GE Privacy and Data Protection Policy

Part A: Definitions (The following definitions apply and are in addition to the definitions set forth in Purchaser's Standard Terms and Conditions of Purchase, C64/I64)

GE Data is any information that is provided by or on behalf of Purchaser to Seller or that is Processed by Seller in support of the performance of services under the Agreement. GE Data shall be deemed confidential information under the Agreement.

GE Restricted Data, for purposes of the Agreement, is information that Purchaser identifies as 'restricted data' in an Agreement, statement of work, attachment, schedule, or other similar document under the Agreement, as well as the following categories of information that may be provided by or on behalf of Purchaser to Seller or that is Processed in support of the performance of services under the Agreement:

- details of mergers, acquisitions or dispositions
- financial results prior to public reporting
- security vulnerability information relating to Purchaser systems or products, or systems that support such systems or products
- Sensitive Personal Data, defined as:
    - Medical records and other personal health information
    - Personal bank account and payment card information (including numbers, expiration dates, PINs or other passwords), and other financial account information
    - National identifiers (e.g., passport numbers, social security numbers, drivers' license numbers)
    - Special data categories under data protection law applicable to Purchaser, including racial or ethnic origin, political opinions, religious or philosophic beliefs, trade union membership, criminal records and information concerning health or sex life
- Controlled Data, defined as:
    - sensitive but unclassified government data
    - export controlled data
- Intellectual Property (IP), defined below (or as may be further specified in the Agreement), that would give Purchaser a significant competitive advantage:
    - engineering drawings
    - formulas
    - specifications
    - technical information
    - methods
    - processes
    - software code

Highly Privileged Accounts, or HPAs, are accounts with system level administrative or super-user access to devices, applications or databases, administration of accounts and passwords on a system, or ability to override system or application controls.

Notices are any filings, communications, notices, press releases, or reports related to any Security Incident.

Personal Data is any information to which Purchaser provides Seller access or that Seller Processes on behalf of Purchaser that relates to an identified or identifiable natural person. By way of example, the following information concerning one or more individuals (Data Subjects) is Personal Data: contact information; information concerning online and offline activities and preferences; human resources data; and personal financial and health information. Legal entities are Data Subjects where required by law. Personal Data is GE Data for purposes of the Agreement.

Process, Processing or *Processed* means any operation or set of operations performed upon GE Data or GE Restricted Data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, accessing, consultation, use, disclosure by transmission, dissemination, or otherwise making available, alignment or combination, blocking, erasure, or destruction.

Security Incident is any actual or suspected event in which GE Data or GE Restricted Data is or may have been lost, stolen, improperly altered, improperly destroyed, used for a purpose not permitted under the Agreement, or accessed by any person other than Seller's personnel with a reasonable need to access such information for the purposes specified in the Agreement.

Supplier Information Systems means any Seller systems used to Process GE Data or GE Restricted Data for the performance of services under the Agreement.

Trusted Connection means a physically isolated segment of the Seller network by which the Seller is granted full access to Purchaser's internal network.

Part B: Collecting, Processing and Sharing GE Data

B.1 Seller shall view and Process GE Data only on a need-to-know basis and only to the extent necessary to perform services under the Agreement or as otherwise instructed by Purchaser in writing. Subject to the provisions of paragraph J. 2, if requested during the term of the Agreement, and in any event upon expiration or termination, Seller shall promptly return to Purchaser any GE Data provided to, developed by, or used by Seller for the performance of services under the Agreement. In lieu of returning copies and reproductions, Purchaser may, at its sole discretion, require Seller to destroy, using agreed upon methods to ensure data is not recoverable, all copies and reproductions of GE Data provided to, developed by, or used by Seller in the performance of services under the Agreement, and certify such destruction.

B.2 Seller must, in each case, seek and obtain Purchaser's prior written approval regarding the scope of any Personal Data to be collected, as well as any notices to be provided and any consent language to be

used when collecting such information, from a Data Subject. In the case of Personal Data collected directly from Data Subjects by Seller, Seller shall comply with applicable data privacy laws and regulations, including the rights of notice, consent, access and correction/deletion.

B.3 Seller warrants and represents that it shall comply with all applicable laws and regulations applicable to Seller's activities governed by this policy, including those concerning onward transfer to a third party, and international transfer, and will act only on Purchaser's written instruction concerning any such transfers. Seller must receive approval from Purchaser prior to (i) moving Personal Data from its Purchaser-approved hosting jurisdiction to a different hosting jurisdiction; or (ii) provisioning remote access to such Personal Data from any location other than the hosting jurisdiction or other Purchaser-approved jurisdiction.

B.4 Prior to providing access to any GE Data to any of its own suppliers, or to any of its Affiliates or subcontractors, Seller must ensure through an appropriate due diligence process that such party is capable of providing the level of security required in this policy. Seller must obtain Purchaser's prior written approval to provide access to any GE Data to any of its own suppliers or subcontractors that were not pre-qualified by or otherwise disclosed to, Purchaser at the time of engagement. Seller shall contractually obligate its suppliers and subcontractors to comply with (at a minimum) the same level of security required by this policy (including physical, organizational and technical information security controls), and Seller shall take reasonable steps to ensure continuing compliance with this policy. Seller will remain responsible at all times for all such Affiliates' and/or third-parties' compliance with the terms of this policy.

B.5 To the extent permitted by law, Seller will notify Purchaser promptly and act only upon Purchaser's instruction concerning any request by law enforcement or other governmental authority for disclosure of GE Data or for information concerning the Processing of GE Data in connection with the Agreement, as well as any request received from an individual concerning his/her Personal Data.

B.6 Any relevant Purchaser entity owning any of the GE Data being accessed pursuant to the Agreement may enforce the terms of this policy as permitted or required by applicable law.

B.7 In the event an applicable law or regulatory requirement impose stricter or additional requirements on Seller's collection and use of Personal Data than provided for in the Agreement and/or this policy, those requirements shall prevail.

Part C: Protecting GE Data

C.1 Seller shall implement appropriate physical, organizational and technical controls to ensure the security and confidentiality of GE Data in order to prevent accidental, unauthorized or unlawful destruction, alteration, modification or loss of GE Data; misuse of GE Data; and unlawful Processing of GE Data. The security measures taken shall be in compliance with applicable data protection regulations. Seller must maintain formal written policies and procedures for the administration of information security throughout its organization.

C.2 Seller's access, and the access by any of its personnel, if applicable, to and use of Purchaser's network shall be only on a need-to-know basis and only to the extent necessary to perform services under the Agreement or as otherwise instructed by Purchaser in writing. Purchaser may review, audit, monitor, intercept, access and disclose information Processed or stored on Purchaser equipment and technology, as well as any activity in the Purchaser's network or on devices accessing Purchaser's network.

C.3 Seller physical security controls will include, at a minimum, the following controls on all locations where GE Data may be stored or accessed:

- Secure perimeters
- External entry points protected against unauthorized access (where authorized access is Seller personnel and authorized visitors)
- Appropriate access controls and authentication mechanisms
- Visitor logs (maintained for at least one year) and continual escort or observation of authorized visitors upon each entry to and exit from the location
- Enforced clear desk policy, including, for example, securing of GE Data in locked offices/file cabinets
- All servers and/or network equipment used to store or access GE Data must be kept in a secure room with the following controls:
    - Additional access control mechanisms are required on entry doors in order to further restrict access to only authorized personnel.
    - Rooms must be located on the interior of the building with no windows unless safeguards are in place to prevent shattering and unauthorized entry (e.g., bars on windows, security grates).
    - Telecommunications equipment, cabling and relays receiving data or supporting services must be protected from interception or damage.
- For rooms containing servers and/or network equipment used to provide services to Purchaser, controls must be implemented to mitigate the risk of power failures (e.g., surge protectors, uninterruptible power supplies, and generators), and environmental conditions (e.g., temperature and humidity).

C.4 Organizational security controls will include the following at a minimum:

- Seller shall require its personnel with access to GE Data to sign and comply with confidentiality agreements that contain obligations consistent with those in this policy.
- Seller personnel with access to GE Data must participate in appropriate information security awareness training provided by the Seller prior to obtaining access to GE Data and thereafter on at least an annual basis while such personnel have access to GE Data.
- Seller will maintain a current inventory of Supplier Information Systems through which GE Data may be accessed that includes information about system locations and owners.
- Seller personnel are to be given no more access to GE Data than is required to perform their respective duties in support of the obligations set forth under the Agreement, and are to be

provided such access only for as long as required to support those obligations. Seller must ensure each account through which GE Data may be accessed is attributable to a single individual with a unique ID and each account must require authentication (e.g., password) prior to accessing GE Data. Shared accounts are not permitted. Seller must implement processes to support the secure creation, modification, and deletion of these accounts and any HPAs. Seller must review and update access rights at least annually, and at least quarterly for HPAs. Where Seller personnel have been assigned Purchaser Single Sign-On (SSO) credentials or other Purchaser-issued access credentials, such credentials must not be shared.

- Seller shall undertake reasonable measures to terminate Seller personnel access to GE Data, whether physical or logical, no later than the date of personnel separation or personnel transfer to a role no longer requiring access to GE Data; where personnel have been assigned Purchaser SSO credentials, Seller must notify Purchaser of any such separation or transfer no later than the day of that event or as soon as immediately practicable given the circumstances.
- If Supplier Information Systems are in a multi-tenant environment, Seller must implement physical and/or logical access controls to prevent unauthorized access to GE Data.
- GE Data may not be stored or accessed on personal accounts (e.g., individual email or cloud services accounts) or on personally-owned computers, devices or media.
- GE Data may not be stored on any computers, devices or media (e.g., laptop computers, phones/PDAs, USB drives, back-up tapes) unless data on such devices or media are encrypted at rest. Seller must approve any such encrypted removable media for access/storage of GE Data, ensuring protecting for that GE Data in a manner that is consistent with the requirements of this policy.
- Where specified in the Agreement, Seller must receive approval from Purchaser prior to moving GE Data from its Purchaser-approved physical location or jurisdiction to a different physical location or jurisdiction.

C.5 Technical security controls will include the following at a minimum:

- Supplier Information Systems must enforce the following password requirements:
    - Temporary passwords must be given to Seller personnel in a secure manner, with expiration on first use
    - Passwords must be encrypted or hashed when transmitting over networks and in storage
    - User account credentials (e.g., password) must not be shared.
    - Strong password practices must be enforced that include minimum password length (at least 8 characters), lockout (maximum 6 incorrect attempts), set expiration period (maximum age of ninety (90) days unless an exception has otherwise been approved by Purchaser in writing), and complexity consistent with industry practices
    - Default passwords are prohibited

- Seller must implement and maintain controls to detect and prevent unauthorized access, intrusions and computer viruses and other malware on its operating systems, infrastructure,

applications and software used for the performance of services under the Agreement. At a minimum such controls must include:
    - Client and server-side antivirus programs that include current antivirus definitions; and
    - Installation and production of all critical patches or security updates as soon as possible, but not later than thirty (30) days from the release of any such updates or patches.
- If Seller has a Trusted Connection granted by Purchaser for performance of services under the Agreement, Supplier must use only Purchaser-managed network devices and Purchaser-approved network architecture to connect to the Purchaser internal network.
- Seller must maintain documented change management procedures that provide a consistent approach for controlling and identifying changes (including emergency changes) for Supplier Information Systems that includes appropriate segregation of duties.
- Development and testing environments for Supplier Information Systems must be physically and/or logically separated from production environments and must not contain GE Data unless specified in the Agreement. Production changes must be approved by the Seller's appropriate system owner and such changes must not be made by any Seller developers.
- Any back-up media containing GE Data stored at Seller's site must be kept in a secure location (e.g., locked office or locked file cabinet). If off-site media storage is used, Seller must have a media check-in/check-out process with locked storage for transportation. Back-up information must be given the same level of physical and environmental protection as the level of control applied at the main site. All back-up media must be encrypted.
- Workstations that access or store GE Data must not be left authenticated when unattended, and must employ a timeout mechanism with a maximum fifteen (15) minute period before screen locking.
- Seller must use an auditable process (e.g., certification of destruction) to remove GE Data from Supplier Information Systems prior to disposal or re-use in a manner that ensures that the information may not be accessed or readable. Upon request, Seller must certify to Purchaser that GE Data has been disposed in a manner in which the data cannot be read or re-created.
- GE Data must be encrypted in accordance with U.S. National Institute of Standards and Technology (NIST) encryption standard or comparable standard when transferred (including emails) over public networks (such as the Internet).
- All HPA access must be established using encryption mechanisms (e.g., secure shell) and HPA usage must be reviewed at minimum weekly.
- Mobile device storage drives and laptop hard drives used to store or access GE Data must be encrypted.
- Mobile devices used to access GE Data (including emails) must have strong mobile device security controls enforced that include required passcode, minimum passcode length (at least 4 digits), inactivity lock after maximum thirty (30) minutes of inactivity, device wipe capabilities, and encryption. Seller must have a process in place to immediately wipe the device when notified that a mobile device is lost.
- Where encryption is required, Seller must maintain cryptographic and hashing algorithm types, strength, and key management processes consistent with industry practices.

- Network layer security devices must allow only authorized connections and rule sets must be reviewed at minimum semi-annually.

Part D: System Availability

D.1 This section, System Availability, applies to any Supplier Information System(s) (i) that Processes GE Restricted Data, and/or (ii) where an outage of the Supplier Information System(s), as identified in the Agreement or Order, is likely to significantly adversely impact Purchaser or overall Purchaser operations, financial position, regulatory compliance, and/or reputation . In either of these cases, Seller must maintain a disaster recovery (DR) program for all Supplier Information Systems and facilities used to provide services under the Agreement to Purchaser. The program must be designed to ensure that Supplier Information Systems can continue to function through an operational interruption and that Seller can continue to provide services as specified in the Agreement. At a minimum, the DR program should include the following elements:

- Seller's operational procedures must verify the successful completion of backups and the backup media must be tested regularly (at minimum quarterly) to ensure that it will operate in the event of an emergency.
- Seller must maintain inventories that list all critical Supplier Information Systems. The inventories must be updated at minimum annually.
- DR plans must be developed for all Supplier Information Systems and facilities that are used to provide services to Purchaser and reviewed/approved at minimum annually.
- Seller must conduct full scale DR tests annually against DR plans (unless otherwise agreed with Purchaser) for Supplier Information Systems that Seller reasonably believes are critical for providing services to Purchaser to ensure that such Supplier Information Systems can be recovered in a manner that meets the contractual service levels specified in the Agreement. DR results must be documented and provided to Purchaser upon request.

Part E: Security Incidents

E.1 Seller shall notify Purchaser within a reasonable period, in no event to exceed seventy-two (72) hours after discovery, of any suspected or actual Security Incident experienced by Seller involving any GE Data. To the extent permitted by applicable law or regulation, Seller shall provide Purchaser a detailed description of the Security Incident, the type of data that was the subject of the Security Incident, the identity of each affected person, and any other information Purchaser reasonably may request concerning such affected persons and the details of the Security Incident, as soon as such information can be collected or otherwise becomes available. Seller shall designate an individual responsible for management of the Security Incident, and will identify such individual to Purchaser promptly. Thereafter, Seller, through its individual, will reasonably cooperate with Purchaser in its

investigation of such incident, including providing reasonable and timely responses to Purchaser's inquiries and requests.

E2. Any notification required pursuant to E.1 shall be made by Seller via the notification mechanism prescribed in the Agreement.

E.3 Seller must develop and maintain an up-to-date incident management plan designed to promptly identify and address any Security Incidents. Seller shall take action immediately, at its own expense, to investigate any Security Incident and to identify, prevent and mitigate the effects of any such Security Incident, and to carry out any recovery or other actions necessary to remedy the impact.

E.4 Seller shall pay for or reimburse Purchaser for all costs, losses and expenses relating to any Security Incident experienced by Seller, including without limitation, costs of forensic assessments, Notices, credit monitoring or other fraud alert services, and all other remedies either required by applicable law or which are customary in the industry or required under Puchaser's then-current policies or contractual commitments.

E.5 Seller shall, if requested by Purchaser, and at Purchaser's direction, send any and all Notices regarding any Security Incident experienced by Seller affecting GE Data unless applicable law requires Purchaser, itself, to send Notices, in which case Seller shall reimburse Purchaser for all costs related thereto. To the extent permitted by applicable law or regulation, Seller shall provide Purchaser with reasonable notice of, and the opportunity to comment on and approve, the content of all Notices prior to any publication or communication thereof to any third party, except Purchaser shall not have the right to reject any content in a Notice that must be included in order to comply with applicable law.

E.6 Other than to law enforcement or as otherwise required by law or regulation, Seller may not make or permit any public statements concerning Purchaser's involvement with any such Security Incident to any third-party without the explicit written authorization of Purchaser's Legal Department.

Part F: Audits

F.1 Seller responsibilities:

- Seller will monitor the effectiveness of its security program by conducting self-audits and risk assessments of Supplier Information Systems against the requirements of written policies and procedures maintained pursuant to this policy no less frequently than every twelve (12) months. Seller shall be responsible for ensuring consistency of its security operations, including proactive monitoring and mitigation of all vulnerabilities across all of its sites.
- Upon request, Seller must provide to Purchaser formal reports of any audits and assessments conducted on Supplier Information Systems, which shall include, at a minimum, the scope of the audit and/or assessment and any vulnerabilities/issues/findings/concerns/recommendations in so far as they impact GE Data. Such formal reports provided by Seller to Purchaser shall be treated as confidential.

- Seller must use its best efforts to remediate any items rated as high or critical (or similar rating indicating commensurately similar risk) in any audits or assessments of Supplier Information Systems within thirty (30) days.

F.2 Purchaser audit rights:

- Upon request, with reasonable advance notice and conducted in such a manner not to unduly interfere with Seller's operations, Purchaser reserves the right to conduct an audit of Seller's compliance with the requirements set forth in this policy relating to GE Data including but not limited to: (i) a review of Seller's applicable policies, processes, and procedures, (ii) a review of the results of Seller's most recent application vulnerability scanning, penetration testing, and similar testing results and accompanying remediation plans, and (iii) on-site assessments of Seller's physical security arrangements, network, and systems during Seller's regular working hours. Seller shall provide access to all concerned facilities, equipment and records in order to conduct such audit. Purchaser reserves the right to conduct an onsite audit of Seller on ten (10) business days prior written notice during regular business hours. This right shall survive termination or expiration of the Agreement so long as Seller Processes GE Data provided under the Agreement. Seller agrees to cooperate fully with Purchaser or its designee during such audits and shall provide access to appropriate resources, provide applicable supporting documentation to Purchaser, and complete security assessment questionnaires that may be requested by Purchaser.
- Unless otherwise agreed by Seller, each Purchaser Affiliate receiving services under the Agreement shall be permitted to exercise this audit right a maximum of once per calendar year unless a Security Incident occurs, in which case each Purchaser Affiliate shall additionally be permitted to audit Seller following each such occurrence. For the purposes of this paragraph, any audit conducted by a Purchaser Affiliate to validate or verify the appropriate completion of remediation items identified in a prior Purchaser audit shall not be subject to the aforementioned limitation.
- Purchaser acknowledges and agrees that nothing in this paragraph F.2 shall oblige Seller to divulge any information relating to its other customers to Purchaser in such a manner that may put Seller in breach of its obligations of confidentiality to such customers.
- If Seller is hosting an internet facing application that Processes GE Data, Purchaser reserves the right to conduct penetration testing of Seller's environment on ten (10) business days prior written notice during regular business hours. Purchaser will provide a plan for such testing and will work with Seller's IT or security team, as applicable, to schedule such testing.
- Seller hereby grants to Purchaser, or shall procure the direct grant to Purchaser, of a royalty free, non-exclusive, non-transferable, license to use such of the Seller's software, systems, documentation, processes and procedures, and such applicable third party software, during the term of the Agreement, for the purpose of Purchaser availing itself of all functionality necessary for Purchaser to adequately manage and oversee Seller's adherence to its obligations set forth herein.

Part G: Additional Regulatory Requirements

G.1 In the event Seller Processes GE Data which is subject to additional regulatory requirements, or in a manner subject to additional regulatory requirements, Seller agrees to cooperate with Purchaser to comply with such requirements. Such cooperation may include, without limitation:

- Execution of additional agreements required by applicable law and identified by Purchaser and/or Seller (e.g., EU Standard Contractual Clauses)
- Entry into U.S. Protected Health Information Agreement, found here http://www.geaviation.com/company/doing-business-with-aviation/aviation-po-requirements.html, where Seller will Process any GE Restricted Data that is protected health information, including any medical, demographic, visual or descriptive information that can be used to identify a particular patient/individual subject to the U.S. Health Insurance Portability and Accountability Act of 1996 and the regulations promulgated under that Act (collectively, HIPAA).
- Implementation of additional security controls required by applicable law (e.g. NIST, U.S. Federal Information Security Management Act (FISMA), HIPAA, US Sarbanes-Oxley Act, U.S. Gramm-Leach-Bliley Financial Services Modernization Act (GLBA) Section 501(b) Standards for Securing Customer Information, Payment Card Industry Data Security Standards (PCI DSS) security requirements)
- Completion of regulatory filings applicable to Seller (e.g. EU data protection authority filings)
- Completion of required regulatory audits (e.g. U.S. Food and Drug Administration (FDA) audits)

G.2 Seller acknowledges and understands that certain Purchaser businesses (including but not limited to GE Healthcare) and business processes are certified to the US-EU and US-Swiss Safe Harbor Frameworks (Safe Harbor). Seller also acknowledges and understands that, as Safe Harbor-certified entities, the relevant Purchaser businesses are obligated pursuant to the Safe Harbor to require Seller to provide at least the same level of privacy protection for Personal Data as is required by the relevant Safe Harbor principles. This policy is designed and intended to satisfy this requirement of the Safe Harbor and, therefore, Seller agrees to comply with this policy in its entirety.

Part H: Additional Requirements for GE Restricted Data

H.1 Sellers that Process GE Restricted Data must comply with the requirements of this Part H in addition to all other applicable requirements of Parts A through G above.

H.2 When Processing GE Restricted Data, Seller must have an IT security organization with clearly defined information security roles, responsibilities and accountability.

H.3 Seller must perform vulnerability assessments on Supplier Information Systems at least annually. For Supplier Information Systems that are internet facing, Seller must engage an independent external party to perform the vulnerability assessment. If any items rated as high or critical (or similar rating indicating commensurately similar risk) are not remediated within thirty (30) days, Seller must notify Purchaser and provide a remediation plan with timing for completion.

H.4 Additional physical security controls when Processing GE Restricted Data will include the following:

- Physical Access must be monitored, recorded and controlled with physical access rights reviewed at minimum annually. Physical access logs detailing access must be stored for a period of one (1) year to the extent permitted by local law. If not staffed 24x7, alarms and entry point security cameras must be installed for off-hours access monitoring with recordings retained for at least thirty (30) days.
- All Seller personnel and authorized visitors must be issued identification cards. Identification cards must be visibly displayed at all times while on the premises. Visitor identification cards must be easily distinguishable from Seller personnel identification cards and must be retrieved and inventoried daily.

H.5 Additional technical security controls when Processing GE Restricted Data include the following:

- Seller networks used to access or store GE Data must have security controls that can detect and prevent attacks by use of network layer firewalls and intrusion detection/prevention Systems (IDS/IPS) in a risk based manner (e.g., between the Internet and DMZ, and between DMZ and internal servers containing GE Restricted Data). IDS/IPS high and critical priority alerts (or similar alerts indicating commensurately similar risk) must be continuously monitored and responded to as soon as reasonably practicable.
- Any Seller personnel accessing Seller's internal network remotely must be authenticated using a minimum two-factor authentication method and such transmissions must be encrypted.
- Seller must implement hardening and configuration requirements meeting SysAdmin Audit Network Security (SANS) Institute, National Institute of Standards Technology (NIST), and Center for Internet Security (CIS).
- Seller must develop and maintain a robust incident management plan. Security-relevant events (e.g., failed log-on attempts, creation of accounts, account lock-outs, privilege escalation) on Suppliers Information Systems must be logged, reviewed on a periodic basis (minimum quarterly), secured, and maintained for a minimum of twelve (12) months.
- GE Restricted Data must not be stored on removable media (e.g., thumb drives or external hard drives) other than physically secured retention media expressly used for the purpose of backup or data retention for business continuity planning/disaster recovery purposes. Such retention media must be encrypted.
- At a minimum, GE Restricted Data must be stored in a directory or folder with controlled access, (e.g., password protection). Where technically feasible, GE Restricted Data must be stored in encrypted form, except where encryption in storage is mandatory in such cases of removable media and mobile devices as set forth above.
- Seller must implement appropriate data loss prevention (DLP) controls (e.g., disabling of USB ports, DLP software, URL/Web filtering) to detect and prevent unauthorized removal of GE Restricted Data from Supplier Information Systems.

Part I: Software Development

I.1 Sellers that either perform code development services for Purchaser, or host Supplier Information Systems that Process GE Restricted Data must comply with the following requirements:

- Seller must have a documented software development lifecycle process that includes requirements gathering, system design, integration testing, user acceptance testing, and system acceptance.
- Seller must provide all developers application security training and information regarding vulnerabilities discovered along with prevention and remediation measures for those vulnerabilities.
- Information security checkpoints following industry best practice, such as The Open Web Application Security Project (OWASP), must be incorporated into the software development lifecycle, including but not limited to risk assessments, documented security requirements, secure coding guidelines and checklists, source code review, and security testing prior to moving to production. All confirmed high/critical vulnerabilities found during testing must be remediated and retested prior to moving to production.

Part J: Termination

J.1 Subject to paragraph J.2 below and to any agreement in writing with Purchaser to the contrary, Seller shall within 30 (thirty) days of termination of the Agreement, for whatever reason, cease all Processing of GE Data and GE Restricted Data and shall return to Purchaser all copies and reproductions of such data. In lieu of returning copies and reproductions, Purchaser may, at its sole discretion, require Seller to destroy, using agreed upon methods to ensure no data is recoverable, all copies and reproductions of GE Data and GE Restricted Data provided to, developed by, or used by Seller in the performance of services under the Agreement and certify to such destruction.

J.2 Purchaser acknowledges that Seller may, by virtue of its standard back-up procedures and/or as a requirement of certain laws/regulations to which Seller is subject, be required to maintain copies and/or back-up copies of GE Data or GE Restricted Data (including as part of records, documents or broader data sets) beyond the period described in paragraph J.1. In such cases, notwithstanding the requirements of paragraph J.1, Purchaser agrees that Seller may continue to retain such GE Data or GE Restricted Data in copies and/or back-up copies beyond the period prescribed in paragraph J.1 provided that (i) Seller notifies Purchaser on termination of its need to retain such copies and/or back-up copies; (ii) Seller has a documented retention period and secure deletion procedure for such copies and back-up copies, with back-up copies retained no longer than 6 (six) months from the date on which they were captured, and legally required copies retained only to the end of their legally required retention period; (iii) such copies and back-up copies shall be deleted in accordance with such documented procedure; (iv) Seller shall perform no Processing of GE Data or GE Restricted Data other than that necessitated by retaining or deleting the relevant copies and back-up copies; and (v) Seller shall continue to comply with all the requirements of this policy in relation to any such retained GE Data or GE Restricted Data until the same is securely deleted.

J.3 Termination of the Agreement, for any reason, shall not relieve the Seller from obligations to continue to protect against the impermissible disclosure of GE Data or GE Restricted Data.

Part K: Supplier Personal Information

K.1 Seller understands and agrees that Purchaser may require Seller to provide certain personal information such as the name, address, telephone number, and e-mail address of Seller's representatives in transactions to facilitate the performance of the Agreement, and that Purchaser and its contractors may store such data in databases located and accessible globally by their personnel and use it for necessary purposes in connection with the performance of the Agreement, including but not limited to Seller payment administration. Purchaser will be the Controller of this data for legal purposes, and agrees to use reasonable technical and organizational measures to ensure that Supplier Personal Information is Processed in conformity with applicable data protection laws. Seller may obtain a copy of the Supplier Personal Information by written request, or submit updates and corrections by written notice to Purchaser.

Part L: Material Breach

L.1 Failure by the Seller to comply with the obligations set forth in this policy shall be construed as a material breach of the Agreement.