DATA PROTECTION PLAN:
PREDIX PLATFORM SERVICE AND SECURITY POLICIES

This Data Protection Plan: Predix Platform Service and Security Policies (the "Data Protection Plan" or "Plan") describes the security policies and procedures applicable to the Predix Industrial Internet Platform and related services (the "Service Offerings") provided by GE Digital LLC and GE Digital International LLC ("GE") to the person or entity (the "Customer") who has entered into an agreement with GE for provision of the Service Offerings (the "Customer Agreement").

1. GE Obligations.

1.1 Security. Section 2, Predix Security, describes the business processes and physical, logical, technical and administrative controls used to protect the confidentiality, integrity, and availability of Customer's information, works, content and other digital materials that GE holds and/or processes as part of the Service Offerings ("Customer Data"). Also described are Customer's and its users' obligations with respect to Customer Data. GE reserves the right to add to, modify, or change such policies at any time to meet evolving security requirements, industry standards, or legal requirements, provided that, during the term of service specified in the Customer Agreement, the level of security provided shall in no event be lower than what is in Section 2.

***1.2* Personal Data.** In providing the Service Offerings, GE acts as a data processor of any personal data, as that term is defined under applicable data protection law, that is part of Customer Data, and the Customer remains the data controller of such personal data. GE will act on Customer's instructions with respect to the processing of such personal data, as specified in the Customer Agreement, including this Data Protection Plan.

1.3 Compliance with Law. GE will comply with all laws and regulations applicable to it as the provider of the Service Offerings. GE shall not be responsible for compliance with laws and regulations except those that are generally applicable to information technology cloud platform service providers providing the services described by the Service Offerings.

1.4 Location of Customer Data. Customer Data may be transferred to, stored and/or processed in the United States or other countries in which GE or its affiliates or subcontractors operate. GE will act in accordance with the requirements of the Customer Agreement regardless of where GE stores or processes Customer Data. Upon Customer's reasonable request, GE will negotiate in good faith regarding any further data processing or data transfer agreement as may be required to support the lawful transfer of personal data outside of the European Economic Area in compliance with applicable laws.

1.5 Disclosure of Customer Data.

1.5.1 To Affiliated Entities, Subcontractors and Agents. GE may transfer Customer Data to GE's affiliates globally and to its agents and subcontractors; all such entities will be bound to treat Customer Data in a manner consistent with the Customer Agreement, including this Data Protection Plan, and GE remains responsible for compliance with such requirements by its affiliates, agents and subcontractors.

1.5.2 For Legal Purposes. In addition, GE may disclose Customer Data to companies, organizations or individuals outside of GE if GE has a good-faith belief that access, use, preservation or disclosure of the Customer Data is reasonably necessary to: (a) meet any applicable law, regulation, legal process or enforceable governmental or other request, including a subpoena, judicial, administrative or arbitral order; (b) enforce GE's rights or investigate potential violations of GE's rights; (c) detect, prevent, or otherwise address fraud, security or technical issues; or (d) protect against harm to the rights, property or safety of GE, GE's users, GE's affiliates, or the public as required or permitted by law. Except as otherwise required by law, GE will promptly notify Customer of any subpoena, judicial, administrative or arbitral order of an executive or administrative agency or other government authority (each a "Demand") that it receives that relates to Customer Data. At Customer's request, GE will provide Customer with assistance reasonably required for Customer to respond to the Demand in a timely manner. Customer acknowledges that GE is under no obligation to interact directly with any entity making a Demand.

1.5.3 Reorganization; Mergers & Acquisitions. GE may disclose Customer Data to third parties in connection with any anticipated or actual merger, acquisition, sale, bankruptcy or other reorganization of some or all of its business, subject to an obligation to protect the confidentiality of Customer Data in a manner consistent with the requirements of the Customer Agreement.

1.5.4 Aggregated Data. GE may disclose aggregated information (i.e., in a form in which customers and individuals may not be identified) to any third party.

1.6 Access to Customer Data. For the active subscription term designated under the Customer Agreement, GE will, at its election and as necessary under applicable law, either: (1) provide Customer with the ability to correct, delete, or block personal data contained in Customer Data, or (2) make such corrections, deletions, or blockages of such personal data on Customer's behalf.

1.7 Addressing Security Incidents. As further specified in the Section 2 below, GE evaluates and responds to incidents that create a suspicion of unauthorized access to or handling of Customer Data. GE will inform Customer promptly following its determination that Customer Data has been misappropriated in a manner that compromises its security, integrity or availability.

2. Predix Security

The section describes the functional, technical and administrative controls GE uses to protect the confidentiality, integrity, and availability of Customer Data as part of the Service Offerings. GE's security practices are aligned to the ISO/IEC 27000 framework.

Functional Area	Control
Administrative Controls **(organization, policies, verification, training)**	**Security Organization.** GE's information security program is managed through a cross-functional, coordinated structure that includes GE Business IT, Legal, Audit, HR, Facilities and Corporate Risk. GE IT sets standards for GE's information security and IT risk management program. **Security Policies.** GE has implemented detailed policies, procedures, and technical measures to secure data, systems, and services associated with its services. **Security Oversight.** • **Chief Information Security Officer.** The CISO oversees risk mitigation for the Service Offerings. Responsibilities include developing and maintaining security policies and standards applicable to the Service Offerings; issuing supporting standards, technical security requirements and guidelines, with approval of the ISC (below); and monitoring and enforcing compliance with applicable policies, standards, and contractual and legal requirements. • **Information Security Committee.** GE has established an Information Security Committee (ISC) for the Service Offerings with responsibility to identify areas of concern within the Service Offerings environment and to act as the first line of defense in addressingidentified concerns. This ISC includes the Chief Information Security Officer, the Director of Finance/Audit, and the Chief Information Officer for Predix Services. The ISC may require changes to specific logical controls, training or other measures designed to improve the Service Offerings' security posture. • **Board Audit Committee.** As part of its oversight role, the Audit Committee of GE's Board of Directors reviews annually the Company's practices and programs related to cybersecurity. The Audit Committee is updated regularly on GE's cyber threats and risk-management strategy. As well, information technology risk leaders and information security leaders in each GE Business and at GE Corporate conduct reviews and discuss issues at regular meetings. **Human Resource Security.** Employment candidates, employees, and suppliers are subject to background verification proportional to their roles, as permitted by applicable law. Employees are required to review information security policies, including the acceptable use of GE information resources, before accessing Customer Data. GE employees receive on-going security awareness training and communications.
Asset and Access Management	**Asset Inventory.** GE follows a standard process for controlling the inventory of GE managed devices and equipment ("GE Assets"). This process requires all GE Assets be identified and tracked

	and the asset manager identified. Asset managers are responsible for maintaining up-to-date information regarding their GE Assets. **Access Control.** GE follows a standard process for controlling access to GE managed infrastructure. This process encompasses account and password control, segregation of duties and monitoring, passwords, and entitlement reviews. • GE 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. GE terminates 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 security policies and requirements consistent with this Plan. • A small set of shared administrative accounts are available to System Administrators for emergencies. These accounts are stored in an encrypted Shared Account Password Management (SAPM) 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 8 hours if not checked in prior to expiration. Use of these emergency accounts is logged and reviewed. From an **Access Authorization** stand point: • GE deactivates authentication credentials that have not been used for a period of time not to exceed six months. • GE identifies those personnel who may grant, alter or cancel authorized access to system resources. From an **Authentication** stand point: • GE uses industry standard practices to identify and authenticate users who attempt to access information systems. • Where authentication mechanisms are based on passwords, GE requires that the passwords are renewed regularly. • Where authentication mechanisms are based on passwords, GE requires the password to be at least eight characters long. • GE stores passwords in a way that makes them unintelligible while they are in force. • GE uses industry standard password protection practices, including practices designed to maintain the confidentiality and integrity of passwords when they are assigned and distributed, and during storage.

	Segregation of Duties and Monitoring • GE technical administrators may require super-user access to systems to perform job duties. Each user is given a unique user ID. Password sharing is prohibited. • Quarterly account access review tests are conducted for database and operating system accounts. Application account reviews are conducted by the responsible GE Business. **Password Settings** • Password settings on GE Assets are governed by the password policies at the Corporate or Business level, as appropriate. Initial operating system level password configuration settings are established by GE IT. Once an environment is provisioned to the GE Business, ownership is transferred to the GE Business for ongoing operating system security. GE Businesses are responsible for securing passwords at the application and database levels. • Passwords settings on all GE Assets are required to meet the minimum requirements that include specific character and character-type (e.g., lower-case, upper-case, numbers) specifications, unless compliance with these requirements is not feasible and other mitigating factors exist and have been approved by the GE Businesses Information Security Leader or GE Corporate CISO through an exception process. **Entitlement Reviews** • An automated account reconciliation process is used to identify and remove accounts of any personnel who have separated from GE or belonged to a contractor/supplier who is either no longer employed by the contracting/supplier company or is no longer working onthe GE account. • A manual review process is used to identify and remove accounts of any personnel who have transferred from GE to another organization/role and no longer requires current access levels to the environment.
Physical and Environmental Security	Except where noted, this section applies to data centers that host GE and GE customer data. These data centers are managed by third party organizations. GE obtains "Service Organization Control" (SOC2) reports for these providers to ensure controls around physical and environmental security meet GE's standards. Some of these controls are summarized below: 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 and are signed in 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 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.

	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.
Change Management	**Information System Acquisition, Development and Maintenance** • GE's System Development Life Cycle incorporates information security into each step of the software application development process for applications implemented within GE's managed infrastructure and the embedded systems within its products. GE's Secure Development team provides education, tools, and governance to support Product Engineering and Development teams. • GE has anti-piracy and open source programs designed to prevent the introduction of counterfeit products or components into its software application products and embedded systems within its products. **Change Management** • GE change management follows a standard process for changes to GE managed infrastructure, including data center facilities, networking devices, servers and other system-level changes. • 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. • There are four types of changes subject to change management procedures: Major, Minor, Standard, and Emergency. o *Major Changes* are changes to assets within/associated with GE managed infrastructure that require approval and testing prior to implementation. Major changesrequire review and approval from both the Technical Change Advisory Board (TCAB) andthe Deployment Change Advisory Board (DCAB) prior to implementation. The Planning Stage within the workflow requires completion prior to migration to production; the planner for the change cannot be the same person as the approver for the change. approval of a change is systematically required prior to change implementation. o *Minor Changes* are categorized by limited impact to production services and the ability to adequately test prior to implementation and easily back-out/recover in the event of an issue. Minor Changes must be tested and documented in the implementation, test, and back out plan fields within the ticket. Minor changes require review and approval by the technology manager of the group performing the change. This approval occurs in the TCAB meeting prior to implementation. o *Standard changes* are low risk, low impact pre-approved changes such as adding capacity to a server. During the Standard change management process, the assignment

	team must validate that the change is a standard change. If the change does appear to be a standard change, the assignment team attaches the documentation of the plan in the "pending plan" section of the change ticket. If the documentation is not included, the change is not considered standard and is redirected through the Major and Minor change management process. ○ *Emergency changes* are necessary to address a production issue. Desired completion date and times outside of normal change windows do not qualify as an emergency change unless the change is to occur prior to the next TCAB review meeting. Emergency changes must be tested and documented in the implementation, test, and back-out plan fields within the ticket. Emergency changes may be approved after implementation. **Backup and Capacity** • GE performs system backups of operating systems, recoveries, and offsite tape rotations for critical configuration items or components that are leveraged to administer the environment. GE executes regularly scheduled backups of the GE infrastructure. GE validates restoration of data periodically for disaster recovery purposes. The GE backup and redundancy program undergoes an annual review and validation.
Operations Management	**Vulnerability Management** GE patch and vulnerability management follows a standard process for discovering vulnerabilities and distributing patches applicable to GE-managed infrastructure. This includes implementing a global security program that identifies critical GE Assets, adding them into a vulnerability scanning cycle, communicating findings, and tracking vulnerabilities through to remediation. In situations where we utilize other Infrastructure as a Service (IaaS) providers, GE obtains "Service Organization Control" (SOC2) reports for these providers to ensure controls around vulnerability management meet GE's standards. **Patch Management** GE's vulnerability management program sends out patch update notifications for GE Assets on a monthly basis based on vendor releases. The patch updates focus on critical patches for GEmanaged servers. The focus for GE managed workstations is on any patch rated important or critical. **Data Classification and Handling** GE classifies its data according to the GE data classification policy and implements controls based upon classification. Customers are responsible for classification of their data. See Section 3.3, Regulatory Responsibility. **Malware Protection**

	GE Assets contain Anti-virus ("AV") software to scan for malware. Updates for Data Definition ("DAT") files along with anti-virus quick scans are performed daily. Also, scans are done on read/write of files, along with a weekly full scan to ensure complete coverage of the endpoint. Any threat data that is found is delivered to the Computer Incident Response Team ("CIRT") real-time for action and/or remediation. **Data Retention** Data retention policies and procedures for GE data are defined and maintained in accordance with regulatory, statutory, contractual, or business requirements applicable to GE or applicable GE Businesses. GE provides the necessary capabilities for customers to exercise their rights related to the data they own. These include rights to access, update, move etc. GE maintains customer data as long as necessary to provide necessary services to customer based on contractual agreements. **Media Disposal** Data on hard drives and rewritable storage media are disposed of by rewriting over data a minimum of three times. Data on floppy disks, tapes, CD-ROM, and other non–writeable storage media are destroyed securely by disintegration, pulverizing, or shredding. Customer Data is disposed of in accordance with the Customer Agreement. Customers are responsible for setting and managing any customer data classification and retention policies and procedures.
Technical Control Environment	**Network Security.** Incoming network communications between external networks and the 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 Service 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 access to all IT, Development and Production systems including cloud and external storage. • User identification and authentication is performed at the application level, even if identification was made at the network level (unless single-sign on or multifactor authentication has been implemented). **Encryption in Transit** • GE utilizes a token-based Virtual Private Network ("VPN") to implement multi-factor authentication for remote access connections to the secured GE network. GE implements 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 requires that all GE managed laptops be encrypted using Advanced Encryption Standard ("AES") 256 encryption algorithm. GE uses a risk based approach for implementation of encryption at O/S, database, and application layers, which is implemented by the local GE Business Information Security Teams.
Vendor Management	**Onboarding** GE performs an information security assessment of all suppliers and partners that will have access to GE data or require a direct GE network connection. On-site assessments are performed as needed based on a risk assessment. GE requires its suppliers, at a minimum, to 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 data to which they may have access are required to comply with additional security controls. **Ongoing** 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, suppliers are required to return to GE and/or delete all copies of data in their possession. As well, where appropriate based on the services provided and associated risk, an off-boarding plan is developed that describes how GE data is to be removed from the supplier's environment. The plan is reviewed and approved by GE IT management.
Incident Management	GE's incident response processes include activities to detect, report, contain, analyze, remediate and coordinate responses to unauthorized intrusions on networks and assets owned and managed by GE. GE's incident management team incorporates cyberthreat information into its response plan to help mitigate the effectiveness of future attacks. GE assesses known threat strings and customizes its enterprise tool suite to address threats across GE's worldwide network. GE's pen testing team simulates real-world threats faced by GE. GE's cyber-incident response plan and elements is tested continually (depending upon element, daily or monthly). When a potential cyber-incident is detected, GE conducts an event analysis to determine if there is a problem and if so, how critical. There is a defined reporting and feedback loop. Information Users are required to report all security incidents immediately to the Cyber Security Incident Response Team (CSIRT). Reports of security incidents are escalated promptly

	Each incident is analyzed to determine if changes in the existing security practice are necessary. All reported incidents are logged and the remedial action indicated. The ISC is responsible for training on any procedural changes that may be required as a result of an incident. Security breaches are investigated promptly. If criminal action is suspected, the CISO or CIO, in conjunction with GE Legal, will determine whether to contact law enforcement and investigative authorities.
Business Continuity	GE maintains a framework to minimize the impact of business disruptive events on GE's business operations globally. GE's business continuity plans are validated on a regular basis to ensure that solutions are viable at time of a business disruptive event. • Assignment of key resource responsibilities • Notification, escalation and declaration processes • Recovery time objectives and recovery point objectives • Continuity plans with documented procedures • Training program for preparing all appropriate parties to execute the continuity plans • A testing, maintenance, and revision process
Compliance and Audit	A comprehensive framework governs the control activities within the GE managed infrastructure. Applicable controls are evaluated against the environment for effectiveness and compliance with regulations applicable to GE and GE Businesses. Changes to the framework itself are maintained by the IT risk team and, where applicable, new or updated controls are implemented and/or evaluated against the processes supporting the GE managed infrastructure. GE performs periodic audits and reviews of its corporate managed infrastructure in the form of an SSAE-16. This report is considered confidential and is not released to external parties. GE personnel who violate information security polices, standards or procedures are subject to disciplinary action up to and including loss of computer network access, discharge from GE and/or legal action. Other users who violate Service Offerings 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 GE information security policies or standards must be approved by the CIO or CISO. The exceptions and mitigation plan must be documented.
Customer Obligations	Customer is responsible for: • Managing access by Customer's End Users to GE-managed environments, including providing unique accounts and user IDs where necessary. • Protecting authentication credentials of End Users to access Service Offerings.

	• Limiting GE's access to Customer Data to the extent necessary for GE to provide the Service Offerings. • Protecting its infrastructure, including computer systems and equipment used in interactions with GE, with anti-virus and firewall systems, Intrusion Detection Systems (IDS), Security Incident and Event Monitoring, up-to-date software, and similar tools. • Protecting its Application and Programming Interfaces (APIs) used in interactions with GE, with securely designed, developed, deployed, and tested APIs in accordance with leading industry standards (e.g., OWASP for web applications). • Managing retention and deletion of Customer Data. • Ensuring that Customer Data may legally be transferred to GE and that GE's access to Customer Data in connection with the Customer Agreement does not violate any laws or contractual agreements. • Scanning Customer Data for malware using industry-standard controls prior to transmission to GE and ensuring that Customer Data does not contain any malware. • Enabling encryption during data transmissions to the Service Offerings, and encrypting any files hosted on the Service Offerings to meet Customer's needs. • Implementing and maintaining privacy and security protections for components of the Service Offerings that Customer provides or controls. • Notifying GE promptly in the event of an actual or suspected compromise of data or systems related to GE's or Customer's provision or use of the Service Offerings.
Standards, Certifications and Audit	GE has adopted ISO 27001 / 27002 based Information Security Management System and Cloud Security Alliance based Common Controls Matrix (CSA-CCM) for building a security governance and controls framework. GE security policies and plans are based on ISO 27001 / 270002. GE provides insights as to its own security practices and assessment methodology to ensure the Customer reaches the level of assurance required in order to conduct business with GE. GE is also SOC2 certified. Independent audits are performed at least on an annual basis for third party audit certification under SOC 2 and ISO27001 / 27002. GE can provide these restrictive use report upon request by customers.

3. Customer Obligations.

3.1 Generally. Customer may use and access the Service Offerings only as expressly permitted in the Customer Agreement. GE reserves all other rights with respect to the Service Offerings.

3.2 Compliance. Customer will comply with all laws and regulations, including without limitation privacy and data protection laws, applicable to its use of the Service Offerings and/or toCustomer or Customer's industry that are not generally applicable to information technology cloud platform service providers providing the services specified in the Service Agreement.

3.3 Regulatory Requirements. Customer is responsible for determining whether any of Customer Data is subject to additional regulatory or security requirements beyond those provided by the Service Offerings. Unless otherwise specified in the Service Agreement, Customer may not use the Service Offerings to store or process data subject to specific regulatory requirements, including without limitation healthcare data, export-controlled or other controlled-distribution data under law in the US or elsewhere, payment card data, or classified or controlled government data.

3.4 Usage and Security. See Section 2, Predix Security, Customer Obligations.

4. Contact GE Predix Services

4.1 If Customer is required to contact GE as described in this Plan, or wishes to contact GE for any other reason related to the security or privacy of the Service Offerings or Customer Data, Customer may contact GE at: Contracts.Software@ge.com The process for providing contractual notices is described in the Customer Agreement.

Approval and Ownership

Owner	Title	Version History	Date
Russ Dietz	CSO	v1.0	Dec 2019
Ross McIntyre	CISO	v1.1	In Progress