forth in the Agreement with respect to the subject matter described herein, this **Exhibit** will control.

ATTACHMENT 1
MINIMUM SAFEGUARDS AND CONTROLS

General Security	(1) Secure business facilities, data centers, paper files, servers, backup systems, and computing equipment, including, but not limited to, all mobile devices and other equipment with information storage capability; (2) implement network, application, database, and platform security; and (3) secure information transmission, storage, and disposal.
Access controls	(1) Physical access controls, secure user authentication protocols, secure access control methods, and firewall protection; and (2) preventing terminated Authorized Persons from accessing Buyer Data, Buyer Systems, and Contractor Systems by promptly terminating their physical and electronic access to such Buyer Data.
Access controls — Secure User Authentication	With respect to Buyer Data and Contractor Systems: (1) maintain secure control over user IDs, passwords and other authentication identifiers; (2) maintain a secure method for selecting and assigning passwords and using authentication technologies such as token devices; (3) restrict access to only active users/ accounts; (4) block user access after multiple unsuccessful attempts to login or otherwise gain access; (5) assign unique user identifications plus passwords, which are not vendor supplied default passwords; and (6) require personnel to change passwords at regular intervals or based on the number of accesses (passwords for privileged accounts should be changed more frequently than normal passwords), whenever there is any indication of possible system or password compromise, and avoid re-using or cycling old passwords.
Risk Assessment and Mitigation	Periodic and regular information security risk assessment and monitoring of Contractor's information security program, Security and Contractor System, at least annually and whenever there is a material change in Contractor's business or technology practices that may impact the availability , confidentiality, integrity , or security of Buyer Data, including: (1) identifying and assessing reasonably foreseeable internal and external threats and risks to the availability, confidentiality, integrity, and security of Buyer Data; (2) assessing the likelihood of, and potential damage that can be caused by, identified threats and risks; (3) regularly evaluating, monitoring, and testing the sufficiency and effectiveness of Security and Security Breach response actions, and documenting same; (4) assessing adequacy of Authorized Persons training concerning, and compliance with, Contractor's information security program; (5) designing, implementing, adjusting and upgrading Security in order to limit identified threats and risks, and address material changes in technology, business and sensitivity of Buyer Data; and (6) assessing whether such information security program is operating in a manner reasonably calculated to prevent unauthorized access or use of Buyer Data; and (6) detecting,

	preventing and responding to attacks, intrusions and other system failures. Risk assessments should be conducted by independent third parties or Authorized Persons independent of those that develop or maintain Contractor's security program.
Intrusion detection and response policies and procedures	Maintain policies and procedures for detecting, monitoring and responding to actual or reasonably suspected intrusions and Security Breaches, and encouraging reporting actual or reasonably suspected Security Breaches, including: (1) training Authorized Persons with access to Buyer Data to recognize actual or potential Security Breaches and to escalate and notify the senior management of the foregoing; (2) mandatory post-incident review of events and actions taken concerning security of Buyer Data, and; (3) policies concerning reporting to regulators and law enforcement agencies.
Off-Premises Security Policies	Policies concerning Security for the Processing of records and media containing Buyer Data outside of business premises.
Vendor Management and Oversight	(1) Use reasonable steps and due diligence to select and retain third party Contractors that are capable of maintaining security consistent with the Exhibit and complying with applicable legal requirements; (2) contractually requiring such Contractors to maintain such security; and (3) regularly assessing and monitoring third party Contractors to confirm their compliance with the applicable security required in the Exhibit and by Applicable Privacy Laws.
Physical Security	(1) Reasonable restrictions on physical access to Buyer Data and Contractor System; and (2) physical protection against damage from civil unrest, earthquake, explosion, fire, flood, and other forms of natural or man-made disaster should be designed and applied.
Minimum necessary access and use	(1) Identify those Authorized Persons or classes of Authorized Persons who must Process the Buyer Data, or access and use the Buyer System, Buyer’s premises, or Contractor System to fulfill Contractor's obligations under the Agreement, and grant applicable rights to Buyer Data, Buyer System, Buyer’s premises, and/or Contractor System only to those Authorized Persons; (2) monitor such Processing by those Authorized Persons; and (3) maintain a list of those Authorized Persons, the access given to each Authorized Persons, and the purpose for such access. This list must be provided to the Buyer at any time upon request.
Encryption of Buyer Data	Strong encryption of Buyer Data: (1) stored on any media; (2) while transmitted by Contractor across any public network (such as the Internet) or wirelessly; (3) while in transit outside of Contractor System; (4) stored on a data storage device outside of Contractor's physical controls; and (5) stored on Contractor System.
Firewalls	Up-to-date firewalls between Contractor System, the Internet (including internal networks connected to the Internet) and other public networks,

	and internal networks operated by Contractor that are not necessary for providing the Work and related services to Buyer, which are reasonably designed to maintain the security of Buyer Data and Contractor System.
Malicious Code Software	(1) Implement and maintain software for Contractor System that detects, protects against, removes and remedies software or computer code designed to perform an unauthorized function on, or permit unauthorized access to, an information system, including without limitation, computer viruses, Trojan horses, worms, and time or logic bombs (“Malicious Code Software”); (2) run Malicious Code Software on at least a weekly basis; (3) update Malicious Code Software on at least a daily basis, including without limitation, obtaining and implementing the most currently available virus signatures.
Change Controls	Prior to implementing changes to Contractor System, assess the potential impact of such changes on Security, and determine whether such changes are consistent with existing Security. No changes to the Contractor System or Security should be made which increase the risk of a Security Breach or which would cause a breach of the Exhibit.
Personnel Security	Implement appropriate personnel security and integrity procedures and practices, including, but not limited to, conducting reasonable background checks of any Authorized Persons that will have access to Buyer Data or Buyer's System, including Criminal Record Bureau checks.
Personnel Training and Education	Regular and periodic training of Authorized Persons concerning: (1) Security and (2) implementing Contractor's information security program.
Segregation of Duties and Dual Controls	Duties and areas of responsibility of Authorized Persons should be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of Contractor System or Buyer Data.
Segregation of Buyer Data	Strictly segregating Buyer Data from information of Contractor or its other customers so that Buyer Data is not commingled with any other types of information.
Monitoring and Logging	Contractor shall provide audit trails that log user activities, system changes, and administrative actions on their platform and ensure real-time monitoring of security events.
Vulnerability and Patch Management	Contractor shall have a schedule for regularly patching and updating their systems and subject their infrastructure to regular vulnerability scans and third-party penetration testing.
Backup and Recovery	Contractor shall ensure customer data is backed up and made redundant to prevent data loss and provide an export feature that allows customers to migrate their data in a compatible format for other systems.

Service Management	Contractor shall notify customers in advance of significant changes to the service, provide advance notice for scheduled maintenance, and communicate promptly in the event of emergency maintenance.
Operational Guidelines and Support	Contractor shall provide operational guidelines, procedures, and contacts to ensure secure handling of data by users and administrators.
Virus and Malware Protection	Contractor shall implement and maintain software that detects, protects against, removes, and remedies malicious code.
Email Security	Contractor shall secure email communications with encryption, SPF, DKIM, and DMARC configurations, detect and prevent email-based threats, monitor outbound email for sensitive data leaks, and train employees on email security.