Third-Party Cyber Security Requirements

Prepared by: Cybersecurity and Technology Risk
Version: 1.1
Effective Date: May 8, 2025

1. INTRODUCTION

The GE HealthCare Third-Party Cyber Security Requirements document outlines the cyber security requirements applicable to GEHC Third Parties, including suppliers and joint ventures. The security requirements outlined herein, are applicable to Third Parties that process, access, interact with, or store GEHC sensitive Information (classified internally as GEHC Confidential or GEHC Highly Confidential), Personal Data or Sensitive Personal Data, have access to a GEHC 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 GEHC, specifically guided by the type of GEHC information the Third-Party Processes, network connection, and products and services provided by the Third-Party, as well as data availability and resiliency requirements.

GEHC reserves the right to update this document from time to time.

2. 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 GEHC 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.

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

GEHC Data includes GEHC Highly Confidential Information, GEHC Confidential Information, Personal Data, Controlled Data or Sensitive Personal Data

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

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

GEHC Trusted Third Party Network means the isolated portion of the GEHC network made available for Trusted Third Parties to connect securely to the GEHC 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 GEHC 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 GEHC 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 GEHC, or from GEHC 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 ThirdParty to correct within the applicable remediation timeframe.

Third-Party or Supplier is the entity that is providing goods or services to GEHC pursuant to the Contract Document. It also refers to GEHC 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 GEHC 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 GEHC, 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 ThirdParty network connected to GEHC internal network in a manner identical to a standard GEHC office.

3. MINIMUM SECURITY REQUIREMENTS

Applicability: The minimum-security requirements are applicable to third parties that process, access or store/host (logically) GEHC Confidential Information.

Minimum Required ISO 27001 Controls	
3.01	8.1 User endpoint devices
3.02	5.9 Inventory of information and other associated assets
3.04	5.11 Return of assets
3.05	5.15 access control
3.06	5.16 Identity management
3.07	5.18 access rights
3.08	8.2 Privileged access rights
3.09	8.3 Information access restriction
3.10	8.5 Secure authentication
3.11	5.17 Authentication information
3.12	8.24 Cryptographic controls
3.13	7.1 Physical security perimeters
3.14	7.2 Physical entry
3.15	7.3 Securing offices, rooms and facilities
3.16	7.5 Protecting against physical and environmental threats
3.17	7.12 Cabling security
3.18	8.31 Separation of development, test and production environments
3.19	8.7 Protection against malware
3.20	8.15 Logging
3.21	8.8 Management of technical vulnerabilities
3.22	8.20 Networks security
3.23	8.22 Segregation of networks
3.24	5.14 Information transfer
3.25	8.26 Application security requirements
3.26	8.33 Test information
3.27	5.19 Information security in supplier relationships
3.28	5.22 Monitoring, review and change management of supplier services
3.29	5.26 Response to information security incidents
3.30	5.35 Independent review of information security
Additional Minimum-Security Requirements	
3.31	Secure configurations for all Third-Party Information System hardware and software shall be established, implemented, and actively managed.
3.32	Network and system vulnerability assessments shall be conducted on an annual basis, at a minimum. Critical vulnerabilities shall be tracked and remediated within 30 days of identification.
3.33	Local accounts shall be disabled if not required or used and shall not be used for privileged access.

3.34	Third-Party shall notify GEHC of any separation or transfer of Third-Party Worker with GEHC Single Sign On (SSO) credentials no later than the day of that event.
3.35	Accounts shall be disabled after 90 days of inactivity, at a minimum.
3.36	GEHC Confidential Information shall not be processed or stored on personal accounts or on personally owned computers, devices or media.
3.37	Third-Party shall not use or provide any products or services to GEHC that are produced by the Kaspersky Lab or the vendors identified on the Entity List (Supplement No. 4 to part 744 of the Export Administration Regulations (EAR)) under the "Country" heading "China, People's Republic of", including but not limited to Huawei, ZTE, Hytera Comms Corporation, Hangzhou Hikvision Digital Tech Company, and Dahua Technology, including their affiliates and subsidiaries.
3.38	All non-GEHC endpoints (laptops, desktops, etc.) that connect to the GEHC network must have, at a minimum, up-to-date antivirus and firewalls installed. The endpoints should also include EDR, DLP, and Encryption.
3.39	If Confidential or Highly Confidential GEHC data is sent via email, the email shall be encrypted using TLS 1.2 or TLS 1.3 (or the latest version of TLS encryption).
3.40	All non-personal accounts (accounts that are used by IT systems, not people) such as service accounts or system accounts shall be managed by an individual or team.
3.41	Network level intrusion detection or prevention system shall monitor on a 24X7X265 basis for "Critical" and "High" alerts.
3.42	If applicable, a web application vulnerability assessment shall be performed on the application that stores, processes, hosts, and/or transmits GEHC data every 12 months.

4. ENHANCED SECURITY REQUIREMENTS

Applicability: The enhanced security requirements are applicable to third parties that process, access or store/host (logically) GEHC Highly Confidential Information, Controlled Data or Sensitive Personal Data.

Enhanced Required ISO 27001 Controls	
4.01	5.1 Policies for information security
4.02	5.2 Information security roles and responsibilities
4.03	5.3 Segregation of duties
4.04	6.1 Screening
4.05	5.4 Management responsibilities
4.06	7.10 Storage media
4.07	5.17 Authentication information
4.08	5.18 access rights
4.09	8.4 access to source code
4.10	7.14 Secure disposal or re-use of equipment
4.11	5.37 Documented operating procedures
4.12	8.32 Change management
4.13	8.15 Logging
4.14	8.19 Installation of software on operational systems
4.15	8.34 Information systems audit controls

4.16	8.32 Change management
4.17	5.24 Information security incident management planning and preparation
4.18	6.8 Information security event reporting
4.19	5.25 Assessment and decision on information security events
4.20	5.27 Learning from information security incidents
4.21	5.34 Privacy and protection of PII
Additional Enhanced Security Requirements	
4.22	Accurate documentation of data flows for all GEHC Highly Confidential Information, Controlled Data, or Sensitive Personal Data resident (permanent or temporary) within the Third-Party's environment shall be maintained.
4.23	Third-Party shall implement Data Loss Prevention (DLP) controls (e.g., disabling of USB ports, DLP software, URL/Web filtering) to detect and prevent unauthorized removal of GEHC Highly Confidential Information, Controlled Data, or Sensitive Personal Data from Third-Party Information Systems.
4.24	Third-Party Information System audit logs shall be centralized and retained for a minimum of 12 months from the time of event or logging, except where prohibited or otherwise required by applicable laws and regulations.
4.25	The Incident Management Plan shall be periodically tested, at minimum annually, (e.g. tabletop test) to verify the soundness of the plan. Tests shall be conducted based on high risk threats to the Third-Party environment (e.g. virus/worm attacks, data compromise, loss of physical assets) and be relevant to the services provided to GEHC.
4.26	Third-Party shall have processes in place to monitor key security metrics. These metrics at a minimum shall include anti-virus agent health, patch and vulnerability management, security baseline configuration management and information security incident management.
4.27	The allocation/resetting of passwords shall be controlled through a formal process. User identity shall be verified prior to password resets. Temporary passwords shall be given to users in a secure manner, with expiration on first use. Knowledge-based authentication resets shall not be used. Password hints shall not be used.
4.28	New passwords shall be checked against a dictionary of known-bad choices, prior to authorizing the user to select their password.
4.29	Third-Party shall implement mechanisms to lock Third-Party workstations after 15 minutes of inactivity, requiring users to re-authenticate. All other Third-Party Information Systems (e.g. application) shall implement mechanism(s) to lock out users after 30 minutes of inactivity.
4.30	The Third-Party shall implement mechanisms to detect and deactivate unauthorized (e.g. rouge) access points.
4.31	Emergency accounts shall only be used in limited situations and have mechanisms in place to allow for traceability to an individual, proper segregation of duties, proper approval, and secure storage of credentials with highly controlled access.
4.32	Third-Party shall use two-factor authentication, at minimum, to access the Third-Party environment remotely. Such transmissions shall be encrypted at a level consistent with industry standards.

4.33	All facilities used to access, process, transmit, and/or store GEHC Highly Confidential Information, Controlled Data, or Sensitive Personal Data, shall have security cameras implemented to monitor the perimeter, entry/exit points, and the interior of the facility. Recordings shall be retained for a minimum of 30 days. All reception areas shall be manned or have other means to control physical access. Server rooms shall be located on the interior of the building with no windows unless safeguards are in place to prevent shattering and unauthorized entry.
4.34	If Active Directory is used, Microsoft best practices for security shall be followed.
4.35	A network based DLP solution shall be implemented to monitor and control inbound and outbound email, network, and application traffic.
4.36	A host-based intrusion prevention system (HIPS) shall be installed on all desktops, laptops, and servers.

5. PHYSICAL SECURITY REQUIREMENTS

Applicability: The physical security requirements are applicable to third parties that host GEHC Confidential Information or store physical documents that contain GEHC Confidential Information.

Note: If GEHC data is only hosted externally (e.g. in a cloud environment) your organization's responsibility is to validate that appropriate security controls are in place at your external (e.g. cloud) hosting provider.

Physical Security Requirements	
5.01	For all facilities used to store GEHC data, badge readers shall be used on all entry points to ensure physical access is restricted to authorized personnel.
5.02	All servers and network equipment used to store GEHC data shall be kept in a secure room with the following controls: 1. Additional access control mechanisms (e.g. badge, biometrics, pin, etc.) on entry doors, 2. Rooms are located on the interior of the building with no windows, unless safeguards are in place to prevent shattering, and 3. Telecommunications equipment, cabling and relays receiving data or supporting services are hidden from view to deter interception or damage?
5.03	For all facilities used to store GEHC data, security cameras shall be implemented to monitor the perimeter, entry/exit points, and the interior of the facility.
5.04	Security camera recordings shall be retained for at least 30 days.
5.05	For all facilities used to store GEHC data, access shall be controlled by a security guard, mantrap, or other means when entering the facility.
5.06	Identification badges shall be issued to all employees, contractors, and visitors and worn always.
5.07	Identification badges shall delineate full time employees from contractors and visitors.
5.08	All physical documents that contain GEHC data/information shall be kept in a locked office, cabinet, or other location which is locked, and access restricted to authorized personnel only.
5.09	Mechanisms shall be in place to notify, investigate, and address potential physical security incidents such as physical intrusion or a stolen asset.
5.10	If all facilities used to store GEHC data are not staffed 24x7x365, alarms shall be installed for off-hour access monitoring.
5.11	If facilities used to store GEHC data are shared with other occupants (e.g. co-located data centre), are protective mechanisms implemented between occupants to prevent unauthorized access to your organizations physical equipment (e.g. locked cage, badge access, etc.)?
5.12	Physical access rights shall be reviewed on an annual basis (at a minimum) and updated as needed to ensure physical access to all facilities used to store GEHC data is restricted to authorized personnel.

6. SOFTWARE DEVELOPMENT

Applicability: The software development requirements are applicable to third parties that provide software that process GEHC Confidential Information.

Software Development Required ISO 27001 Control	
6.01	8.25 Secure development life cycle
6.02	8.29 Security testing in development and acceptance
Additional Software Development Requirements	
6.03	Third-Party shall provide all developers application security training. Developers shall be provided with feedback on the number of common vulnerabilities found along with prevention and remediation measures.
6.04	Information security checkpoints shall be incorporated into the software development lifecycle including, but not limited to. • Risk assessment process. • Documented security requirements • Secure coding guidelines and checklists • Secure design/architecture review • Source code review. • Security testing
6.05	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. A formal report including the scope and results of security testing (including any issues/exceptions) shall be provided to GEHC upon request.
6.06	All Third-Party hosted applications shall be reassessed every two years. Reassessment includes but is not limited to a technical penetration test (manual and/or automated).

7. ENHANCED SOFTWARE DEVELOPMENT

Applicability: The enhanced software development security requirements are applicable to third parties that develop software specific to GEHC's needs that process GEHC Confidential Information.

Enhanced Software Development Required ISO 27001 Control	
7.01	6.3 Information security awareness, education and training
7.02	8.31 Separation of development, test and production environments
7.03	8.30 Outsourced development
Additional Enhanced Software Development Requirements	
7.04	Third-Party shall have a designated application security representative that acts as the primary liaison between Third-Party and GEHC in matters related to secure application development, ensuring that Third Party development teams meet all GEHC requirements for secure application development, and provides to GEHC, upon request, evidence of compliance with requirements listed in this section.
7.05	Prior to the initiation of any project, Third-Party shall request the application's risk classification (Critical vs. non-Critical) and network exposure designation (External or Internal facing) from the GEHC application owner. These risk factors shall be determined prior to the initiation of code development.

7.06	Documented security requirements shall be formally defined for all new development of applications including projects involving significant changes to existing applications with the GEHC designation of “Critical” and/or “External facing”. These requirements shall be developed in collaboration with the GEHC application owner and other key stakeholders as necessary. All secure design requirements shall be documented and maintained with the broader set of application requirements.
7.07	Software development teams shall use GEHC-provided version control processes and tools.
7.08	Application development shall take place in a secured development environment. The development environment shall incorporate the following controls: access Control, Offsite backup, Logical separation between different development environments (e.g. development, staging, testing, etc.), change control for associated systems supporting development environments, approval process for code changes of the application prior to production release, specific permissions and logging of approvals associated with movement of code and test data into and out of the environment.
7.09	Static Application Security Testing (SAST) is required for all applications that are coded in programming language(s) supported by the GEHC solution. The list of languages is available from GEHC Cybersecurity & Technology Risk. If the application source code is not supported by the GEHC-provided solution, then SAST is not required, and only manual code review is necessary.
7.10	All confirmed high/critical vulnerabilities found during manual and automated (SAST) code review, shall be corrected prior to release to GEHC (to include deployment to production). SAST shall be performed utilizing the GEHC-provided solution. If coding is paused or halted, then SAST does not need to be performed until coding is resumed.
7.11	Dynamic application security testing (DAST) is required for all applications that have a browser interface. Shall be conducted prior minimally once prior to the completion of the project. All confirmed critical and high vulnerabilities found during DAST testing, shall be remediated and verified prior to release back to GEHC, to include deployment to production. DAST shall be performed utilizing the GEHC provided solution.
7.12	Security design review shall be incorporated to verify required security features and functionality.
7.13	A threat model is required for all applications that are developed for GEHC.
7.14	Any software developed for GEHC shall not contain any software (proprietary or open source) developed or sold by an entity other than the contracting Third-Party unless approved by GEHC.
7.15	All software delivered to GEHC shall be free of defects/vulnerabilities identified as "critical" or "high” risk. If software shall be delivered with critical or high-risk vulnerabilities, approval from the GEHC business application owner shall be obtained. When requesting approval, the businesses’ application security leader shall be copied on the communication, which shall be in the form of an email.
7.16	If the Third-Party hosted application undergoes Significant Changes or Enhancements, GEHC has the option to perform a technical penetration test (manual and/or automated) prior to the changes being implemented in production. In cases deemed acceptable by GEHC, a Third-Party’s penetration test results shall be leveraged if the report meets GEHC’s quality standards and was conducted within the last 12 months.

8. SYSTEM AND DATA AVAILABILITY

Applicability: The system and data availability requirements are applicable to third parties that Processes, access, or store GEHC Confidential Information that has high availability as defined by GEHC.

System and Data Availability Required ISO 27001 Controls	
8.01	5.37 Documented operating procedures
8.02	8.6 Capacity management
8.03	8.13 Information backup
8.04	5.29 Information security during disruption
Additional System and Data Availability Requirements	
8.05	Third-Party shall maintain a Disaster Recovery Plan (DRP) for all locations and applications used to provide services to GEHC. The DRP shall include the following elements: a. Documented critical business functions, applications and supporting technologies. b. Document what factors trigger a disaster, who is authorized to declare a disaster, and the communication plan, including notification to GEHC. c. Identify alternate locations with the necessary infrastructure to support the recovery needs. d. Document the management and membership of the disaster response and recovery teams. e. Document service level, RTO's and RPO's. f. Document the required recovery actions, identify and ensure the availability of required resources, and compile this information as the recovery plan. g. Identify critical technology service provider dependencies and recovery support capability.
8.06	If Third-Party provides a SaaS service, Third-Party shall provide GEHC with geographically resilient hosting options. Third-Party shall have more than one provider for each service for which there is a service delivery dependency.
8.07	The disaster recovery plan must be reviewed and signed off every 12 months. Lessons learned should be captured as part of the disaster recovery exercise.
8.08	All data retention requirements should be documented and approved by GEHC.

9. CLOUD SECURITY

Applicability: The cloud security requirements are applicable to Third-Party that host a cloud computing application (in a SAAS, PAAS, IAAS, or DRAAS environment) that Processes GEHC Confidential Information, or the third-party provides a cloud computing platform that allows GEHC to develop, run, and manage applications, or the third party is responsible for the management of virtual machine image and/or hypervisor.

Cloud Security Requirements	
9.01	Root/administrator access to the management console shall require multi-factor authentication.
9.02	Dedicated secure networks shall be separate from customer production infrastructure, leveraged to provide management access to the cloud infrastructure.
9.03	Third-Party supplier shall have the ability to provide logs which are specific to the instances used for GEHC / GEHC engagement.
9.04	Third-Party supplier shall enable console and resource level logging across regions in the cloud infrastructure.
9.05	All logs in the cloud environment shall feed into a central log aggregation tool.

9.06	Third-Party supplier shall regularly back up application configuration, data within the application, database and configuration of systems within cloud infrastructure to ensure that data can be restored if needed.
9.07	Third-Party supplier shall retain the original structure and format of data residing within the cloud application for easy movement to another cloud solution / cloud service provider.
9.08	Third-Party supplier shall support federated authentication (e.g.: SAML) or are standards-based identity protocols (e.g. OpenID Connect, OAuth2, etc.) leveraged for propagating and enforcing identity controls through the SaaS and API.
9.09	Third-Party supplier shall have cryptographic controls implemented to make sure that GEHC data at rest within cloud infrastructure is always encrypted (e.g.: AES-256).
9.10	Third-Party supplier shall have mechanisms in place to control encryption key generation, distribution, storage, access and destruction.
9.11	Third-Party supplier shall have access to management consoles and cloud application(s) restricted through Role Based access Control & based on the least privilege principle.
9.12	If keys (e.g.: access key, secret key for cloud accounts or ssh keys used for managing cloud instances) are used for managing the cloud infrastructure; the Third-Party vendor shall keep in a protected vault with access controls.
9.13	Third-Party supplier shall have a cyber incident management program in place wherein the cyber events/incidents are evaluated, contained, remediated, and responded to.
9.14	Third-Party supplier shall have a patch management process for (cloud infrastructure hosting or storing or processing or transmitting GEHC data) identifying and applying all relevant vendor patches and security updates within 30 days of release by vendor.
9.15	Third-Party supplier shall have the root/administrator account credentials vaulted.
9.16	A web application vulnerability assessment or penetration test shall be performed on the cloud application(s) hosting, storing, processing and/or transmitting GEHC data, in the last 12 months.
9.17	A network vulnerability assessment shall be performed on the cloud instances and systems (servers, databases, networking components/devices) which store, process, host, or transmit GEHC data within the last 12 months.
9.18	Third-Party supplier shall have application support for both single tenancy and multi-tenancy deployment.
9.19	Third-Party supplier shall support web application firewall (WAF) implementations which comply at minimum with the OWASP top 10 risks.
9.20	Third-Party supplier shall have controls in place to ensure non-public exposure of data, including but not limited to S3 buckets and Elasticsearch.
9.21	Third-Party shall have audits to monitor for configuration drift.
9.22	Third-Party shall have controls to automatically shut down publicly exposed data.

10. DATA CENTER SECURITY

Applicability: The data centre security requirements are applicable to third parties that provide data centre facility services.

Data Centre Security Required ISO 27001 Controls	
10.01	7.5 Protecting against physical and environmental threats
10.02	7.2 Physical entry
10.03	7.8 Equipment siting and protection
10.04	7.11 Supporting utilities
10.05	7.13 Equipment maintenance
10.06	8.14 Redundancy of information processing facilities
Additional Data Centre Security Requirements	
10.07	Data centre walls shall be resistant to fire or explosions.
10.08	Data centres with glass windows are not allowed unless shatter proof and impact resistant barriers are in place.
10.09	Physical data centre access rights shall be reviewed at a minimum quarterly using a documented process.
10.10	All data centres shall have professionally installed intrusion alarm systems monitored by either a contracted security monitoring service or by members of the local security team within the building. All ingress points shall be alarmed and monitored. The alarm system shall be capable of continuous operation in the event of a loss of power.
10.11	Emergency doors shall have audible alarms and display appropriate signage.
10.12	Upon entrance to the data centre, access shall be restricted to only the areas the person needs access to. Both ingress and egress points shall be controlled and monitored 24x7x365 to minimize tailgating and provide detailed location logging. Logs shall be retained for a minimum one year from time of event or logging, except where prohibited or otherwise required by applicable laws and regulations. Logs relevant to pending or foreseeable litigation, investigation or audit (even when not subject to a formal document retention notice) shall be preserved as directed by GEHC. Visitors shall be escorted or observed at all times.
10.13	Closed-Circuit Television (CCTV) systems and appropriate signage shall be in place on the exterior and all datacentre floor entry points. Cameras shall be monitored during operational hours and be retained for a minimum 30 days.
10.14	Management of security alarms, entrance control, environmental controls, & CCTV systems shall be physically and logically restricted to staff responsible for these functions.
10.15	All entrances of the building containing the data centre shall be designed to block entering the building interior or boarding elevators without first undergoing a manned identification check. The main entrance accessible to the public shall be manned 24/7. Multiple secured entrances shall exist between public and data centre floor area.
10.16	Assets containing GEHC Confidential Information shall be caged off physically from the rest of the data centre. The cage shall utilize the main security card access control system with multi factor authentication or a controlled key process. Cages shall be real floor to real ceiling to prevent unauthorized entry. Cages shall be designed to prevent intrusion or breach from outside of the cage. Finally, cages shall have a camera covering the entrance and be wired into the internal 24x7x365 CCTV system.

10.17	Anyone requiring badge access to any computer room shall follow a defined procedure approved by the Third-Party including the badge holder's name, badge number, computer room location, reason access is needed, and termination date for a fixed duration. The Third-Party security office shall not configure any badge for computer room access without being authorized by the Third-Party or designated team members.
10.18	The building exterior shall be periodically checked by scheduled security walk-throughs. Suspicious packages, activities, vehicles and/or people shall be investigated.
10.19	Data centre parking area shall have physical obstacles in place to reduce risk of vehicle or car bomb penetrating exterior walls.
10.20	All data centre workers shall be trained in control and storage of combustible materials (including paper and cardboard), and on the correct processes to follow when detecting a fire.
10.21	Server rooms shall not be used for storage and shall be clear of all unnecessary equipment and material not in use.
10.22	Detective monitoring and controls shall be implemented to mitigate the risk of overhead water sources impacting the IT equipment. Water detection shall be placed near air conditioners and any other water sources at the lowest level of the room.
10.23	Multiple methods of early fire detection shall be implemented and monitored 24X7x365 including smoke and temperature detection.
10.24	All data centres shall have a fire suppression system.
10.25	Loading bays and docks shall have CCTV coverage that provides a clear head-on view of the vehicle. This view shall be positioned to enable recognition of the driver, make of vehicle and registration number plate. The doors from the holding area into the data centre shall conform to the interior security requirements for entrance to the data centre. The movement, delivery or removal of any material or equipment into and out of the facility shall be recorded.
10.26	All switches and/or controls, which permit emergency shutdown of vital systems, shall have physical protection, audible alarm and signage to avoid accidental activation.
10.27	Third-Party shall ensure that all computer devices are connected to surge protectors to protect them against spikes and surges in the electrical power supply.
10.28	Third-Party shall ensure that backup power supply is available in the form of local generator(s).
10.29	Third-Party shall ensure that all electrical and mechanical infrastructures are maintained per manufacturer specifications.
10.30	Emergency lighting, powered by a supply other than the main power, shall be implemented throughout the data centre in accordance with local fire and health and safety regulations. Emergency lighting shall be activated when the fire alarm is raised, or when a degradation of power prevents the standard lights from operating.
10.31	The data centre shall have systems in place to control and monitor temperature and humidity, air conditioning system to control air quality and minimize contamination. Server room temperature shall be controlled and monitored within the range of 18 - 27°C. Server room humidity shall be controlled and monitored within the range of 40-60% relative humidity.
10.32	The data centre shall have air conditioning systems with separate zones for standard working areas, and areas containing equipment such as server rooms.
10.33	The air conditioning system supporting server rooms shall have dust filtration systems in place and shall be reviewed periodically to ensure air quality does not degrade / contamination increases.
10.34	Server rooms shall have positive pressurization to minimize contaminants entering these areas.

10.35	A process shall be in place for scheduled testing and maintenance of all critical data centre infrastructure including security, power & environmental systems. Repairs or modification to facility security components (e.g. doors, locks, walls, hardware) shall be documented.
10.36	Critical data centre infrastructure including power & environmental systems shall be engineered to function through an operational interruption. The design shall be a minimum of N+1. IT equipment with multiple power supplies shall leverage the redundant power infrastructure.
10.37	The data centre access control system, and doors, shall be designed to maintain operation during scenarios such as: The failure of the access control application or hardware platform and a utility power outage.
10.38	All GEHC equipment shall be properly mounted in appropriately sized racks which are ground and/or ceiling mounted in accordance with local earthquake guidelines. Racks shall be labelled. Equipment in racks as well as cables into racks shall also have labels.
10.39	New equipment shall be stored in a secured area. Third-Party personnel shall inspect the box for tampering before opening. Movement of used equipment containing GEHC Data shall be done under the supervision of Third-Party personnel via a security approved process.
10.40	Third-Party shall have a documented equipment or media delivery or handling process.
10.41	Data centres shall have a disaster recovery plan for the facility and environmental that at least identifies and mitigates risks to GEHC services in the event of a disaster. The plan shall provide for contingencies to restore facility service if a disaster occurs, such as identified alternate data centre sites. The plan shall be shared with GEHC to ensure GEHC can coordinate with its own DRP.
10.42	Data centres shall conduct an electrical blackout test, at least annually, to validate continue functionality through an operational interruption. Additionally, the data centre shall participate and support GEHC DRP and associated testing.
10.43	All GEHC equipment shall be completely network segregated from non-GEHC parts of the data centre.

11. DIRECT NETWORK CONNECTIVITY SECURITY

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

Direct Network Connectivity Security Requirements	
11.01	Third-Party shall use only GEHC managed network devices to connect to the Trusted Third-Party connection. GEHC requires out of band connectivity to the remote device for administration.
11.02	Third-Party shall implement a firewall between the third-party parent network and the Trusted Third-Party network. The firewall shall be managed by GEHC and configured to allow only the connections authorized by GEHC.
11.03	GEHC conducts periodic scans on all GEHC IP addresses. If GEHC notifies the Third-Party of any confirmed high or critical vulnerability found, the Third-Party shall remediate the confirmed vulnerability within 30 days. The Trusted Third-Party shall ensure that nothing will be placed in line to limit the ability for GEHC to perform vulnerability scanning of the Trusted Third-Party network.
11.04	All internet traffic shall be directed to a GEHC managed external proxy.
11.05	Remote access to the Trusted Third-Party network is only allowed through the GEHC Virtual Private Network (VPN) hub infrastructure with two-factor authentication.

11.06	GEHC managed network equipment shall be housed in a caged environment and/or be physically separated from the Third-Party equipment. Third-Party shall ensure that the network equipment is locked, and access is limited to GEHC approved Third-Party Workers and approved GEHC employees. The Third-Party shall also maintain a listing of all individuals that have access to equipment.
11.07	The Trusted Third-Party shall ensure that its employees will not bridge the Trusted Third-Party network with the non-Trusted Third-Party parent network. There shall not be physical or logical connectivity to any network other than the GEHC network. The business network of the Third-Party shall not share any layer-2 switches or network devices with GEHC except for the terminating firewall.
11.08	Third-Party shall ensure that all wireless deployments on Trusted Third-Party networks follow the GEHC Third-Party network change request process and are configured/managed by GEHC.
11.09	All unused switch ports shall be disabled on network equipment. In addition, all new connection requests shall be submitted to GEHC.

12. PRODUCT SECURITY

Applicability: The product security requirements are applicable to third parties that provide any Products (as defined below) under the Contract Document that include executable binary code. The product security requirements are also 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	
12.01	Supplier shall ensure all Products have been developed in accordance with principles of secure software development consistent with software development industry best practices, including, security design review, secure coding practices, risk-based testing and remediation requirements. Supplier's software development environment used to develop the Products must have security controls that can detect and prevent attacks by use of network layer firewalls and intrusion detection/prevention systems (IDS/IPS) in a risk-based manner.
12.02	Supplier shall implement processes to ensure malware protection measures are implemented for the Products development environment and relevant assets.
12.03	The Supplier shall have a process to ensure the systems used in Products development environment(s) are properly and timely patched.
12.04	Supplier shall include cybersecurity guidance in the Product documentation provided to GEHC. This documentation shall include guidance on how to configure the Products and/or the surrounding environment to best ensure security. It shall also include guidance on which logical or physical ports are required for the product to function. If authentication is used to protect access to any service or capability of the Products, regardless of the intended user of that service/capability, the Supplier shall ensure: (i) Products shall not provide access to that service or capability using a default account/password (ii) Products shall be configured with least privilege for all user accounts, file systems, and application-to-application communications, examples of file systems which implement file protection based on privileges are *nix and NTFS; (iii) Products shall not provide access to that service or capability using "Backdoor" account/password; (iv) Products' associated authentication and password change processes shall be implemented with an appropriately secure cryptographic level; and (v) GEHC shall be able to change any passwords supported by the Products.

12.05	Services or capabilities that are not required to implement the Product's functionality shall by default be disabled or shall require authentication to protect access to this service or capability.
12.06	If any wireless technology is incorporated in any Product, Supplier shall document that the wireless technology complies with standard operational and security requirements specified in applicable wireless standard(s) or specification(s) (e.g., applicable IEEE standards, such as 802.11).
12.07	In the event that any cryptographic systems are contained in the Product, Supplier shall only use cryptographic algorithms and key lengths that meet or exceed the most current version of the National Institute of Standards and Technology (NIST) Special Publication 800-131A, and Supplier shall provide an automated remote key-establishment (update) method that protects the confidentiality and integrity of the cryptographic keys.
12.08	A list of all high-risk technologies (e.g. Huawei, ZTE, Kaspersky) used in the Product development process shall be maintained by the vendor. High risk technologies shall not be used in Products developed for GEHC unless prior approval is obtained from GEHC.
12.09	Supplier must develop and maintain an up-to-date Cybersecurity Vulnerability management plan designed to promptly identify, prevent, investigate, and mitigate any Cybersecurity Vulnerabilities and perform any required recovery actions to remedy the impact.
12.10	Supplier shall notify GEHC within a reasonable period, in no event to exceed five (5) business days after discovery, or shorter if required by applicable law or regulation, of any potential Cybersecurity Vulnerability. Supplier shall report all critical Cybersecurity Vulnerability that would have a significant adverse effect on GEHC and any Cybersecurity Vulnerability with a fix to GEHC at 3PS.GEHCSECURITY@gehealthcare.com with "PSIRT" in the subject line, or at such contact information communicated to Supplier from time to time. Within a reasonable time thereafter, Supplier shall provide GEHC, free of charge, with any upgrades, updates, releases, maintenance releases and error or bug fixes necessary to remediate any Cybersecurity Vulnerability. Supplier shall reasonably cooperate with GEHC in its investigation of a Cybersecurity Vulnerability, whether discovered by Supplier, GEHC, or a Third-Party, which shall include providing GEHC a detailed description of the Cybersecurity Vulnerability, the remediation plan, and any other information GEHC reasonably may request concerning the Cybersecurity Vulnerability, as soon as such information can be collected or otherwise becomes available. GEHC or GEHC's agent shall have the right to conduct a cybersecurity assessment of the applicable Products, and the Product development lifecycle, which includes tests intended to identify potential cybersecurity vulnerabilities. Supplier shall designate an individual responsible for management of the Cybersecurity Vulnerability and shall identify such individual to GEHC promptly.
12.11	The Supplier shall have a process to ensure appropriate physical and digital security mechanisms are in place, including, but not limited to, (i) allowing access to GEHC's components' environment only to personnel cleared by both supplier and GEHC; (ii) the use of tamper evident seals on media and containers, to detect unauthorized access to protected products (e.g. tamper evident labels or seals, which selfdestruct and leave a residue sticker if removed); and (iii) tamper-resistant production (e.g. digital signatures for software and corresponding hardware mechanisms).
12.12	Open Source Software and Third-Party Materials Warranty. Supplier represents, warrants and covenants that (i) it has disclosed all Open Source Software and Third-Party Materials utilized with the Products, and no Open Source Software or Third-Party Materials have been or will be provided to GEHC or used as a component of or in relation to any Products provided under the Agreement, except with the prior written authorization of GEHC; and (ii) all Open Source Software contained within the Products are and shall be in material compliance with the terms and conditions of the applicable licenses governing their use, and the Products or the use thereof by GEHC shall not cause GEHC or GEHC's intellectual property rights to be subject to the terms or conditions of a Copyleft License, or require GEHC to fulfill any open source license obligations for any Open Source Software contained within the Products.

12.13	Code Integrity Warranty. Supplier represents, warrants, and covenants that the Products: (a) do not contain any restrictive devices such as any key, node lock, time-out, time bomb, or other function, whether implemented by electronic, mechanical, or other means, which may restrict or otherwise impair the operation or use of the Products or any material embodying or comprising Products; and (b) shall be free of viruses, malware, and other harmful code (including, without limitation, time-out features) which may interfere with the use of the Products regardless of whether Supplier or its personnel purposefully placed such code in the Products. In addition to exercising any of GEHC's other rights and remedies under this Agreement or otherwise at law or in equity, Supplier shall provide GEHC, free of charge, with any and all new versions, upgrades, updates, releases, maintenance releases, and error or bug fixes of the Products (collectively, "Revised Code") which prevents a breach of any of the warranties provided under this Agreement or corrects a breach of such warranties. Revised Code contained in the Products constitutes Products for purposes of this Agreement.
12.14	Supplier shall obtain Technology Errors & Omissions Liability Insurance, with a minimum limit of USD $5,000,000 per claim and in the aggregate, covering all Products including failure of IT security and data privacy breach and software copyright infringement. If coverage is on a claims-made basis, the policy must contain a retro date which precedes the effective date of this Agreement and continuity must be maintained for 1 year following termination or expiration of this Agreement.
12.15	A product security leader and enterprise security architects shall be designated to support in the execution of the product security program and resolution of cyber threats.
12.16	All software and firmware components shall undergo a Static Application Security Test SAST) and have all critical and high vulnerabilities been remediated in the product version that GEHC will purchase. Note: This can be done on the source code or binaries.
12.17	A Dynamic Application Security Test (DAST) shall be performed on all external interfaces.
12.18	Penetration testing shall be performed on the component(s) that GEHC is purchasing.
12.19	Remote access of the component shall be configured to limit the number of concurrent remote sessions.
12.20	Remote access of the component shall be configured to automatically terminate a user session after a predefined time period of inactivity.
12.21	The component shall have audit logging capability, such as successful and failed login records, time, duration of user logged etc.
12.22	The component shall have built-in mechanism to prevent normal users to access logs other than administrators.
12.23	The component shall have ability to store audit logs for at least 180 days.
12.24	The component shall have ability to transfer audit logs to external systems like Syslog servers.
12.25	The component shall use internal system clocks to generate time stamps for audit records.
12.26	Your organization shall have a product security incident response policy that address purpose, scope, roles, management commitment, coordination among organizational entities and has compliance been documented and disseminated to all employees working within product development, program, project, or management staff roles.
12.27	The product security incident response capability shall be tested on at least yearly basis using tabletop exercise, automated simulations and incident test plans to determine the incident response effectiveness and documents the results.
12.28	Your organization shall receive security alerts, advisories and directives from network vendors and the US-CERT on an ongoing basis and generate internal security alerts, advisories and directives as deemed necessary.

12.29	Your organization shall have a role specific cyber security awareness and training plan that identifies the training needed to develop and maintain a culture of product security integrity, and the expertise necessary to perform product security activities effectively and consistently to design secure products.
12.30	Your organization shall review the current security awareness and training policy annually and update it every three years at a minimum.
12.31	Your organization shall provide role-based security training to employees before authorizing access to the system used to develop the product and on an annual basis after.
12.32	Your organization shall document and monitor individual information system security training activities including basic security awareness training and role-based security training and retain individual training records for at least two years.
12.33	Your organization shall require your suppliers to adhere to product cybersecurity requirements consistent with this requirements document.
12.34	Your organization shall perform periodic security reviews and/or on-site audits/assessments of suppliers to ensure that the security controls of all third-party suppliers are consistent with your organizational security policies and as per contract with your organization and the supplier.
12.35	Your organization shall have a documented secure development life cycle standard that sets forth the following requirements for the product GEHC is purchasing:1. product inherent risk assessment, 2. security plan,3. define security requirements, 4. architect security solution, 5. implement security solution, 6. perform residual risk assessment, 7. maintain product inventory,8. product life cycle consideration, 9. continue deployment compliance.
12.36	Coding standards shall be established that address known vulnerabilities in the programming languages and frameworks used in the component that GEHC is purchasing.
12.37	A plan shall be developed that identifies the applicable software development lifecycle objectives and customer / regulatory cybersecurity requirements.
12.38	The component that GEHC is purchasing shall undergo a threat modeling exercise to assess and document the components inherent security risks.
12.39	Security requirements and assumptions shall be documented to provide the measures necessary to mitigate each threat identified during the threat modeling exercise.
12.40	Have a base set of security requirements been defined with best practices and lessons learned appropriate for technologies and use cases that are to be implemented for all projects.
12.41	A security architecture shall be developed and documented for the component that GEHC is purchasing.
12.42	A digital obsolescence and end-of-life strategy shall be developed and executed for digital components and covered products which achieves the following: 1. communicates PLCs to relevant stakeholders, including customers ,2. addresses the risk posed by PLCs through an appropriate risk remediation: mitigate, accept, transfer, or ‘End of Life' process.
12.43	A continued deployment compliance plan shall be developed which includes the schedule and scope of reoccurring validation.

13. RESILIENCY SECURITY REQUIREMENTS

Applicability: The resiliency security requirements are applicable to suppliers who have a critical impact on GEHC operations or production of critical products.

Resiliency Security Requirements	
13.01	The information security incident management plan shall be reviewed and updated.
13.02	Your organization shall identify the stakeholders and assigned roles & responsibilities to staff for carrying out the activities described in the security incident management plan.
13.03	Your organization's security incident management process shall capture the following aspects: 1. Categorization of security events 2. Analysis of security events to determine if they are related to other events 3. A method to prioritize the security events 4. Record and track the status of all security events "Does your organization's security incident management process capture the following aspects? 1. Categorization of security events 2. Analysis of security events to determine if they are related to other events 3. A method to prioritize the security events 4. Record and track the status of all security events 5. Review the remediation activities performed for security events to make sure they are tracked down to proper resolution.
13.04	There shall be a process to ensure that security event evidences are identified, collected and handled as required by law or other obligations (rules, laws, regulations, policies etc.).
13.05	There shall be a process by which incidents are escalated to stakeholders for input and resolution.
13.06	Incident status and responses shall be communicated to affected parties (including public relations staff and external media outlets).
13.07	There shall be a link between the incident management process and other related processes (problem management, risk management, change management, etc.).
13.08	The lessons learned from incident management shall be used to improve asset protection and service continuity strategies.
13.09	Risks related to the performance of incident management activities shall be identified, analysed, disposed of, monitored, and controlled.
13.10	There shall be management oversight of the performance of the incident management activities.
13.11	Service continuity plans shall be stored in a controlled manner and available to all those who need to know.
13.12	Mechanisms (e.g., failsafe, load balancing, hot swap capabilities) shall be implemented to achieve resilience requirements in normal and adverse situations.
13.13	Stakeholders for service continuity activities shall be identified and made aware of their roles.
13.14	There management oversight of the performance of the service continuity activities.

13.15	Your organization shall have a documented plan for external dependencies/relationships (service providers, suppliers, vendors, partners, consultants, outsourcing partners etc.) management including but not limited to: 1. Identification of all external dependencies/relationships which are critical to the services provided to GEHC 2. Maintaining an active inventory of all external dependencies related to the services provided to GEHC 3. Prioritizing the list of external dependencies 4. Identifying the stakeholders related to external dependency management activities 5. Establishing roles & responsibilities for stakeholders related to external dependency management activities 6. Implementing guidelines and processes associated with external dependency management activities
13.16	There shall be an established process to identify, analyse and manage the risks arising from external dependency/relationship management
13.17	Your organization shall have a documented plan for external dependencies/relationships (service providers, suppliers, vendors, partners, consultants, outsourcing partners etc.) management including but not limited to: 1. Identification of all external dependencies/relationships which are critical to the services provided to GEHC 2. Maintaining an active inventory of all external dependencies related to the services provided to GEHC 3. Prioritizing the list of external dependencies 4. Identifying the stakeholders related to external dependency management activities 5. Establishing roles & responsibilities for stakeholders related to external dependency management activities 6. Implementing guidelines and processes associated with external dependency management activities
13.18	The performance of external dependencies/relationships monitored against resilience requirements.
13.19	Corrective actions shall be taken to address performance issues (as related to resiliency requirements) arising from external dependencies/relationships and tracked until resolution.
13.20	Infrastructure providers on which the critical service depends (telecommunications and telephone services, energy sources, etc.) shall be identified.
13.21	External dependency/relationship management activities shall be periodically reviewed and measured to ensure they are effective, producing the intended results and adhering to the plan.
13,22	There shall be management oversight of the performance of the external dependency management activities.
13.23	Responsibility for monitoring sources of threat information shall be assigned.
13.24	Threat monitoring procedures shall be implemented.
13.25	Resources shall be assigned and trained to perform threat monitoring.
13.26	Internal stakeholders (such as the critical service owner and incident management staff) shall be identified to whom threat information must be communicated.
13.27	External stakeholders (such as emergency management personnel, regulatory, and information sharing organizations) shall be identified to whom threat information must be communicated.
13.28	Threat information shall be communicated to stakeholders.
13.29	Resources shall be assigned authority and accountability for communicating threat information.
13.30	Resources shall be trained with respect to their specific role in communicating threat information.

14. OPERATION TECHNOLOGY (O.T) / MANUFACTURING SECURITY REQUIREMENTS

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

Operational Technology Security Requirements	
14.01	All hardware and software assets in your manufacturing environment shall be recorded and tracked in an asset inventory system.
14.02	All assets in your manufacturing environment shall be contained in a locked facility or one that is badge access controlled.
14.03	All system drives and media in your manufacturing environment shall be scanned for malware prior to being used.
14.04	All asset operating systems, software, and firmware in your manufacturing environment shall be maintained with the latest security patches/updates.
14.05	All assets in your manufacturing environment shall be scanned for malware bi-annually, at a minimum.
14.06	All assets that are network accessible (directly or via another connected system) in your manufacturing environment shall be protected using a dedicated, centrally managed, and monitored, firewall.
14.07	Removable media such as USB devices, external hard drives, floppy disks, or compact disks shall be safeguarded if used in your manufacturing environment.
14.08	An owner shall be assigned to every removable media.
14.09	All removable media devices used in your manufacturing environment shall be owned and issued by your company.
14.10	All removable media devices shall be scanned for malware before being used in your manufacturing environment.
14.11	All remote-control capable software within your manufacturing environment shall be registered for use through a software request and licensing process and approved for use before being utilized.
14.12	All individuals who remotely access assets in your manufacturing environment shall use unique ID and passwords.
14.13	All individuals who remotely access assets in your manufacturing environment shall be required to authenticate using a username and password, at a minimum.
14.14	All highly privileged users (e.g. System Administrators) who remotely access assets in your manufacturing environment shall be required to use two factor authentications, at a minimum.
14.15	All remote network connections to devices/equipment within your manufacturing environment shall be encrypted using AES 128, 192, or 256.
14.16	Firewall restrictions shall be in place to limit remote connections to authorized endpoints only.
14.17	All assets that have data storage media shall be securely sanitized or destroyed prior to the asset leaving your company's custody or being redeployed to another site.
14.18	All assets in your manufacturing environment shall be monitored for abnormal/malicious activity.
14.19	Your organization shall have a documented information security incident management plan for your manufacturing operations and assets that includes the following aspects:1. Reporting (internal and external mechanisms to raise potential incidents),2. Preparation (procedures, checklist, communication plan including legal/governmental authorities and regulatory authorities if applicable),3. Identification (methods in place to report incidents, severity assessment),4. Containment (log recording steps, evidence collection),5. Eradication (root cause analysis),6.

	Recovery (system recovery steps),7. Lessons learned (incident reports), and8. Tracking (inventory of incidents, workflows, status, outcome).
14.20	Your organization shall conduct periodic tests, at minimum annually, of the incident management plan in order to verify that users have been properly trained and the plan can be carried out effectively if needed. Note: A tabletop test is an example of what constitutes proper incident management plan testing. Further, the tests must be conducted based on high risk threats to your organization's environment (e.g. virus/worm attacks, data compromise, loss of physical assets).
14.21	If your manufacturing operations were adversely impacted due to a cyber incident, your organization shall have the capability to notify GEHC of a breach or unauthorized access to GEHC data within 72 hours of identification.
14.22	Business continuity and disaster recovery plans for your manufacturing environment shall be developed and documented.
14.23	Your organization shall 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.
14.24	Your organization shall capture and retain backups of manufacturing system software and firmware assets where possible.
14.25	Your organization shall implement a change control and a change notification process for manufacturing hardware, software, and firmware assets.
14.26	The change control and notification process shall be managed in a central system.
14.27	Your organization shall use 3rd party software, firmware, or hardware in your manufacturing environment.
14.28	A list of the 3rd parties and the software, firmware, or hardware that is used shall be documented.
14.29	3rd parties that have remote access to any assets within your manufacturing environment shall be managed and periodically reviewed for accuracy.

15. SECURITY CONTROL APPLICABILITY MATRIX

Applicability	Minimum Security	Enhanced Security	Physical Security	Software development	Enhanced Software Development	System and Data Availability	Cloud security	Data Center	Direct Network Connectivity Security	Product Security	Resiliency Security Requirements	Operation Technology (O.T) / Manufacturing Security Requirements
Process, access, or store/host (logically) GEHC Confidential Information	X											
Process, access, or store/host (logically) GEHC Highly Confidential Information	X	X										
Host GEHC Confidential Information or store physical documents			X									
Provide software that process GEHC Confidential Information				X								
Develop software specific to GEHC's needs					X							
Services or Data that require high availability as defined by GEHC						X						
Utilizes Cloud Technology (SAAS, PAAS, IAAS)							X					
Provide data centre facility services.								X				
Have a GEHC Trusted Third-Party network connection.									X			
Provides a digital component to be utilized in a GEHC Product										X		
Supplier has a critical impact on GEHC operations or production of critical products											X	
Manufactures products, components or materials for GEHC												X