ATTACHMENT A: CYBERSECURITY REQUIREMENTS

CONFIDENTIALITY, COMPUTER NETWORK USAGE, AUDIT, AND COMPLIANCE

A. Definition: Each party agrees that any Personal Information and Information relating to the other party's business, including but not limited to intellectual property, information security systems that could be used to gain unauthorized access or pose a security threat to a party, customer, employee, retiree, shareholder or supplier information, or technical, financial, administrative and internal activities or any business plans and methods, operating and technical data, reports, drawings, operating documents, project documents, reports, and all non-public information, financial or otherwise, data specific to each party and its business or its customers shall not be disclosed to any unauthorized parties without the other party's consent. "Personal Information" means any information relating to an identified or identifiable individual, including, but not limited to, name; postal address; email address or other online contact information (such as an online user ID); telephone number; date of birth; Social Security number (or its equivalent); driver's license number (or other government-issued identification numbers); account information (including financial account information); payment card data (including primary account number, expiration date, security code, complete magnetic stripe data or equivalent on a chip, or PIN); access code, password, security questions and answers; medical information; health insurance information; biometric data; Internet Protocol (IP) address; or any other unique identifier.

B. Definition Exclusions: Except with respect to "Personal Information," "Confidential Information" shall not include any information that: (i) was already known to the receiving party at the time it was disclosed by the disclosing party; (ii) was available to the public at the time the disclosing party disclosed it; (iii) becomes available to the public after being disclosed by the disclosing party through no wrongful act of, or breach of this Agreement by the receiving party; (iv) is received by the receiving party without restriction as to use, or disclosure from a third party free of any obligations owed to the disclosing party, or (v) is independently developed by the receiving party without benefit of any disclosure of information by the disclosing party.

C. Disclosure Prohibited: Each party agrees that it shall not use (except for the purpose described herein) share, transfer, disclose, publish, or otherwise provide the Confidential Information of the other party to any third party (including affiliates and subcontractors) for any reason unless approved in writing by the disclosing party.

- **a.** With the consent of Mesa, if the Supplier provides third-party access to Mesa Confidential Information; the Supplier shall impose obligations on such third party substantially similar to those imposed on the Supplier by Mesa.
- **b.** The Supplier shall only retain subcontractors that the Supplier reasonably expects to be suitable and capable of performing the delegated obligations per the cybersecurity requirements in this Agreement. The Supplier shall be responsible for and remain liable to Mesa for any third-party compliance with these cybersecurity requirements.

D. Use Restrictions: The receiving party agrees to use Confidential Information solely for the purpose of this Agreement. Confidential Information will only be distributed to the receiving party's employees on a need-to-know basis for the purpose of this Agreement. Such employees receiving Confidential Informaiton shall have previously agreed, either as a condition to employment or in order to obtain Confidential Information, to be bound by terms and conditions substantially similar to but no less restrictive than the confidentiality obligations set forth in this Agreement.. Each party shall (i) provide training, as appropriate, regarding the privacy, confidentiality, and information security requirements outlined in this Agreement and (ii) exercise the necessary and appropriate supervision over its relevant employees to maintain the appropriate privacy, confidentiality, and security of Confidential Information. Each party shall be responsible for and remain liable to the other party for its employees' compliance with this Agreement.

E. Degree of Care: Each party agrees to protect the other party's Confidential Information with at least the same degree of care used to protect its own confidential information but in no event less than reasonable care.

F. Non-Disclosure Agreements: To the extent the parties have an existing non-disclosure or other confidentiality agreement covering the same subject matter as this Agreement in effect as of this Agreement's effective date; this Agreement shall supersede such agreement unless otherwise agreed by the parties.

G. Court Order: If the receiving party is requested or ordered by a court or governmental entity to disclose any or all of the Confidential Information, the receiving party shall (i) promptly notify the disclosing party of the existence, terms, and circumstances surrounding the request or order; (ii) consult with the disclosing party on the advisability of taking steps to resist or narrow the request or order; (iii) cooperate with the disclosing party in any lawful effort the disclosing party undertakes to obtain any such relief and with any efforts to obtain reliable assurance that confidential treatment will be given to that portion of Confidential Information that is disclosed; and (iv) furnish only that portion of the Confidential Information that it is legally required to furnish, unless the disclosing party expressly authorizes broader disclosure in writing.

H. Storage and Encryption of Mesa Confidential Information and Mesa Personal Information:

a. The Supplier shall not store, access, or maintain any Mesa Confidential Information outside the United States (including its territories and protectorates) or any cloud service or facility without the express prior written consent of Mesa.

b. The Supplier shall encrypt all Mesa electronically stored Mesa Confidential Information in its possession at rest and in transit.

c. The Supplier shall encrypt all Mesa electronically stored Mesa Personal Information data elements listed in the above definitions using the following design elements:

1 The Mesa Personal Information shall be encrypted in all applications where the Mesa Personal Information is initially acquired.

2 The decryption of data elements of the Mesa Personal Information shall only occur in a consuming application, or output, with a Legitimate Business Requirement for native data elements of the Personal Information. (A "Legitimate Business Requirement" is a need that supports or fulfills the provision of a Service under this Agreement.)

3 Access to a fully decrypted data element of the Mesa Personal Information is provided only to individuals/entities with a Legitimate Business Requirement for such access, where such access is authenticated using identity management techniques.

4 Masking output is utilized to provide access to, or display, a portion of decrypted data in the absence of a Legitimate Business Requirement for decrypted access (i.e., mask all but the last four digits of the social security number on reports).

5 Custom application(s) will be developed to accommodate ad hoc database queries returning decrypted results appropriate for the individual's Legitimate Business Requirement.

d. The Supplier shall use encryption algorithms endorsed by NIST (www.nist.gov) to handle and store Mesa Confidential Information and Mesa Personal Information. Such algorithms shall be updated regularly. The Suppliers are not permitted to use proprietary encryption algorithms.

e. The Supplier shall employ encryption/decryption key management such that the keys are managed confidentially.

I. **Return of Mesa Hardware and Removable Media:** Promptly upon the expiration or earlier termination of this Agreement, or such earlier time as Mesa requests in writing, the Supplier will return to Mesa or its designee all hardware and removable media provided by Mesa containing Mesa Confidential Information. Confidential information in such returned hardware and removable media shall not be removed or altered in any way. The hardware and removable media should be physically sealed and returned via a bonded courier or otherwise directed by Mesa if the return of hardware or removable is not reasonably feasible or desirable to Mesa (which decision will be at Mesa's sole discretion). In that case, the Supplier shall dispose of hardware following disposal procedures that are compliant with current NIST Special Publication 800-88 and provide Mesa written certification from one of the Supplier's officers within fifteen (15) calendar days after destruction with information detailing the destruction method used, the date of destruction, and the entity or individual who performed the destruction.

J. **Return of Confidential Information:** Promptly upon the expiration or earlier termination of this Agreement, or such earlier time as requested in writing by the disclosing party, the receiving party shall cease use of all Confindential Information received hereunder and shall return to the disclosing party or its designee, or render unreadable or undecipherable if return is not reasonably feasible or desirable to the discolosing party each and every original and copy in every media of all Confidential Information in the receiving party’s possession, custody or control including all information and materials that contain or are derived from Confidential Information ("Data Return Requirements"), unless the receiving party is required by law to keep copies of such Confidential Information,. To the extent the receiving party is required by law to keep copies of Confidential Information by , the receiving party shall provide the disclosing party with a written, detailed inventory of such information and a citation to the applicable law for each such item, in advance of keeping such copies. Any Confidential Information retained by the receiving party in accordance with this section shall remain subject to the confidentiality provisions of this Agreement. Promptly following any return or alternate action taken to comply with the Data Return Requirements, the receiving party will provide the disclosing party with a written certification from one of the receiving party’s officers certifying that such return or alternate action occurred.

K. **Vendor Network:** Upon request, Mesa may provide the Supplier access to an external network to access the Internet ("Vendor Network") while the Supplier works on-premises at a Mesa facility. The Supplier agrees that any use of the Internet and electronic mail through the Vendor Network will be solely for necessary business purposes.

L. **Internal Network:** Mesa's internal network ("Internal Network") is independent of the Vendor or Supplier's Network. The Supplier agrees that it may access the Internal Network solely to perform the Services. The Internal Network contains Mesa Confidential Information, which the Supplier may be required to access to perform the Services. The Supplier agrees that access to the Internal Network for other purposes, or the use of the Internal Network to access other non-Services-related networks, is strictly forbidden. The Supplier shall be liable for all damages arising or resulting from such unauthorized access. The Supplier further agrees that such activity may result in the discontinuation of all Mesa network access.

M. **Internet Access:** Per Mesa's existing Internet usage policies, the Supplier and its employees shall not access any restricted websites outlined in Mesa's Acceptable Use Policy from either the Vendor Network or the Internal Network; introduce any viruses, worms, Trojan horses, or other bugs or errors in any Mesa network; or forward any chain letters, executable "ready to run" files or other files which may cause damage to Mesa's computer or network systems. Mesa reserves the right to monitor the Supplier's use of the Vendor Network, the Internal Network, the Internet through the Vendor and Internal Networks, and Mesa's information systems for these or other unauthorized or unlawful activities.

N. **Access Termination:** Mesa reserves the right, in its sole discretion, to terminate the Supplier's access to and use of the Vendor Network or Internal Network at any time, for any reason, and without notice to the Supplier.

O. Compliance with Privacy Laws: The Supplier shall comply, and shall require its subcontractors to comply, with (i) all applicable international, federal, state, provincial and local laws, rules, regulations, directives and governmental requirements currently in effect and as they become effective relating in any way to the privacy, confidentiality or security of Confidential Information ("Privacy Laws"); (ii) all applicable industry standards concerning privacy, confidentiality or information security including, without limitation, the ISO/IEC 27001 and ISO/IEC 27002 Standards, the National Institute of Standards and Technology ("NIST") Framework for Improving Critical Infrastructure Cybersecurity and the Payment Card Industry Data Security Standard ("PCI DSS"); and (iii) applicable provisions of Mesa's written requirements currently in effect and as they become effective relating in any way to the privacy, confidentiality or security of Confidential Information, or applicable privacy policies, statements or notices that are provided to the Supplier by Mesa in writing.

P. The Supplier's Security Procedures; The Supplier's Security Program Requirements:

a. In addition to any other privacy, confidentiality, or security requirements set forth herein, the Supplier will maintain a comprehensive data and systems security program ("Security Program") (which encompasses, but is not be limited to, any of the Supplier's goods that contain software (including firmware) ("Software") executed or installed on any device connected to a Mesa information system or network and any of the Supplier's Services that support or maintain such software or connect to a Mesa information system or network). The Security Program shall include but not be limited to reasonable and appropriate technical, organizational, administrative, and physical security measures to (i) ensure the security and confidentiality of and (ii) protect against the destruction, loss, and unauthorized access, acquisition, use, disclosure or alteration of:

(iii) Mesa Confidential and Personal Information,

(iv) Mesa's information systems, and

(v) Mesa's networks.

b. Without limiting the generality of the preceding, the Supplier's Security Program shall, (unless otherwise agreed in advance, in writing) at a minimum: (i) use industry-standard software and hardware data and system security tools generally available on the market and shall not use the Supplier's proprietary technology; (ii) include secure user authentication protocols; secure access control measures; reasonable monitoring of systems on which Confidential Information is maintained; appropriate segregation of Confidential Information from information of the Supplier or its other customers; effective systems for identifying and responding to threats; effective systems for identifying and addressing information security vulnerabilities; and appropriate personnel security and integrity procedures and practices; (iii) use best-practice cybersecurity and coding practices that address issues identified in the then-current Open Web Application Security Project Top 10 and the SysAdmin, Audit, Networking, and Security ("SANS") Top 25 Programming Errors, and SANS top 20 critical controls, and (iv) include a documented and annually tested Business Continuity and Disaster recovery plan with the ability to restore critical data and services

c. The Supplier shall promptly, upon Mesa's request: (i) disclose to Mesa IT Security all backdoors, embedded credentials, and interactive remote management/support capabilities, and (ii) verify that unused features have been disabled. The content and implementation of the Supplier's Security Program shall be fully documented in writing by the Supplier. Upon Mesa's request, the Supplier shall permit Mesa to review such documentation and inspect the Supplier's compliance with the Security Program.

Q. Notification and Coordination of Cyber-Security Compromises, and Disclosure and Remediation of Known Vulnerabilities

Prior to the delivery of Digital Materials or performance of Digital Services, the Supplier will provide notice to Mesa and summary documentation of publicly disclosed Vulnerabilities in Digital Materials or Digital Services. Also, after delivery, the Supplier will provide notice to Mesa and summary documentation of all known Vulnerabilities in the Digital Materials or Digital Services, not previously disclosed, within thirty (30) calendar days after such Vulnerabilities become known to Supplier. Specifically:

a. The Supplier agrees to notify Mesa, per these security requirements hereof, and with a copy to toffei@mesainc.com, as soon as reasonably possible, but in no case later than twenty-four (24) hours, after it becomes aware of any threatened, attempted, or successful breach or loss of, destruction of, unauthorized access to, acquisition of, use of, disclosure of, or other compromises of (i) Mesa Confidential Information (ii) Mesa's information systems, or (iii) Mesa's computer networks (each such event referred to herein as a "Security Event"). The Supplier further agrees to provide notification within twenty-four (24) hours after it becomes aware of any such Security Event that is reasonably likely to have a material adverse effect on the integrity or operation of a Critical Cyber System (as defined below). Such notice shall summarize in reasonable detail the effect on Mesa, if known, of the Security Event, and the corrective action taken or to be taken by the Supplier. Upon the occurrence of a Security Event Supplier shall:

1. Immediately investigate and perform a root cause analysis of the Security Event.

2. Cooperate fully with Mesa and remediate the effects of such Security Event; and

3. Provide Mesa with such assurances as Mesa shall request that such a Security Event is not likely to recur.

b. The content of any filing, communication, notice, press release, or report related to any Security Event must be approved by Mesa before any publication or communication.

c. "Critical Cyber System" means any computer or information network, system, facility, equipment, hardware device, or software which, if misused, degraded, destroyed, or rendered unavailable, would adversely affect the reliable operation of Mesa's bulk electric systems, nuclear facilities or electric distribution system.

d. Upon the occurrence of a Security Event involving (i) Confidential Information in the possession, custody or control of the Supplier or for which the Supplier is otherwise responsible, or (ii) Critical Cyber Systems accessed by or accessible to the Supplier in connection with the Supplier's performance of the Services for or on behalf of Mesa, the Supplier shall reimburse Mesa on demand for all Notification Related Costs (as defined below) incurred by Mesa arising out of or in connection with any such Security Event. "Related Notification Costs" shall include Mesa's internal and external costs associated with investigating, addressing, and responding to the Security Event, including but not limited to: (i) preparation and mailing or other transmissions of notifications or other communications to consumers, employees or others as Mesa deems reasonably appropriate; (ii) establishment of a call center or other communications procedures in response to such Security Event (e.g., customer service FAQs, talking points and training); (iii) public relations and other similar crisis management services; (iv) legal, consulting, forensic expert and accounting fees and expenses associated with Mesa's investigation of and response to such event; and (v) costs for commercially reasonable credit monitoring or identity protection services.

R. Verification of Software Integrity and Authenticity of all Software and Security Patches Provided by the Supplier

To the extent that Supplier supplies software, firmware, or Security Patches to Mesa, Supplier will comply with the following within ninety (90) days of contract execution.

a. Firmware, Software, and Security Patch Integrity and Authenticity

1. The Supplier shall specify how digital delivery for Digital Materials (e.g., firmware, software, and data), including Security Patches, will be validated and monitored to ensure the digital delivery remains specified. If Mesa deems that it is warranted, the Supplier will apply encryption to protect Digital Materials throughout the delivery process.
2. If the Supplier provides software or Security Patches to Mesa, Supplier will publish, provide, or direct Mesa to an available source of a hash in conforming to the Federal Information Processing Standard (FIPS) Security for Cryptographic Modules (FIPS 140-2) or similar standard information on the software and Security Patches to enable Mesa to use the hash value as a checksum to independently verify the integrity of the software and Security Patches and avoid downloading Software or Security Patches infected with a virus or otherwise corrupted.
3. The Supplier will identify or provide Mesa with a method to identify the country (or countries) of origin of the procured material and its components (including software and firmware). The Supplier will identify the countries where the development, manufacturing, maintenance, and service for the material are provided. The Supplier will notify Mesa of changes in the list of countries where Material maintenance or other Services are provided in support of the procured material. This notification will occur 180 days prior to initiating a change in the list of countries.
4. The Supplier will use or arrange for trusted channels to ship Digital materials, including U.S. registered mail.
5. The Supplier will demonstrate a capability for detecting unauthorized access to the digital Materials throughout the delivery process (e.g., tamper-resistant packaging).

b. Security Patch Governance

1. Prior to delivering any Digital Materials and Digital Services to Mesa, the Supplier will provide documentation regarding the Security Patch management and Vulnerability management/mitigation programs and update process (including third-party software and firmware) for such Digital Materials and Digital Services. This documentation will include information regarding: the resources and technical capabilities to sustain this program and process, such as the method or recommendation for how Mesa validates the integrity of a Security Patch; and the approach and capabilities available to remediate newly reported zero-day Vulnerabilities in supplied Digital Materials and Services.
2. Unless otherwise approved by Mesa in writing, the current or supported version of Digital Materials and Digital Services supplied or performed by Supplier will 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.).
3. The Supplier will verify and provide documentation that procured Digital Materials (including third-party hardware, software, firmware, and services) have appropriate updates and Security Patches installed prior to delivery to Mesa.

4. When the Supplier provides third-party software (including open-source software) and firmware to Mesa, the Supplier will provide or arrange for appropriate hardware, software, and firmware updates to remediate newly discovered Vulnerabilities or weaknesses within sixty (60) days. Updates to remediate critical Vulnerabilities will be provided within a shorter period than other updates within thirty (30) days. If these third-party updates cannot be made available by Supplier within these periods, Supplier will provide or arrange for the provision of mitigations, and workarounds to (i) remediate newly discovered Vulnerabilities or weaknesses with third-party software within sixty (60) days and (ii) to remediate critical Vulnerabilities to third party software within thirty (30) days.

S. Viruses, Firmware, and Malware

a. The Supplier will use reasonable efforts to investigate whether computer viruses or malware are present in any software or Security Patches for Digital Materials and Digital Services before installing or using them for the Digital Materials and Digital Services or providing them to the Mesa. To the extent Supplier is supplying third-party Digital Materials or Digital Services to the Mesa, the Supplier will use reasonable efforts to ensure the third-party investigates whether computer viruses or malware are present in any software or Security Patches for Digital Materials and Digital Services before installing or using them for the Digital Materials and Digital Services or providing them to Mesa.

b. The 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 the Supplier is supplying third-party Digital Materials or Digital Services to Mesa, 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.

T. Data Security and Compliance Audits: If the Supplier: (i) provides any Software that is installed on a Mesa computer or network; or (ii) has access to, or stores or processes any Mesa Confidential Information; or (iii) connects its computer systems, software, and applications to any Mesa network, including but not limited to, the Vendor Network or Internal Network, then Mesa shall have the right to monitor the Supplier's compliance with the terms of this Section and perform data security and system integrity audits ("Audits") on any of the Supplier's applicable systems and applications used to provide the Software or Services. The Supplier hereby grants permission to Mesa to perform such Audits.

a. On an annual basis, the Supplier, at the Supplier's expense, shall require auditors to conduct an examination of the controls placed in operation and a test of operating effectiveness, as defined by Statement on Standards for Attestation Engagements No. 18, Reporting on Controls at a Service Organization ("SSAE 18"), of the services performed by the Supplier for or on behalf of Mesa and issue SOC 1 and SOC 2 reports (Type II) thereon (collectively "SOC Reports") for the applicable calendar year. The Supplier shall submit any changes or updates to previous control objectives to Mesa for review prior to conducting the audit. The Supplier shall deliver to Mesa a copy of the SOC Reports within six (6) weeks after conducting the SSAE 18 assessment for the calendar year. The Supplier shall correct any audit control issues, deficiencies, or weaknesses identified in any SOC Reports at no additional cost to Mesa. If the Supplier does not implement specific audit recommendations, then the Supplier should implement such alternative steps reasonably satisfactory to Mesa to minimize or eliminate the risks identified in any such SOC Report.

b. If the Supplier does not cause an SSAE 18 examination of the controls placed in operation and a test of operating effectiveness to be conducted as described in paragraph a. above and deliver the SOC Reports to Mesa, Mesa shall, at its discretion, conduct an audit, or have an audit conducted by a designated representative, at Mesa's expense, at a date and time mutually agreed to by Mesa and the Supplier. Such Audits shall include, but shall not be limited to, physical inspection of facilities and equipment, external scan, process reviews, and reviews of system configurations, including firewall rule sets, and any information or materials in the Supplier's possession, custody, or control, relating in any way to the Supplier's obligations under this Section. Mesa has the right to review copies of the internal scans that have been performed on the Supplier's internal servers connected to the Internal Network.

c. Should the Audits result in the discovery of material, data security, or system integrity risks to Mesa, Mesa shall notify the Supplier of such risks. The Supplier shall respond to Mesa in writing with the Supplier's plan to take reasonable measures to promptly correct, repair, or modify its network or application to eliminate the risk, at no cost to Mesa. The Supplier shall have ten (10) business days to cure such data security or system integrity risks unless Mesa agrees to a more extended period for such cure. If data security or system integrity risk is, in good faith, found by Mesa and such risk cannot be alleviated in the timeframe contemplated by this Section, based on the nature of the risk, Mesa may terminate its network connection to the Supplier immediately with or without notice to the Supplier without cost or liability to Mesa.

d. Upon Mesa's written request, the Supplier shall complete and submit to Mesa an information security due diligence questionnaire provided by Mesa to enable Mesa to determine the Supplier's security posture as part of our Supply Chain Risk Management Program requirements within the timeframe requested by Mesa.

e. To the fullest extent permitted by law, the Supplier hereby waives the right , under any applicable state or federal law, to pursue a cause of action against Mesa based on actions permitted under this Section related cybersecurity.

U. Cybersecurity Insurance Coverage: The Supplier or Supplier shall, at its own expense, procure and maintain in full force at all times during the term of this Agreement, Cyber Insurance covering cyber and network risks. Such insurance shall include, but not be limited to, coverage for (a) liability arising from theft, dissemination, and use of Confidential Information stored or transmitted in electronic form; and (b) liability arising from the introduction of a computer virus into, or otherwise causing damage to, a customer's or third person's computer, computer system, network or similar computer-related property and the data, software, and programs stored thereon. Such insurance will be maintained with limits of no less than $2,000,000 per claim and in the annual aggregate and may be maintained on a stand-alone basis or as cyber insurance coverage provided as part of any professional liability insurance policy. This insurance shall have a retroactive date that equals or precedes the effective date of this Agreement. The Supplier shall maintain such coverage until the later of (i) a minimum period of three (3) years following termination or completion this Agreement, or (ii) until The Supplier or Supplier has returned or destroyed all Confidential Information in its possession, care, custody or control, including any copies maintained for archival or record-keeping processes.

V. Injunctive Relief: The Supplier agrees that any use, disclosure, or handling of Confidential Information in violation of this Agreement or any applicable Privacy Law, or any other violation of this Agreement, including a Security Event, may cause immediate and irreparable harm to Mesa, and Mesa shall be entitled to equitable relief, including an injunction and specific performance, in addition to all other remedies available at law or equity. Therefore, the Supplier agrees that Mesa may obtain specific performance and injunctive or other equitable relief for any such violation, in addition to remedies at law, without proof of actual damages and without the necessity of securing or posting any bond in connection with such remedy.