GE DIGITAL
DATA PROTECTION PLAN

This Data Protection Plan ("Data Protection Plan") describes the data protection policies and procedures applicable to Customer Content (defined below) processed by GE Digital ("GE Digital; we; us; our") as part of our products and services (the "GE Offerings"). This Data Protection Plan is incorporated by reference, and forms part of your agreement with GE Digital (the "Customer Agreement"). In the event of any conflict or inconsistency between this Data Protection Plan and the terms in your Customer Agreement, the Data Protection Plan shall prevail. Your use of any third-party products or services, including in connection with the GE Offerings, will be governed by such separate third-party terms. For purposes of this Data Protection Plan, "GE Digital" means the GE Digital entity set forth in your Customer Agreement. All other terms shall be as defined herein, or in your Customer Agreement.

1. GE Digital's Obligations.

1.1 Security. Section 2 describes the technical and organizational measures we use to protect the confidentiality, integrity, and availability of the data, information, documentation, and software, if any, you provide to us in connection with the GE Offerings ("Customer Content"). Section 2 also describes your obligations with respect to any Customer Content you provide to us.

We reserve the right to modify this Data Protection Plan at any time, including to meet our evolving security requirements, industry standards, or legal requirements; provided that, during the term specified in your Customer Agreement, the level of security we provide in processing the Customer Content shall in no event be less protective than what is described in this Data Protection Plan.

1.2 Personal Data. We act as a "data processor" of any personal data included as part of your Customer Content as that term is defined under applicable data protection laws. You remain the data controller of all such personal data. We will act on your documented instructions when processing your personal data as part of your Customer Content, and use reasonable efforts to assist you in fulfilling your obligation under applicable data protection laws, including when notifying relevant supervisory authorities and data subjects about security incidents involving your personal data. We will comply at all times with our privacy policy when processing your personal data https://www.ge.com/privacy ("GE Privacy Policy").

1.3 Compliance with Law. Each Party will comply with the laws and regulations applicable to its obligations under this Data Protection Plan. If Customer Content includes any data subject to specific legal or regulatory requirements (including, but not limited to, health care data, EU personal data, export-controlled data, or sensitive government data), you agree to notify us in writing of such requirements and provide any information that is necessary or reasonably requested by us to determine the applicable regulatory requirements. Except as may be specified by us in writing, we will not have any responsibility to discover or provide GE Offerings that comply with such legal or regulatory requirements.

1.4 Location and Transfer of Customer Content. Customer Content may be transferred to, stored and/or processed in the United States or other countries in which we or our affiliates or subcontractors operate. We will act in accordance with the requirements of the Customer Agreement and applicable data protection law regardless of where we store or process Customer Content. Upon your reasonable request, we will negotiate in good faith regarding any further data processing, localization or data transfer agreements as may be required to support the lawful processing or transfer of personal data. Our processing and transfers of personal data, if any, included in the Customer Content will be performed as described in the GE Privacy Policy.

2. GE Digital Security Measures.

This section describes technical and organizational measures we use to protect the confidentiality, integrity, and availability of Customer Content you provide to us as part of the GE Offerings.

Functional Area	Measure
Administrative Controls (organization, policies, verification, training)	**Security Organization.** Our information security program is managed through a cross-functional, coordinated structure that includes our Business, IT, Legal, HR, Facilities and Cyber Security stakeholders. **Security Policies.** We have implemented detailed policies, procedures, and technical measures to secure data, systems, and services associated with the GE Offerings. **Security Oversight.** • **Chief Information Security Officer**. The CISO oversees risk mitigation for the GE Offerings. Responsibilities include developing and maintaining security policies applicable to the GE Offerings; issuing supporting standards, technical security requirements and guidelines; and monitoring and enforcing compliance with applicable policies, standards, and contractual and legal requirements. • **GE Board of Directors.** As part of its oversight role, GE's Board of Directors reviews our practices and programs related to cybersecurity. The committee is updated regularly on our cyber threats and risk-management strategy. **Human Resource Security.** Our employment candidates, employees, and suppliers are subject to background verification proportional to their roles, consistent with applicable law. Our employees are required to undergo training regarding our privacy and information security policies, including the acceptable use of GE information resources, before accessing customer data. GE employees receive on-going privacy and security awareness training and communications.
Asset and Access Management	**Asset Inventory.** We follow a standard process for controlling the inventory of our managed devices and equipment ("GE Assets"). This process requires all GE Assets be identified and tracked, and the asset owners identified. GE Asset owners are responsible for maintaining up-to-date information regarding their GE Assets. **Access Control.** We follow a standard process for controlling access to GE Digital managed infrastructure. This process encompasses account and password control, segregation of duties and monitoring, passwords, and entitlement reviews. • GE Digital user IDs may be created and/or modified only with the approval of designated personnel. Accounts are requested and approved via workflows, and each account is attributable to a single individual with a unique ID (not shared) and requires authentication(e.g., password) prior to access. We terminate user logical and physical access to accounts promptly following personnel separation or transfer to a role no longer requiring access. • Prior to granting physical or logical access to facilities, systems or data, suppliers and customers are required to sign agreements setting forth their responsibility for managing information security in a manner consistent, as applicable, with GE Digital security policies and requirements consistent with this Data Protection Plan.

	• A small set of shared administrative accounts are available to our designated system administrators for emergencies. These accounts are stored in an encrypted shared account password management application that may be accessed only by approved administrators. This 'password safe' application requires two-factor authentication. Access to the safe is controlled via roles. Authenticated users can retrieve passwords for specific servers or approved applications. Passwords retrieved from the safes are reset upon check-in or forcibly reset after eight (8) hours if not checked in prior to expiration. Use of these emergency accounts is logged and reviewed. • We deactivate authentication credentials that have not been used for six months or more. • We identify those personnel who may add, modify, or remove authorized access to system resources. **Authentication**. We use industry standard password protection practices and policies, including practices designed to maintain the confidentiality and integrity of passwords when they are assigned and distributed, and during storage. • We use industry standard practices to identify and authenticate users who attempt to access information systems. • Where authentication mechanisms are based on passwords, we require the password to be at least eight characters long and meet complexity requirements. • Where authentication mechanisms are based on passwords, we require that the passwords are renewed regularly. • We store passwords in a way that makes them unintelligible while they are in force.
Physical and Environmental Security	**GE Digital Managed Data Centers.** We use industry standard practices for physical and environmental security. • Physical access is controlled both at the perimeter and at building ingress points by professional security staff utilizing electronic means. • Authorized staff utilize multi-factor authentication mechanisms to access data center floors. • Data center physical access is provided only to approved employees and contractors who have a legitimate business need for such privileges. • Visitors are required to present identification, are logged, and escorted by authorized staff. • When an employee or contractor no longer requires these privileges, his or her access is revoked. • Access privileges are reviewed periodically. Access that is no longer required is removed as part of the review. • Environment controls include fire detection/suppression and protection. • Data center electrical power systems are designed to provide back-up power via generators and Uninterruptible Power Supply (UPS). • Data centers are conditioned to maintain atmospheric conditions at specified levels. **Third Party Data Center Providers.** We obtain "Service Organization Control" (SOC 2) reports for our hosting providers to ensure controls around physical and environmental security meet our data protection standards, where available.

Change Management	**Information System Acquisition, Development and Maintenance** • A Secure Development Lifecycle (SDL) program is contained within our Software Development Life Cycle (SDLC). • Our Cyber Security team provides education, tools, and guidance to support Product Engineering and Development teams. • We have anti-piracy and open-source programs designed to prevent the introduction of counterfeit products or components into our products. **Change Management** • Our change management follows a standard process for changes to GE Digital-managed infrastructure, including data center facilities, networking devices, servers, and other system-level changes we control. • The change management process includes risk assessment, planning, business-defined and Change Advisory Board (CAB) approval, implementation, and closure. CABs meet on a regular basis to review requested changes. **Backup and Capacity** We perform backups of our systems, critical configuration items and components that are used to administer the environment. We validate restoration of data periodically for disaster recovery purposes. Our backup and redundancy processes undergo periodic review and validation.
Operations Management	**Vulnerability Management** We use discovery tools to identify vulnerabilities in the GE Offerings. The vulnerability management processes include risk assessment, communicating findings, remediation guidance that may include identification of available patches, and tracking vulnerabilities through to remediation. In situations where we utilize other Infrastructure as a Service (IaaS) providers, where available, we obtain "Service Organization Control" (SOC 2) reports from providers to ensure controls around vulnerability management meet our standards. **Data Classification and Handling** We classify our data according to a data classification policy and implement controls based upon classification for our data. **Malware Protection** GE deploys malware protection of infrastructure and hosted GE Offerings. Automatic and manual updates are applied to protect against new threats. Data of discovered threats is delivered real-time to our Cyber Incident Response Team (CIRT) for action. **Data Retention** • Data retention policies and procedures are defined and maintained in accordance with regulatory, statutory, contractual, or business requirements applicable to us. We maintain Customer Content as long as necessary to provide GE Offerings based on Customer Agreements. You must inform us with respect to any data retention requirements applicable to the customer data we process as part of the GE Offerings. We provide the capabilities for customers to exercise their rights related to the data we process, as described in our GE Privacy Policy. These include rights to access, update, move etc. as afforded under applicable data protection laws.

	Media Disposal • Data on hard drives and rewritable storage media are disposed of by rewriting over data a minimumof three times. Data on floppy disks, tapes, CD-ROM, and other non–writeable storage media are destroyed securely by disintegration, pulverizing, or shredding. • Customer Content is disposed of in accordance with the Customer Agreement. You are responsible for setting and managing any customer data classification and retention policies and procedures applicable to your Customer Content and informing us of the same.
Technical Control Environment	**Network Security.** Incoming network communications between external networks and our internal GE production network are managed using controls that provide for identification, authentication, authorization, and logging. • Service monitoring includes network access to internal, external, and edge-facing GE Offerings equipment (from the outside in) including, but not limited to, routers, switches, bridges, firewalls, access points, broadband cards, and VPN devices, as well as Systems accessto all IT, Development and Production systems including cloud and external storage. • User identification and authentication is performed at the application level, even if identificationwas made at the network level (unless single sign-on or multifactor authentication has been implemented). **Encryption in Transit.** We utilize a token-based Virtual Private Network ("VPN") to implement multi-factor authentication for remote access connections to the secured GE Digital network. We maintain Transport Layer Security ("TLS") for secure email transmission, Secure File Transfer Protocol ("SFTP") for secure file transfers, and Secure Sockets Layer ("SSL") encryption for secure internet transmissions. **Encryption in Storage.** GE-managed laptops are encrypted using Advanced Encryption Standard ("AES") 256 encryption algorithm. We use a risk-based approach for implementation of encryption at the operating system, database, and application layers, which is implemented by our local Information Security Teams.
Vendor Management	**Onboarding.** We perform an information security assessment of all suppliers and partners that will have access to Customer Content or require a direct GE Digital network connection. On-site assessments are performed as needed based on a risk assessment. We require our suppliers, at a minimum, comply with the level of security in this document applicable to the services they provide. Suppliers deemed to be high risk based on the sensitivity of Customer Content to which they may have access may be required to comply with additional security controls. **Ongoing.** Our suppliers are assessed on an ongoing basis at a frequency determined by their risk rating. Any concerns discovered during an assessment are tracked to resolution. **Off boarding.** When a supplier relationship ends, our suppliers are required to return to us, and/or delete all copies of Customer Content in their possession. Where appropriate, an off-boarding plan is developed that describes how Customer Content is to be removed from the supplier's environment. The plan is reviewed and approved by our IT management team, and with the customer, as appropriate.

Incident Management	Our incident management processes include the detection, triage, reporting, containment, analysis, remediation, and coordination of responses to unauthorized intrusions on networks and assets owned and managed by us as part of the GE Offerings. Our incident management team incorporates cyber threat information into our response plan to help mitigate the effectiveness of future attacks. We assess known threats and customize our enterprise tool suite to address threats across our worldwide network. Our penetration testing team simulates real-world threats faced by us. Our cyber-incident response plan and its elements are tested regularly. Each incident and test is analyzed to determine if changes in existing security practices are necessary. Allreported incidents are logged, and the remedial action indicated. GE Digital employees are required to report all security incidents immediately to the Cyber Incident Response Team (CIRT). Reports of security incidents are escalated promptly. Security breaches are investigated promptly. If criminal action is suspected, the CISO or CIO, in conjunction with our Legal Team and other stakeholders, will determine whether to contact law enforcement, data protection and investigative authorities. Incidents involving personal data are managed in accordance with applicable data protection laws and our GE Privacy Policy.
Business Continuity	We maintain a framework to minimize the impact of business disruptive events on our business operations globally. Our business continuity plans are validated for viability in the event of a business disruptive event.
Compliance and Audit	We maintain a comprehensive framework to govern the control activities for GE Offerings. Changes to the framework are maintained by our Cyber Security team and, where applicable, new or updated controls are implemented and/or evaluated against existing processes. We perform periodic reviews of our processes. Our personnel who violate information security policies, standards or procedures are subject to disciplinary action, up to and including, loss of computer network access, discharge and/or legal action. Other users who violate our policies, standards or procedures are subject to actions that include loss of computer access, termination of contracts, and/or legal action.
Exceptions	Any exceptions to our information security policies or standards must be approved by the CIO or CISO, or appropriate delegate. The exceptions and mitigation plan must be documented.
Standards, Certifications and Audit	We have adopted an ISO 27001-based security governance andcontrols framework for select products and services. Independent external audits are performed at least annually for continued certification under ISO27001. Certificates for GE products and services which are currently ISO-certified will be made available upon request.

3. Customer Security Measures.

This section describes technical and organizational controls required from customers to protect the confidentiality, integrity, and availability of Customer Content you provide to us as part of the GE Offerings and the infrastructure supporting those GE Offerings.

Access Management	• Perform all user administration of your users accessing our hosted GE Offerings. This includes provisioning of unique user IDs and limiting use of shared accounts. • Protect authentication credentials of your users accessing our hosted GE Offerings. • Limit our access to Customer Data to the extent necessary for us to provide GE Offerings, and minimize our processing of Customer Data in accordance with applicable data protection laws.
Security Management	• Protect your infrastructure, including computer systems and equipment used in interactions with us through the use of malicious code prevention software, firewall systems, Intrusion Detection Systems (IDS), Security Incident and Event Monitoring, up-to-date software, and similar tools. • Protect your Application and Programming Interfaces (APIs) used in interactions with us, with securely designed, developed, deployed, and tested APIs in accordance with leading industry standards (e.g., OWASP for web applications).
Data Protection	• Provide classification details of Customer Content provided to us. • Manage retention, corrections, updates, modifications-to and deletion of all Customer Data. • Ensure Customer Data that may legally be transferred to and processed by us and that our access to Customer Data in connection with the Customer Agreement does not violate any laws, regulations or contractual agreements applicable to such Customer Data. • Scan Customer Data for malware or vulnerabilities using industry-standard controls prior to transmission to us and ensuring that Customer Data does not contain any malware or other vulnerabilities. • Enable encryption during data transmissions to the GE Offerings, and encrypt anyfiles hosted on the GE Offerings to meet your needs. • Implement and maintain privacy and security protections for components of the GE Offerings that you provide or control. • Notifying us promptly in the event of an actual or suspected security or privacy incident relating to Customer Data, or compromise of data or systemsrelated to our or your provision or use of the GE Offerings. • Provide data retention requirements applicable to the Customer Data we process as part of the GE Offerings. • Set and manage any data classification and retention policies and procedures applicable to your Customer Content and informing us of the same. •
Laws and Regulations	To the extent you process any of our personal data in the course of receiving the GE Offering under your Customer Agreement, you will comply with all applicable data protection laws, and will only process our personal data in order to perform your obligations under the Customer Agreement in accordance with our documented instructions, or to comply with your legal and regulatory obligations applicable to such data.
Breach Notification	You will notify us as soon as reasonably practicable upon becoming aware of a breach affecting personal data, and, where reasonably practicable, provide a copy of any proposed notification and consider in good faith any comments made by us before notifying any third parties, and provide all reasonable assistance required for us to comply with our obligations under data protection laws.

4. Contact GE Digital.

If you are required to contact us as described in this Data Protection Plan, or wish to contact us for any other reason related to the security or privacy of the GE Offerings or Customer Content, you may contact us asdescribed in the Customer Agreement. For privacy-related inquiries, please see our Privacy Policy.

Version History	Date
v1.0	Dec 2019
v1.1	January 2021
V1.2	March 2023