GE Vernova Third-Party Cyber Security Requirements

Prepared by: GE Vernova 3rd Party Security Team

Version: 2.2

Effective Date: April 1st, 2024

1. INTRODUCTION

The GE Vernova Third-Party Cyber Security Requirements document outlines the cyber security requirements applicable to GE Vernova third-parties, including suppliers and joint ventures. The security requirements outlined herein, are applicable to third-parties that process, access, interact with, or store GE Vernova sensitive Information (classified internally as GE Vernova Confidential or GE Vernova High Confidential), PII or Sensitive PII, have access to a GE Vernova Information System, or provide certain services/products, to include OT/Manufacturing services, as described below. The security requirements are designed to vary based on the level of risk the Third-Party presents to GE Vernova, specifically guided by the type of GE Vernova information the Third-Party processes, network connection, and products and services provided by the Third-Party, as well as data availability and resiliency requirements. In addition to GE Vernova cyber security requirements, third-parties are required to abide by applicable regulatory requirements.

Cyber security requirements mentioned in this document are high level security requirements which are supplemented by the cyber security controls discussed during the GE Vernova security assessment.

GE Vernova reserves the right to update this document from time to time.

2. IT SECURITY REQUIREMENTS

Applicability: IT security requirements are applicable to third-parties that process, access, or stores GE Vernova Confidential Information or Personal Data, GE Vernova Highly Confidential Information or Sensitive Personal Data, Controlled Data, or if the Third-Party has a direct network connection to the GE Vernova managed network.

IT Security Requirements	
2.1	Third-Party must have a documented and evidenced identity and access management process for granting, modifying, and revoking access to ensure confidentiality, integrity, and availability of systems used to access, process, store and transmit GE Vernova Data.
2.2	Third-Party must enforce strong password requirements on their IT assets.
2.3	Third-Party must change default passwords of all their IT assets.
2.4	Third-Party must centrally manage user accounts especially privileged accounts (using RSA, RADIUS, TACACS, LDAP etc.).
2.5	Third-Party must ensure that all administrators use two accounts; regular accounts for normal activities and domain administrator accounts for activities requires escalated privileges.
2.6	Third-Party must ensure that security relevant events logs are reviewed & stored for at least 90 days on all servers (Including but not Limited to DHCP & DNS servers), and critical network devices (e.g., firewalls, Intrusion Detection System, routers, etc.).
2.7	Third-Party must have personnel in place to identify anomalous / high-risk transactions for users supporting GE Vernova engagements. This analysis may be done within the Third Party's enterprise Security Incident & Event Management (SIEM) or User & Entity Behavioral Analytics (UEBA) platforms.

2.8	If a Third-Party experienced a ransomware attack, data breach, or any other significant cyber event in the last 24 months then they must provide detailed information on the breach that was identified, it's impact, and how it was remediated. For any future external attacks and/or compromises, the Third Party must report it to security@gevernova.com (GE Vernova CIRT). For any concern related to the misuse or unauthorized access / disclosure of GE Vernova Proprietary Information, they must report it to tidal@ge.com (GE Vernova Insider Threat). Copy itrisk3pc.itauditors@gevernova.com (GE Vernova third party security team) in these emails.
2.9	Third-Party must have a documented change control process in place.
2.10	Third-Party must have DLP agents on all IT assets used to access, process, store or transmit GE Vernova data. DLP must be configured at least for the following: logging of endpoint transactions, blocking of unsanctioned / high-risk software, blocking of high-risk endpoint ports/protocols (e.g. blocking of USB ports, Bluetooth file transfer etc.), & blocking of movement to personal devices (e.g. remote data transfer).
2.11	Third-Party must have a process to protect cryptographic keys if they are used to encrypt GE Vernova data.
2.12	Third-Party must ensure to store GE Vernova data in encrypted form using an encryption algorithm equivalent to AES 128, 192, or 256.
2.13	Third-Party must have Endpoint Detection and Response (EDR) capabilities implemented on all applicable IT assets.
2.14	Third-Party must have Antivirus (AV) & host-based firewall (FW) installed, updated and operational on all applicable IT assets.
2.15	Third-Party must not utilize any high-risk technologies mentioned in US FCC's covered list in the IT environment being used by GE Vernova. Refer https://www.fcc.gov/supplychain/coveredlist for details.
2.16	Third-Party must have a documented information security incident management plan that is tested at least annually.
2.17	Third-Party must maintain an inventory of all their IT assets including physical devices, software, internally and externally hosted applications, cloud providers, third-party network connections etc.
2.18	Third-Party must have a comprehensive network security program in place.
2.19	Third-Party must have network level intrusion detection or prevention system to monitor their network 24x7x365 and a process to act on critical & high alerts.
2.20	Third-Party must have enforced secure wireless encryption protocol (e.g., WPA2) to connect to their organization's Wi-Fi.
2.21	Third-Party must enforce multi-factor authentication while connecting remotely to company network.
2.22	Third-Party must have a patch management process which includes applying all relevant vendor rated critical patches and security updates within 30 days of release by the vendor.
2.23	Third-Party must not use any end of life (EOL) technology.
2.24	Third-Party must perform periodic security awareness training and assessment.
2.25	If Third-Party needs to outsource any GE Vernova related work or have to share GE Vernova Information to their suppliers/contractors, they must have a process to identify, assess, and manage supply chain cyber risks and perform cyber security assessments of their suppliers/contractors before sharing GE Vernova Information. Third-Party must have processes, policies, and controls to only allow sharing of GE Vernova Information to vetted suppliers/partners and reassess their suppliers/contractors on a periodic basis.
2.26	Third-Party must perform at least annual network vulnerability assessment or penetration test on the local & cloud IT infrastructure which store, process, host, or transmit GE Vernova data.

2.27	If Third-Party use application(s) to store, process, host, and/or transmit GE Vernova data they must perform annual web application vulnerability assessment or penetration test.
2.28	Third-Party must have a policy to remediate all critical or high rated security vulnerabilities or issues within 30 days of identification. This includes issues identified in IT security audits or vulnerabilities identified in network or web application vulnerability assessments or penetration test.
2.29	Third-Party must configure session timeouts on all IT assets. Recommended ideal session timeout for workstations and servers is 15 minutes and for applications it is 30 minutes.
2.30	Third-Party must have a controls/process in place to ensure only authorized software will be installed on desktops, laptops, and servers.
2.31	Third-Party must have a mechanism in place to make sure no one has access to tamper logs on their SIEM/local systems.
2.32	Third-Party must perform pre-employment background screening for those who require access to GE Vernova data, systems, or work in GE Vernova project.
2.33	Third-Party must not store GE Vernova data on any removable media. If there is any such requirement, it must be approved by GE Vernova business counterpart and the backup media must be encrypted.
2.34	Third-Party must have a data flow diagram for GE Vernova engagement.
2.35	Third-Party must have a documented media disposal process.
2.36	If Third-Party is using mobile devices to access, process, store, and/or transmit GE Vernova data then those mobile devices should be managed by a mobile device management (MDM) solution.
2.37	Third-Party must have an IT Security organization in place. The role of this team will be to perform IT risk assessments, internal audits, supporting external audits, maintain and monitor security metrics, reporting security posture to higher management etc.
2.38	Third-Party must ensure that a Disaster Recovery Plan (DRP) is documented and at least annually tested.
2.39	Third party must have controls in place to block GE Vernova Information from being uploaded to high-risk web applications (E.g. Personal cloud storage, personal email services, etc.).
2.40	All Third-Party employees who have a non-GE Vernova issued endpoint, & are supporting a GE Vernova engagement, must route all internet traffic/web workloads through GE Vernova's Remote Access agent after successful connection to GE Vernova VPN solution.
2.41	Third-Party must install GE Vernova endpoint agents or use GE Vernova infrastructure / services where required by GE Vernova.
2.42	Third-Party must have controls in place to restrict both permissions & access for exiting employees to prevent the misuse / unauthorized disclosure of GE Vernova Information.
2.43	If a Third-Party becomes aware that an employee is exiting, the Third-Party must immediately notify the relevant GE Vernova sponsor, and ensure that access to GE Vernova resources is terminated immediately after the employee's last day worked.
2.44	Third party must disable internet connection sharing / network connection sharing on IT assets deployed in GE Vernova project.
2.45	Third party must have hardening standard in place for all applicable technologies used to access, process, store or transmit GE Vernova data and they should perform periodic hardening scanning to identify any deviation from initial hardened state of IT assets.
2.46	Third party must not expose GE Vernova data to DeepSeek AI.

2.47	The Third Party shall maintain AI governance practices, including controls to prevent GE Vernova data from being exposed to or used with public or unauthorized generative AI models, and to manage associated AI security risks.
2.48	The Third Party shall assess and manage cybersecurity risks arising from advanced and malicious use of AI and maintain appropriate governance to monitor and respond to emerging AI-related cyber risks.
2.49	The Third Party shall maintain capabilities to address Frontier AI-enabled vulnerability discovery and exploitation, including AI-assisted security testing of internally developed software. The Third Party shall periodically reassess patching timelines for critical systems in response to evolving Frontier AI-driven threats.
2.50	The Third Party shall maintain capabilities to detect, respond to, and recover from AI-enabled and highly automated cyber-attacks and keep incident response playbooks current for AI-driven attacks, and validate readiness through AI-scenario exercises.
2.51	The Third Party shall maintain appropriate controls and awareness programs to protect against AI-enabled phishing, impersonation, deepfakes, and other sophisticated social engineering attacks.

3. PHYSICAL SECURITY REQUIREMENTS

Applicability: The physical security requirements are applicable to third-parties that process, access, or stores (logically or physically) GE Vernova Confidential Information or Personal Data, GE Vernova Highly Confidential Information or Sensitive Personal Data, Controlled Data or if the Third-Party has a direct network connection to the GE Vernova managed network.

Physical Security Requirements	
3.1	Third-Party must ensure that all facilities used to access, process, transmit, and/or store GE Vernova data, have badge readers, security cameras, security guard and mantrap on all entry & exit points to ensure physical access is restricted to authorized personnel.
3.2	Third-Party must ensure that all servers and network equipment used to store and/or access GE Vernova data shall be kept in a secure room with the proper controls in place.
3.3	Third-Party must retain security camera recordings for at least 30 days.
3.4	Third-Party must have/issue an identification badges for all employees, contractors, and visitors and delineate full time employees from contractors and visitors.
3.5	If applicable, third-party must ensure that all physical documents that contain GE Vernova data/information shall be kept in a locked office, cabinet, or other location which is locked, and access restricted to authorized personnel only.
3.6	Third-Party must ensure to have a mechanism in place to notify, investigate, and address potential physical security incidents such as physical intrusion or a stolen asset.
3.7	Third-Party must ensure that all facilities used to access, process, transmit, and/or store GE Vernova data are staffed 24x7x365 and if not, alarms should be installed for off-hour access monitoring.

3.8	Third-Party must ensure if a facility used to access, process, transmit, and/or store GE Vernova data are not shared with other occupants (e.g.co-located data center). If it is shared, then protective mechanisms should be implemented between occupants to prevent unauthorized access to their organization's physical equipment.
3.9	Third-Party must ensure that physical access rights should be reviewed on an annual basis (at a minimum) and updated as needed to ensure physical access to all facilities used to access, process, transmit, and/or store GE Vernova data is restricted to authorized personnel.

4. SOFTWARE DEVELOPMENT

Applicability: The software development requirements are applicable to third-parties that develop software specific to GE Vernova's needs or hosts applications that Process GE Vernova Highly Confidential Information, Confidential Information, Controlled Data, or Sensitive Personal Information.

Software Development Requirements	
4.1	Third-Party must ensure to have Software Development life cycle process documented and communicated to all employees and train them accordingly.
4.2	Third-Party must ensure to provide proper training to software developers based on their role.
4.3	Third-Party must ensure that all confirmed critical/high vulnerabilities (mediums and low depending on impact) found during testing shall be remediated and retested within 30 days of identification and prior to moving code to production.
4.4	Third-Party must ensure that any software developed for GE Vernova shall not contain any proprietary or open-source code developed or sold by an entity other than the contracting third-party unless approved by GE Vernova.
4.5	Third-Party must ensure that all software delivered to GE Vernova shall be free of defects/vulnerabilities.
4.6	Third-Party must ensure that if the third-party hosted application undergoes Significant Changes or Enhancements, GE Vernova has the option to perform a technical penetration test (manual and/or automated) prior to the changes being implemented in production.
4.7	Third-Party must ensure that all third-party hosted applications shall be reassessed every two years.
4.8	Third-Party must ensure to have a designated application security representative that acts as the primary liaison between the Third-Party and GE Vernova in matters related to secure application development, ensuring that their team following all GE Vernova requirements for secure application development and provide requested evidence as per the request.
4.9	Third-Party must ensure that application's risk classification (Critical vs. non-Critical) and network exposure designation (External or Internal facing) are requested from the GE Vernova application owner.
4.10	Third-Party must have a secure design requirement documented & defined in collaboration with the GE application owner and other key stakeholders.
4.11	Third-Party must ensure to have proper backup of code on a regular basis.
4.12	Third-Party must ensure that application development shall take place in a secured development environment.

4.13	Third-Party must ensure to perform Static Application Security Testing (SAST) & Dynamic Application Security Testing (DAST) on the code & application.
4.14	Third-Party must ensure to perform security design review to verify required security features and functionality.

5. CLOUD SECURITY

Applicability: The cloud security requirements are applicable to the third-party that host a cloud computing application (in a SAAS, PAAS, IAAS, DRAAS etc. environment) that processes GE Vernova Highly Confidential Information, Confidential Information, Controlled Data, or Sensitive Personal Data, or the third-party provides a cloud computing platform that allows GE Vernova to develop, run, or manage applications, or the third-party is responsible for the management of virtual machine image and/or hypervisor.

Cloud Security Requirements	
5.1	Third-Party must ensure that root/administrator access to the management console shall require multifactor authentication.
5.2	Third-Party must ensure a dedicated secure network, which shall be separate from customer production infrastructure, leveraged to provide management access to the cloud infrastructure.
5.3	Third-Party must ensure to store all cloud & account activities logs into a central log aggregation tool and they must have the ability to provide logs which are specific to the instances used for GE Vernova/GE Vernova engagement.
5.4	Third-Party must have a backup process for cloud VPC and a periodic restoration testing process.
5.5	Third-Party must ensure to retain the original structure and format of data residing within the cloud application for easy movement to another cloud solution/cloud service provider.
5.6	In cloud environment, Third-Party must ensure to encrypt GE Vernova data at rest and control in place to protect encryption keys.
5.7	Third-Party must have an access management control for their cloud application & VPC.
5.8	Third-Party must have a cyber incident management process for their cloud application & VPC.
5.9	Third-Party must have a patch management process for their cloud application & VPC.
5.10	Third-Party must vault root/administrator account credentials.
5.11	Third-Party must ensure that web application/network vulnerability assessment or penetration test shall be performed for their cloud application & VPC at least annually.
5.12	Third-Party must implement web application firewall (WAF) for their cloud application.
5.13	Third-Party must have a control in place for monitoring configuration drift.

6. DATA CENTER SECURITY

Applicability: The data center security requirements are applicable to third-parties which provides data center facility services.

Additional Data Center Security Requirements	
6.1	Third-Party must ensure to have proper physical security controls in place at their data center.
6.2	Third-Party must ensure that all assets containing GE Vernova data shall be caged off physically from the rest of the data center and have physical security control in place to access those assets.
6.3	Third-Party must ensure to have an access management process of granting access to data center. They must store all access & user logs for at least 1 year and review them on a regular basis.
6.4	Third-Party must ensure that server rooms shall not be used for storage and shall be clear of all unnecessary equipment and material not in use.
6.5	Third-Party must ensure to have detective monitoring and controls implemented to mitigate the risk of overhead water sources impacting the IT equipment.
6.6	Third-Party must ensure that all data centers shall have a fire suppression system and all data center workers will be trained in control and storage of combustible materials and on the correct processes to follow when detecting a fire.
6.7	Third-Party must ensure that all computer devices are connected to surge protectors to protect them against spikes and surges in the electrical power supply.
6.8	Third-Party must ensure that backup power supply is available in the form of local generator(s).
6.9	Third-Party must ensure to have Emergency lighting, powered by a supply other than the main power, shall be implemented throughout the data center in accordance with local fire and health and safety regulations.
6.10	Third-Party must ensure that data center have a system in place to control and monitor temperature and humidity, air conditioning system to control air quality and minimize contamination.
6.11	Third-Party must ensure that data center shall have air conditioning systems with dust filtration systems by separating zones for standard working areas, and areas containing equipment such as server rooms.
6.12	Third-Party must ensure that server rooms shall have positive pressurization to minimize contaminants entering these areas.
6.13	Third-Party must ensure to have a process in place for scheduled testing and maintenance of all critical data center infrastructure including security, power & environmental systems.
6.14	Third-Party must ensure that critical data center infrastructure including power & environmental systems shall be engineered to function through an operational interruption. The design shall be a minimum of N+1.
6.15	Third-Party must ensure that all GE Vernova equipment shall be properly mounted in appropriately sized racks which are ground and/or ceiling mounted in accordance with local earthquake guidelines.
6.16	Third-Party must ensure to have process in place for a movement of equipment.

6.17	Third-Party must ensure to have a documented equipment or media delivery or handling process.
6.18	Third-Party must ensure to have a DRP documented & tested.
6.19	Third-Party must ensure that all GE Vernova equipment shall be completely network segregated from non-GE Vernova parts of the data center.

7. DIRECT NETWORK CONNECTIVITY SECURITY

Applicability: The direct network connectivity security requirements are applicable to third-parties that have a GE Vernova Trusted Third-Party network connection.

Direct Network Connectivity Security Requirements	
7.1	Third-Party shall use only GE Vernova managed network devices to connect to the Trusted Third-Party connection. GE Vernova requires out of band connectivity to the remote device for administration.
7.2	Third-Party shall implement a firewall between the third-party parent network and the Trusted Third-Party network.
7.3	Third-Party shall remediate all critical or high vulnerabilities within 30 days of notification by GE Vernova.
7.4	Third-Party must ensure that all internet traffic shall be directed to a GE Vernova managed external proxy.
7.5	Third-Party must ensure that remote access to the Trusted Third-Party network is only allowed through the GE Vernova Virtual Private Network (VPN) hub infrastructure with two-factor authentication.
7.6	Third-Party must ensure that GE Vernova managed network equipment shall be housed in a caged environment and/or be physically separated from the Third-Party equipment.
7.7	Third-Party must ensure to have a physical security control in place on GE Vernova managed network equipment.
7.8	Third-Party shall ensure that all wireless deployments on Trusted Third-Party networks must follow the GE Vernova Third-Party network change request process and are configured/managed by GE Vernova.
7.9	Third-Party must ensure that all unused switch ports shall be disabled on network equipment. In addition, all new connection requests shall be submitted to GE Vernova.

8. PRODUCT SECURITY

Applicability: The product security requirements are applicable if the third party provides a product, component or service that includes or supports the following: software, firmware, and/or complex hardware (i.e. logic bearing device, HMI/Scada Software, Historians, IEC Device, Switch/router, PLC); designed to be operated in networked environment (i.e. provides a communication interface); USB/portable media access (e.g. CD/DVD/ext. disk); remote access (e.g. remote desktop protocol); services that include a software or networked component; Integrated solutions or a system of systems that work together to provide logical control and input/output interfaces (Windfarm, DCS System, Project based solutions); Cloud Applications that interact with or receive data from OT.

Product Security Requirements – Secure Software Development	
8.1	Third Party must ensure that all products have been developed in accordance with principles of secure software development consistent with software development industry best practices, including, special purpose security design review, secure coding practices, risk-based testing, and remediation requirements. Also, third party's software development environment used to develop the products must have security controls that can detect and prevent attacks.
8.2	If applicable, Third-party must provide cyber-security certifications, declarations of conformity or proof of compliance, including but not limited to the following: • Third Party Attestations • Security by design with CMMI for development (v1.3) • IEC62443 3-3, 4-1 or 4-2 • ISO27001 • EU Cyber Resilience Act (EU) 2024/2847
8.3	The Third Party must maintain the security and integrity of the product development environment by adhering to the following standards: • Asset and Software Governance: All assets, software, and firmware used in product development must be properly licensed, scanned regularly (minimum cadence is quarterly), for malware, and maintained with the latest security patches and updates. • Vulnerability Support Lifecycle: The Third Party shall provide effective vulnerability management for a minimum of five (5) years, or for the duration of the product's lifecycle, whichever is shorter. • Patch Management and Disclosure: The Third Party must maintain a formal patch management process. Upon the release of security patches or updates, the Third Party must: o Disseminate these updates to GE Vernova without delay and at no additional cost. o Provide formal advisory documentation accompanying each release, detailing the addressed security issues and any required actions to be taken by the user.
8.4	The Third Party must enforce authentication for all services and capabilities, ensuring that no default, hard-coded, or 'backdoor' accounts or passwords are utilized. The system must adhere to the following security standards: • Products must be configured to enforce the principle of least privilege across all user accounts, file systems, and application-to-application communications. • The product must support passwords with a minimum length of 12 characters (or the system maximum) and a complexity requirement of at least three different character types (e.g., uppercase, lowercase, numeric, and non-alphanumeric). • All authentication and password change processes must utilize secure cryptographic standards. • GE Vernova must retain the ability to modify all passwords supported by the product. • The system must implement an automated account lockout mechanism or provide alerts upon exceeding a defined threshold of consecutive failed authentication attempts to mitigate brute-force risks.

	• Access to administrative functions, system logs, and security settings must be restricted to authorized personnel only.
8.5	Third Party must ensure that an obsolescence and end of life strategy have been developed and documented for digital components and products and must notify GE Vernova no less than 24 months prior to the End-of-Life date.
8.6	Third-party must document the wireless technology complies with standard operational and security requirements specified in applicable wireless standard(s), specification(s) (e.g., applicable IEEE standards, such as 802.11) or regulatory requirements (Radio Equipment Directive 2014/53/EU) if any wireless technology is incorporated in the product.
8.7	If any cryptographic systems are contained in the product, then third-party must use cryptographic algorithms and key lengths that meet or exceed the most current version of the National Institute of Standards and Technology (NIST) Special Publication 800-131A, and third-party shall provide an automated remote key-establishment (update) method that protects the confidentiality and integrity of the cryptographic keys.
8.8	Third-party must ensure that all software and firmware components shall undergo the release testing including below: (i) Static Code Analysis Testing (ii) Dynamic Application. Security Testing (iii) Secrets Detection (iv) Open-Source Vulnerability Detection (v) Open-Source license detection (vi) Infrastructure as Code (vii) Container Security All Critical, High or Known Exploitable Vulnerabilities must be remediated in the product that GE Vernova will receive Note: This can be done on the source code or binaries.
8.9	Third-party must ensure that penetration testing will be performed on the component(s) that GE Vernova is purchasing by third party and all the test results shall be retained and made available to GE Vernova on request, which includes date of testing, methodology used, impact, mitigation adopted, residual risk.
8.10	Third-party shall incorporate AI frontier models as part of the product testing and validation process to assess performance, identify potential defects, and support compliance with applicable requirements. The supplier must ensure such models are used in a controlled, documented, and auditable manner, with appropriate human oversight and validation of outputs before product release.
8.11	If the component supports remote access, the third party must implement security controls to manage session integrity and access. These controls must include: • Session Inactivity Timeout: Automated termination of user sessions following a configurable period of inactivity.

	• Concurrent Session Management: A configurable limit on the number of simultaneous remote sessions permitted per user or account. • Last Logon Notification**:** A mechanism to display the date and time of the user's last successful logon upon their next access to the system. • Utilization of current industry-standard cryptographic protocols. • Enforcement of secure session token expiration
8.12	The third party must ensure that all software and firmware components are cryptographically verified for integrity and digitally signed prior to delivery. All deliverables must be signed using a certificate from a trusted authority that is verifiable by GE Vernova's internal security systems to ensure authenticity of the deliverables.
8.13	The third party must ensure the component implements robust audit logging, capturing critical events including successful and failed authentication attempts, timestamps (synchronized to internal system clocks), and session duration. Audit logs must be protected against unauthorized access and tampering, with restricted access limited to authorized administrators only. The product shall maintain logs for a minimum of 180 days and provide the functionality to securely export logs to external systems (e.g., syslog servers) for centralized monitoring. Logging mut be implemented in a way that does not lead to resource exhaustion if abused.
8.14	The Third Party must complete and maintain a Product Secure Development Lifecycle (SDL) Assessment and a Product Technical Security Capabilities Assessment. These documents must be kept current and updated promptly upon GE Vernova's request to reflect any changes to the product or environment.
8.15	The third party must implement a robust secure procurement process to identify and mitigate security risks associated with all third-party components, including Free and Open-Source Software. At a minimum the process must assess the following: • The product's lifecycle and support period • The products' technical capabilities against all capabilities specified within this document • How to report a vulnerability • Open or unmitigated vulnerabilities • Verification of the product's CE marking and EU Declaration of Conformity where applicable As part of this process, the Third Party must maintain and provide GE Vernova a comprehensive list of all high-risk technologies, vendors, or components (e.g., those restricted by trade compliance or cybersecurity policy, such as Huawei, ZTE, or Kaspersky) utilized within the product or its development lifecycle. Certain high-risk vendors are banned by GE Vernova and must not be utilized.
8.16	Third-party must ensure to have a documented secure development life cycle standard in place and up to date based on industry recognized best practices such as IEC62443, NIST or CIS.
8.17	Third-party must ensure that coding standards are established that address known vulnerabilities in the programming languages and frameworks used in the component that GE Vernova is purchasing.
8.18	The Third Party shall establish and maintain a process to identify applicable software development lifecycle (SDL) objectives and all relevant customer and regulatory cybersecurity requirements and ensure that internal processes and documentation are updated to reflect these new requirements.
8.19	The Third Party must conduct a comprehensive threat model based on an industry standard framework, such as STRIDE, for the component being provided to GE Vernova. This exercise shall identify, assess,

	and document all inherent security risks. The resulting threat model and risk assessment documentation must be made available to GE Vernova upon request.
8.20	Third-party must ensure that the security requirements and assumptions shall be documented to provide the measures necessary to mitigate each threat identified during the threat modeling exercise.
8.21	The Third Party must establish and maintain a baseline set of security requirements for all projects. This baseline shall be derived from industry best practices, the requirements outlined in this document and lessons learned and must be appropriately tailored to the specific technologies and use cases implemented.
8.22	Third-party must ensure that security verification and validation plans been developed & documented.
8.23	Third-party must ensure that they have a developed continued deployment compliance plan which includes the schedule and scope of reoccurring validation.
8.24	Third party must document and disclose any AI features or capabilities implemented within the product with descriptions to identify the technology used and the extent of the technology's capabilities within the product.
Product Security Requirements – Audit and Verification	
8.25	Third party must ensure that the security controls of all third-party suppliers are consistent with their organizational security policies and as per contract with their organization and the supplier. GE Vernova also reserves the right to perform its own audits of supplier processes and documentation associated with its cyber security program.
Product Security Requirements - Cybersecurity Vulnerabilities, Assessment and Reporting	
8.26	Third-party must ensure to develop and maintain an up-to-date Cybersecurity **Vulnerability** management plan designed to promptly identify, prevent, investigate, and mitigate any known Cybersecurity Vulnerabilities. This plan follows industry best practices, such as NERC, IEC 62443, NIST or CIS. In the event of a Cybersecurity Vulnerability involving GE Vernova, the Third Party shall notify GE Vernova at GEV.PSIRT@gevernova.com with "PSIRT" in the subject line within 24 hours with the following information: (i) Description of the Cybersecurity Vulnerability (ii) the remediation plan (including advice on temporary security measures/workarounds) (iii) any other information GE Vernova requires, within reason. One or more of the following remediations shall be provided to GE Vernova without delay but no later than 90 days: (i) Upgrades (ii) Updates (iii) Maintenance releases (iv) Error or bug fixes
8.27	Where the third party becomes aware of an actively exploited vulnerability or a severe incident having an impact on the security of the product supplied to GE Vernova, it shall notify GE Vernova PSIRT and CIRT in accordance with the following timelines:

	(a) early-warning notification within 24 hours of becoming aware; (b) vulnerability/incident notification within 72 hours providing general information, an initial assessment, and corrective or mitigating measures; (c) for vulnerabilities, a final report no later than 14 days after a corrective measure becomes available; (d) for severe incidents, a final report within one month of the incident notification.
8.28	Third Party must ensure to have a cybersecurity **incident** response and reporting policy that addresses identification, classification, and response to cybersecurity incidents. This policy shall follow industry best practices such as NERC, IEC 62443, NIST or CIS. In the event of a cybersecurity incident involving GE Vernova data, the Third Party shall notify the following GE Vernova contacts within 24 hours of confirmation of an incident. (i) Vernova.CIRT@gevernova.com (ii) GEV.PSIRT@gevernova.com
8.29	Third-party must ensure that the product security incident response capability shall be tested on at least yearly basis using tabletop exercise, automated simulations, and or an actual incident. Updates to the incident response shall be performed based on the results from the yearly test.
8.30	The Third Party shall not issue or authorize any public statements, disclosures, or communications regarding GE Vernova's involvement in any cybersecurity vulnerability or incident without prior, explicit written authorization from GE Vernova's Legal Department, except where such disclosure is strictly required by applicable law or regulation.
8.31	Third Party shall receive security alerts, advisories and directives from network vendors, the US-CERT and the EU ENISA on an ongoing basis and generate internal security alerts, advisories and directives as deemed necessary.
8.32	GE Vernova shall have reserved the right to conduct a cybersecurity assessment of the applicable Products, and the Product development lifecycle, which includes tests intended to identify potential cybersecurity vulnerabilities. Third Party shall designate an individual responsible for management of the Cybersecurity Vulnerabilities and shall identify this individual to GE Vernova promptly upon establishment or change.
Product Security Requirements - Physical Security and Distribution Integrity	
8.33	Third-party must ensure to have a process for physical security and distribution security mechanisms are in place, including, but not limited to the following: (i) Only allowing access to GE Vernova's components' environment only to personnel cleared by both third party and GE Vernova. (ii) The use of tamper evident seals on media and containers, to detect unauthorized access to protected products (e.g. tamper evident labels or seals, which self-destruct and leave a residue sticker if removed) (iii) Tamper-resistant production (e.g. digital signatures for software and corresponding hardware mechanisms).
Product Security Requirements - Additional Insurance	
8.34	Third-party shall obtain Technology Errors & Omissions Liability Insurance, with a minimum limit of USD $5,000,000 per claim and in the aggregate, covering all Products including failure of IT security and data privacy breach and software copyright infringement. If coverage is on a claims-made basis, the policy must contain a retro date which precedes the effective date of this Agreement and continuity must be maintained for 1 year following termination or expiration of this Agreement.

Product Security Requirements - SBOM	
8.35	As a third party for GE Vernova, we require SBOMs, covering at minimum top-level dependencies, for products sold to any GE Vernova business unit, either being utilized directly within GE Vernova or included as a packaged component distributed to our customers. While the definitions for what comprises an SBOM can be broad, GE Vernova has determined what we consider as the minimum elements needed to produce a valuable SBOM for consumption: (i) Product Names (ii) Common Platform Enumerations (CPEs) or Unique Identifier; if applicable (iii) Included Component Libraries, Packages, and Modules (iv) Upstream Dependencies (v) Applicable Versions (vi) Supplier Name (Both for Self and Dependencies) (vii) Date of SBOM Creation SBOMs will be provided in a standard machine-readable format (such as SPDX or CycloneDX) to facilitate our automated ingestion processes. The SBOM shall be updated upon every release, security update, or substantial modification, and retained for the longer of ten (10) years or the support period.
Product Security Requirements – User Manuals, Guides and Documentation	
8.36	The Third Party must provide comprehensive cybersecurity documentation to GE Vernova, detailing the necessary configurations to secure both the product and its surrounding environment. This documentation must explicitly identify: • Intended purpose and foreseeable use and misuse cases • EU Declaration of Conformity Location, if applicable • How to report a vulnerability • all logical and physical ports required for product functionality • Account management guidelines for permissions and privileges • The products lifecycle and support period • Default accounts used by the product and instructions for changing default accounts and passwords. • hardening best practices to minimize the attack surface of the deployment. • How to reset the product to a default state • Personal data that may be collected or processed as part of the product's use and the justification of such collected data. • How to securely decommission the product
8.37	Third-party must ensure to keep the technical documentation and the required certifications (general description, design/development, vulnerability-handling processes, SBOM, risk assessment, support-period rationale, list of harmonized standards / common specifications applied, test reports, EU declaration of conformity) for at least 10 years for all products supplied to GE Vernova after the product with digital elements has been placed on the market or for the support period, whichever is longer. This documentation shall be provided within 24 hours upon request from GE Vernova.

Product Security Requirements - Training	
8.38	Third-party must have a training process to ensure its personnel and subcontractors have been informed of, accept, and comply with GE Vernova's cyber security policies. Third Party personnel and subcontractors must undergo an awareness and role-based training program that promotes cyber security equivalent to our GE Vernova awareness program. This includes relevant security policies, procedures and awareness of industry standards (e.g. IEC62443, NERC and EU directives). The training shall be given to personnel and subcontractors on a yearly basis at a minimum.
Product Security Requirements - Additional Representations and Warranties	
8.39	Open-Source Software and Third-party Materials Warranty. Third Party represents warrants and covenants that: (i) It has disclosed all Open-Source Software and Third-party Materials utilized with the Products supplied to GE Vernova, and no Open-Source Software or Third-party Materials have been or will be provided to GE Vernova or used as a component of or in relation to any Products provided under the Agreement, except with the prior written authorization of GE Vernova (ii) All Open Source Software contained within the Products are and shall be in material compliance with the terms and conditions of the applicable licenses governing their use, and the Products or the use thereof by GE Vernova shall not cause GE Vernova or GE Vernova's intellectual property rights to be subject to the terms or conditions of a Copyleft License, or require GE Vernova to fulfil any open source license obligations for any Open Source Software contained within the Products.
8.40	Code Integrity Warranty. Third-party represents, warrants, and covenants that the Products: (i) Do not contain any restrictive devices such as any key, node lock, time-out, time bomb, or other function, whether implemented by electronic, mechanical, or other means, which may restrict or otherwise impair the operation or use of the Products or any material embodying or comprising products. (ii) Must be free of viruses, malware, and other harmful code (including, without limitation, time-out features) which may interfere with the use of the Products regardless of whether Third Party or its personnel purposefully placed such code in the Products. In addition to exercising any of GE Vernova's other rights and remedies under this Agreement or otherwise at law or in equity, Third party shall provide GE Vernova, free of charge, with any and all new versions, upgrades, updates, releases, maintenance releases, and error or bug fixes of the Products (collectively, "Revised Code") which prevents a breach of any of the warranties provided under this Agreement or corrects a breach of such warranties. Revised Code contained in the Products constitutes Products for purposes of this Agreement.

9. RESILIENCY REQUIREMENTS

Applicability: The resiliency requirements are applicable to third-parties that process, access, or stores (logically or physically) GE Vernova Highly Confidential Information or Sensitive Personal Data, Controlled Data, if the supplier is a sole source or single source manufacturer of products, components, or materials for GE Vernova where the supplier has a critical or high impact on operations/production of critical products.

Resiliency Requirements	
9.1	Third-Party must have an information security incident management plan in place.
9.2	Third-Party must identify a stakeholder and assign roles & responsibilities to staff for carrying out the activities described in the security incident management plan.
9.3	Third-Party must have a process in place to escalate/communicate to stakeholders/effected parties about incident.
9.4	Third-Party must have management oversight of the performance on incident management activities and performance of the external dependency activities.
9.5	Third-Party must have service continuity plans in place.
9.6	Third-Party must have mechanisms in place to achieve resilience requirements in normal and adverse situations.
9.7	Third-Party must have a documented resilience requirements for external dependencies/relationships management.
9.8	Third-Party must have a process to identify, analyze and manage the risk arising from external dependency/relationship management
9.9	Third-Party must identify infrastructure providers on which the critical service depends.
9.10	Third-Party must have external dependency/relationship management activities reviewed periodically and measured to ensure they are effective, producing the intended results and adhering to the plan.
9.11	Third-Party must ensure to identify a resource to monitor threat and trained to communicate threat information for respective parties (internal/external)

10. OPERATIONAL TECHNOLOGY (O.T.)/MANUFACTURING SECURITY REQUIREMENTS

Applicability: The O.T./Manufacturing security requirements are applicable to third-parties that manufactures products, components or materials for GE Vernova; excluding Commercial Off-the-Shelf (COTS) items, low cost and high-volume commodity items, and commercially available raw materials.

Operational Technology Security Requirements	
10.1	Third-Party must ensure that all hardware and software assets used in their manufacturing environment are centrally managed and protected by the firewall.
10.2	Third-Party must contain all manufacturing assets in a locked facility or one that is badge access controlled.

10.3	Third-Party must ensure that all assets, software & firmware in their manufacturing environment are licensed and periodically scanned for malware & update to date with security patches/updates.
10.4	Third-Party must have a process in place to manage removable media such as USB devices, external hard drives, floppy disks, or compact disks.
10.5	Third-Party must have access management & password security controls in place for accessing assets in manufacturing environment.
10.6	Third-Party must ensure that all remote network connections to devices/equipment within their manufacturing environment are encrypted using AES 128, 192, or 256.
10.7	Third-Party must have a firewall restriction in place to limit remote connections to authorized endpoints only.
10.8	Third-Party must have a documented media disposal process in place.
10.9	Third-Party must monitor all assets in manufacturing environment for abnormal/malicious activity.
10.10	Third-Party must have a document incident management plan in place that covers their manufacturing environment.
10.11	Third-Party must have a process in place to inform GE Vernova if have any data breach or other incidents within 72 hrs.
10.12	Third-Party have a documented BCP/DRP process for manufacturing environment.
10.13	Third-Party must have at least one manufacturing site that could be leveraged in the event the primary manufacturing site is adversely impacted due to a cyber incident.
10.14	Third-Party must capture and retain backups of manufacturing system software and firmware assets where possible.
10.15	Third-Party must have a document change management process for their manufacturing environment.
10.16	Third-Party must ensure to document the list of all the 3rd party software, firmware, or hardware used in their manufacturing environment
10.17	Third-Party must ensure to manage and periodically review the 3rd parties that have remote access to any assets within their manufacturing environment.

11. GENERATIVE ARTIFICIAL INTELLIGENCE REQUIREMENTS

Applicability: The Generative Artificial Intelligence security requirement is applicable to third parties providing Gen AI services or use Gen AI to process/analyze GE Vernova data.

Generative Artificial Intelligence Security Requirements	
11.1	Third-Party must have controls in place to ensure the integrity of the Gen AI learning models (For examples Checksum or digital signatures).
11.2	Third-Party must have access controls in place to protect Gen AI system/model & the systems linked to Gen AI models. Note: Make sure your organization grants limited access to a set of privileged users with two-person control (TPC) and two-person integrity (TPI)

11.3	Third-Party must have authentication and authorization mechanisms for API access to Gen AI application/systems.
11.4	Third-Party must have controls in place to protect Gen AI models against tampering or unauthorized access.
11.5	Third-Party must ensure that privacy impact assessment is performed on their Gen AI system/modules to identify and mitigate risks to personal data.
11.6	Third-Party must ensure to identify and protect all proprietary data sources they use in Gen AI model training or fine-tuning, and they must ensure the fairness and quality of the data via established data management policies.
11.7	Third-Party must have controls in place to prevent GE Vernova data include prompts from being used in training foundational models and ensure that model improvements & training are disabled by default unless requested by the GE Vernova.
11.8	Third-Party must ensure to log and monitor critical activities like identifying abuse, tampering, or corruption of model data, performance and usage metrics, or logging of any other critical activities.
11.9	Third-Party must have control/process in place for anomaly detection techniques to identify unusual patterns or behaviors pertaining to AI/FM/LLM services.
11.10	Third-Party must have process in place for monitoring, alerting, and handling of incidents related to abuse, tampering, or corruption of the solution which include details on level of automation and human intervention & analysis.
11.11	Third-Party must have a process in place to notify the customer for any type of incidents linked to AI/FM/LLM services.
11.12	Third-Party must have a process in place to assess all their third parties that they rely on for AI/FM/LLM services.
11.13	Third-Party must ensure & validate the authenticity of 3rd party data sources which are used to train/ supplement Gem AI systems.
11.14	Third-Party must have documented the steps taken to detect and mitigate bias in the Gen AI application to ensure fairness and transparency in AI decision making processes.
11.15	Third-Party must provide Gen AI security awareness training to educate users on security best practices when using Gen AI applications.
11.16	Third-Party must provide Gen AI security awareness training for developers working on Gen AI platforms.
11.17	Third-Party must apply 'secure by design' principles and 'Zero Trust' (ZT) frameworks to manage risks to and from the Gen AI system.
11.18	Third-Party must carefully inspect models, especially imported pre-trained models, inside a secure development zone prior to considering them for tuning, training, and deployment in enterprise environment.
11.19	Third-Party must ensure to have a control related to content safety for the LLM to mitigate risks such as bias, hallucination, explicit images, etc.
11.20	Third-Party must ensure to have a control to protect GE Vernova prompts and confidential or highly confidential data from leaking to the internet or search engines.
11.21	Third-Party must ensure that their 3rd party contractual agreements include provisions for security, data protection, and incident response.

11.22	If third-Party is using a 3rd Party LLM, the terms and conditions of the LLM must disclose the use of copyrighted data sources and the licensing agreements specify "acceptable usage" of the LLM.

12. DEFINITIONS

Controlled Data is technical or government information with distribution and/or handling requirements proscribed by law, including but not limited to controlled unclassified information and license required export-controlled data, which is provided by GE Vernova to the Third-Party in connection with performance of the Contract Document.

Copyleft License means the GNU General Public Licenses version 2.0 (GPLv2) or version 3.0 (GPLv3), Affero General Public License version 3 (AGPLv3), or any other license that requires, as a condition of use, modification and/or distribution of or making available over a network any materials licensed under such a license to be: (a) licensed under its original license; (b) disclosed or distributed in source code form; (c) distributed at no charge; or (d) subject to restrictions on assertions of a licensor's or distributor's patents.

Cybersecurity Vulnerability (ies) means any bug, software defect, design flaw, or other issue with software associated with a Product that could adversely impact the confidentiality, integrity or availability of information or processes associated with the Product.

GE Vernova Confidential Information is information created, collected, or modified by GE Vernova that would pose a risk of causing harm to GE Vernova if disclosed or used improperly, and is provided and identified as such to the Supplier under the Contract Document. GE Vernova Confidential Information includes Highly Confidential, Personal, Controlled, or Sensitive Personal Data.

GE Vernova Data includes Highly Confidential, Confidential, Personal, Controlled, or Sensitive Personal Data.

GE Vernova Highly Confidential Information is GE Vernova Confidential Information that GE Vernova identifies as "highly confidential" in the Contract Document, or that GE Vernova identifies as "Restricted," "Highly Confidential," or similar at the time of disclosure.

GE Vernova Information System(s) means any systems and/or computers managed by GE Vernova, which includes laptops and network devices.

GE Vernova Trusted Third Party Network means the isolated portion of the GE Vernova network made available for Trusted Third Parties to connect securely to the GE Vernova network.
Highly Privileged Accounts (Users), 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.

Mobile Devices means tablets, smartphones and similar devices running mobile operating systems. Laptops are not considered Mobile Devices.

Open Source Software means any material that is distributed as "open source software" or "freeware" or is otherwise distributed publicly or made generally available in source code form under terms that permit modification and redistribution of the material on one or more of the following conditions: (a) that if the

material, whether or not modified, is redistributed, that it shall be: (i) disclosed or distributed in source code form; (ii) licensed for the purpose of making derivative works; and/or (iii) distributed at no charge; (b) that redistribution must be licensed or distributed under any Copyleft License, or any of the following license agreements or distribution models: (1) GNU's General Public License (GPL), Lesser/Library GPL (LGPL), or Affero General Public License (AGPL), (2) the Artistic License (e.g., PERL), (3) the Mozilla Public License, (4) Common Public License, (5) the Sun Community Source License (SCSL), (6) the BSD License, (7) the Apache License and/or (8) other Open Source Software licenses; and/or (c) which is subject to any restrictions on assertions of patents.

Personal Data means any information related to an identified or identifiable natural person (Data Subject), as defined under applicable law Processed in connection with the Contract Document. Legal entities are Data Subjects where required by law. Personal Data is GE Vernova Confidential Information.

Product(s) mean any goods, products, software and deliverables supplied under the Contract Document.

Process(ing) means to perform any operation or set of operations upon GE Vernova data, whether or not by automatic means, including but not limited to, collecting, recording, organizing, storing, adapting or altering, retrieving, accessing, consulting, using, disclosing by transmission, disseminating, or otherwise making available, aligning or combining, blocking, erasing, or destroying.

Sensitive Personal Data is a category of Personal Data considered to be especially sensitive and includes medical records and other personal health information, including protected health information (PHI), as defined in and subject to the U.S. Health Insurance and Portability Act of 1996; personal bank account and payment card information and other financial account information; customer bank account and payment card information; national identifiers; and special categories of data under applicable law (such as racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic and biometric data, home life and sexual orientation).

Significant Change or Enhancement (to software) means: • Any code change that impacts application interfaces (modifies data stream inputs/outputs).

- Any code change to the application that modifies access to or use of external components (database, files, DLLs, etc.).
- Any code change that impacts access control.
- A complete or partial rewrite of an application into a different language (ex. C++ to Java) or different framework (ex. Struts and Spring).
- A change in the application that results in internet exposure where previously it was not.
- A change in the application that results in the Risk Level increasing (ex. reclassification from Level 4 to Level 3).
- Transferal of development responsibilities from one Third-Party to another, from a Third-Party to GE Vernova, or from GE Vernova to a Third-Party. The correction of any existing critical or high vulnerabilities must be conducted prior to transfer or included in the work order for the new Third Party to correct within the applicable remediation timeframe.

Third-Party or Supplier is the entity that is providing goods or services to GE Vernova pursuant to the Contract Document. It also refers to GE Vernova joint ventures.

Third-Party Information System(s) means any Third-Party system(s) and/or computer(s) used to Process, Store, Transmit and/or Access GE Vernova Confidential Information pursuant to the Contract Document, which includes laptops and network devices.

Third-Party Materials means materials which are incorporated by Supplier in any Products provided to GE Vernova, the proprietary rights to which are owned by one or more Third-Party individuals or entities.

Third-Party Workers means all persons or entities providing services and/or deliverables under the Contract Document, including Supplier's employees, permitted affiliates, suppliers, contractors, subcontractors and agents, as well as anyone directly or indirectly employed or retained by any of them.

Trusted Third Party Network Connection is a physically and/or logically isolated segment of the Third-Party network connected to GE Vernova internal network in a manner identical to a standard GE Vernova office.