GE Vernova Third-Party Cyber Security Requirements

Prepared by: GE Vernova 3rd Party Security Team

Version: 2.0

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@ge.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.

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 multi-factor 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: 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); 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.

Product Security Requirements	
8.1	Third-Party must ensure to have a documented product security policy that mandates requirements for reasonable industry specific measures to protect the products your company manufactures.
8.2	Third-Party must ensure to identify a product security leader and enterprise security architects in the execution of the product security program and resolution of cyber threats.

8.3	Third-Party must ensure to perform a Static Application Security Test (SAST) & Dynamic Application Security Test (DAST) on the product & software/firmware accordingly.
8.4	Third-Party must ensure that developer verify the integrity of software and firmware components.
8.5	Third-Party must ensure that proper testing will be performed on the open-source software or 3rd party components if they are included in the component GE Vernova is purchasing.
8.6	Third-Party must ensure to have a proper authentication and authorization controls in place if the component is capable, which includes access & password management.
8.7	Third-Party must ensure to have a control in place if the component have remote access capability. Which includes encrypting the connections, limit the connection, etc.
8.8	Third-Party must ensure that if component have an interface/port to connect to portable storage devices then it should have controls in place to protect and have a documentation for connecting.
8.9	Third-Party must ensure to have capability to store & retain all type of logs for 180 days and make sure no one can tamper the logs.
8.10	Third-Party must ensure to have a product security incident response policy. Also, in future if Third-Party identifies any cyber breach related to the product, then your organization must inform at security@gevernova.com (GE Vernova CIRT), & GE Vernova Business SPOC. Please copy itrisk3pc.itauditors@ge.com (GE Vernova third party security team) in these emails.
8.11	Third-Party must ensure to have product patch management process in place.
8.12	If applicable, Third-Party must ensure to have cyber-security certifications (example security by design with CMMI for development (v1.3), Wurldtech Achilles Communication Certifications, Wurldtech APC (IEC 62443-2-4)
8.13	Third-Party must ensure to have a product cyber security awareness training and make sure all employees are trained accordingly.
8.14	Third-Party must ensure to perform periodic security reviews and/or on-site audits/assessments of their suppliers/contractors if they work along with your organization in developing this component and they must comply with GE Vernova product requirement.
8.15	Third-Party must ensure that services or capabilities that are not required to implement in the product functionality by default are disabled or require authentication.
8.16	Third-Party must perform penetration testing on the component(s) that GE Vernova is purchasing.
8.17	Third-Party must ensure that product will comply with wireless standard(s) or specification(s) (e.g., applicable IEEE standards, such as 802.11) if the product incorporated with wireless technology.
8.18	Third-Party must ensure that they follow cryptographic controls to encrypt GE Vernova data on the product and comply with NIST Special Publication 800-131A.
8.19	Third-Party must ensure to have a product vulnerability management process.
8.20	Third-Party must ensure that all software been digitally signed to ensure its integrity.
8.21	Third-Party must have a documented secure development life cycle standard in place.
8.22	Third-Party must develop a plan that identifies the applicable software development lifecycle objectives and customer/regulatory cybersecurity requirements.
8.23	Third-Party must ensure that the component that GE Vernova is purchasing undergone a threat modeling exercise to assess and document the components inherent security risks.
8.24	Third-Party must have security architecture been developed and documented for the component that GE Vernova is purchasing.
8.25	Third-Party must ensure that security verification and validation plan been developed & documented.

8.26	Third-Party must ensure that a digital obsolescence and end-of-life strategy been developed and documented.
8.27	Third-Party must have a continued deployment compliance plan been developed which includes the schedule and scope of reoccurring validation.

9. RESILIENCY SECURITY REQUIREMENTS

Applicability: The resiliency security 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 Security 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. ARTIFICIAL INTELLIGENCE REQUIREMENTS

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

Artificial Intelligence Security Requirements	
11.1	Third-Party must have controls in place to ensure the integrity of the AI learning models (For examples Checksum or digital signatures).
11.2	Third-Party must use cryptographic methods, digital signatures, and checksums to confirm each artifact's origin and integrity to protect sensitive information from unauthorized access during AI processes.
11.3	Third-Party must have access controls in place to protect AI system/model & the systems linked to 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)
11.4	Third-Party must have authentication and authorization mechanisms for API access to Gen AI application/systems.
11.5	Third-Party must have controls in place to protect AI models against tampering or unauthorized access.

11.6	Third-Party must have a process in place to recertify AI system access including frequency of recertification, review process details, and responsible approvers.
11.7	Third-Party must ensure that security audits or assessments are performed on their AI systems/models.
11.8	Third-Party must ensure that AI risks from third-party sources are monitored and risk controls are identified & applied.
11.9	Third-Party must have threat model for their AI systems.
11.10	Third-Party must ensure that privacy impact assessment is performed on their AI system/modules to identify and mitigate risks to personal data.
11.11	Third-Party must ensure to identify and protect all proprietary data sources they use in AI model training or fine-tuning, and they must ensure the fairness and quality of the data via established data management policies.
11.12	Third-Party must ensure that they test the newly updated/different version of AI model before they deploy and track version changes.
11.13	Third-Party must have controls in place to prevent GE Vernova data from being used in training foundational models.
11.14	Third-Party must have a process for customers to opt out of model improvements or training or abuse monitoring.
11.15	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.
11.16	Third-Party must have control/process in place for anomaly detection techniques to identify unusual patterns or behaviors pertaining to AI/FM/LLM services.
11.17	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.
11.18	Third-Party must have a process in place to notify the customer for any type of incidents linked to AI/FM/LLM services.
11.19	Third-Party must have a process in place to assess all their third parties that they rely on for AI/FM/LLM services.
11.20	Third-Party must ensure & validate the authenticity of 3rd party data sources which are used to train/ supplement AI systems.
11.21	Third-Party must have measures in place to mitigate risks from 3rd party components.
11.22	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.
11.23	Third-Party must provide security awareness training to educate users on security best practices when using Gen AI applications.
11.24	Third-Party must provide security awareness training for developers working on Gen AI platforms.
11.25	Third-Party must apply 'secure by design' principles and 'Zero Trust' (ZT) frameworks to manage risks to and from the AI system.
11.26	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.
11.27	Third-Party must securely encrypt sensitive AI information & GEV data at rest and protect encryption/cryptographic keys.

11.28	Third-Party must have a process to protect model weights? **Note:** Model weights can be likened to the building blocks of a language model's intelligence. They are numerical values that the model learns and adjusts during its training phase.
11.29	Third-Party must ensure that their AI systems will not interact with any open internet resources at the time of data gathering.
11.30	Third-Party must maintain a catalog of trusted and valid data sources which will help protect against potential data poisoning or backdoor attacks. **Note:** For data acquired from third parties, consider contractual or service level agreement (SLA).
11.31	Third-Party must ensure that their 3rd party contractual agreements include provisions for security, data protection, and incident response.
11.32	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.