Third Party Information Security Requirements

Prepared by: Cybersecurity and Technology Risk

Version: 1.0

Effective Date: April 1, 2019

1. INTRODUCTION

The Current Third Party Information Security Requirements document outlines the security requirements applicable to Current Third Parties, including suppliers and joint ventures. The security requirements outlined herein, are applicable to Third Parties that Process Current Confidential Information, have access to a Current Information System, or provide certain services/products, as described below. The security requirements are designed to vary based on the level of risk the Third Party presents to Current, specifically guided by the type of Current information the Third-Party Processes, network connection, services provided by the Third Party, and data availability requirements.

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

2. MINIMUM SECURITY REQUIREMENTS

Applicability: Third Party Processes Current Confidential Information or Personal Data, or if the Third Party has a direct network connection to the Current managed network.

Required ISO 27001 Controls	
2.1	7.2.2 Information security awareness, education and training
2.2	8.1.1 Inventory of assets
2.3	8.1.4 Return of assets
2.4	9.1.2 Access to networks and network services
2.5	9.2.1 User registration and de-registration
2.6	9.2.2 User access provisioning
2.7	9.2.3 Management of privileged access rights
2.8	9.2.6 Removal or adjustment of access rights
2.9	9.4.1 Information access restriction
2.10	9.4.2 Secure log-on procedures
2.11	9.4.3 Password management system
2.12	11.1.1 Physical security perimeter
2.13	11.1.2 Physical entry controls
2.14	11.1.3 Securing offices, rooms and facilities
2.15	11.1.4 Protecting against external and environmental threats
2.16	11.2.3 Cabling security
2.17	12.1.4 Separation of development, testing and operational environments
2.18	12.2.1 Controls against malware
2.19	12.4.1 Event logging
2.20	12.4.3 Administrator and operator logs
2.21	12.6.1 Management of technical vulnerabilities
2.22	13.1.1 Network controls
2.23	13.1.3 Segregation in networks
2.24	13.2.3 Electronic messaging
2.25	14.1.3 Protecting application services transactions
2.26	14.3.1 Protection of test data
2.27	15.1.1 Information security policy for supplier relationships
2.28	15.2.1 Monitoring and review of supplier services
2.29	15.2.2 Managing changes to supplier services
2.30	16.1.5 Response to information security incidents
2.31	18.2.1 Independent review of information security
2.32	18.2.3 Technical compliance review

Additional Minimum Security Requirements	
2.33	Secure configurations for all Third-Party Information System hardware and software shall be established, implemented and actively managed.
2.34	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.
2.35	Local accounts shall be disabled if not required or used and shall not be used for privileged access.
2.36	Third party shall notify Current of any separation or transfer of Third Party Worker with Current Single Sign On (SSO) credentials no later than the day of that event.
2.37	Accounts shall be disabled after 90 days of inactivity, at a minimum.
2.38	Current Confidential Information shall not be processed or stored on personal accounts or on personally-owned computers, devices or media.
2.39	A list of all high-risk technologies (e.g. Huawei, ZTE, Kaspersky) used shall be maintained by the vendor. High risk technologies shall not be used in the environment used by Current unless prior approval is obtained from Current.

3. ENHANCED SECURITY REQUIREMENTS

Applicability: Third Party Processes Current Highly Confidential Information, Controlled Data, or Sensitive Personal Data (including EU PII), or supports one or multiple critical business functions. These requirements are in addition to the minimum-security requirements.

Required ISO 27001 Controls	
3.1	5.1.1 Policies for information security
3.2	5.1.2 Review of the policies for information security
3.3	6.1.1 Information security roles and responsibilities
3.4	6.1.2 Segregation of duties
3.5	7.1.1 Screening
3.6	7.2.1 Management responsibilities
3.7	8.3.1 Management of removable media
3.8	8.3.2 Disposal of media
3.9	8.3.3 Physical media transfer
3.10	9.2.4 Management of secret authentication information of users
3.11	9.2.5 Review of user access rights
3.12	9.4.5 Access control to program source code
3.13	11.2.7 Secure disposal or re-use of equipment
3.14	12.1.1 Documented operating procedures
3.15	12.1.2 Change management
3.16	12.4.2 Protection of log information
3.17	12.5.1 Installation of software on operational systems
3.18	12.6.2 Restrictions on software installation
3.19	12.7.1 Information systems audit controls
3.20	14.2.2 System change control procedures
3.21	16.1.1 Responsibilities and procedures
3.22	16.1.2 Reporting information security events
3.23	16.1.4 Assessment of and decision on information security events
3.24	16.1.6 Learning from information security incidents
3.25	18.1.4 Privacy and protection of personally identifiable information

Additional Enhanced Security Requirements	
3.26	Accurate documentation of data flows for all Current Highly Confidential Information, Controlled Data, or Sensitive Personal Data resident (permanent or temporary) within the third party's environment shall be maintained.
3.27	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 Current Highly Confidential Information, Controlled Data, or Sensitive Personal Data from Third Party Information Systems.
3.28	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.
3.29	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 Current.
3.30	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.
3.31	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 shallnot be used.
3.32	New passwords shall be checked against a dictionary of known-bad choices, prior to authorizing the user to select their password.
3.33	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.
3.34	The Third Party shall implement mechanisms to detect and deactivate unauthorized (e.g. rouge) access points.
3.35	Short Message Service (SMS) shall not be used to transmit pins when authenticating with multi factor authentication.
3.36	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.
3.37	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.
3.38	All facilities used to access, process, transmit, and/or store Current 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. SOFTWARE DEVELOPMENT

Applicability: Third Party develops software specific to Current's needs or hosts applications that Process Current Highly Confidential Information, Confidential Information, Controlled Data, or Sensitive Personal Information with no Trusted Third-Party Network connectivity to Current.

Required ISO 27001 Control	
4.1	14.2.1 Secure development policy
4.2	14.2.8 System security testing
4.3	14.2.9 System acceptance testing

Additional Software Development Requirements	
4.4	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.
4.5	Information security checkpoints shall be incorporated into the software development lifecycle including, but not limited to; a. Risk assessment process b. Documented security requirements c. Secure coding guidelines and checklists d. Secure design/architecture review e. Source code review f. Security testing
4.6	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 Current upon request.
4.7	Any software developed for Current shall not contain any software (proprietary or open source) developed or sold by an entity other than the contracting third party unless approved by Current.
4.8	All software delivered to Current 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 Current 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.
4.9	If the Third Party hosted application undergoes Significant Changes or Enhancements, Current 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 Current, a Third Party's penetration test results shall be leveraged if the report meets Current's quality standards and was conducted within the last 12 months.
4.10	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).

5. ENHANCED SOFTWARE DEVELOPMENT

Applicability: Third Party develops software specific to Current's needs or host applications that Process Highly Confidential Information, Confidential Information, Controlled Data, or Sensitive Personal Data with Trusted Third-Party Network Connectivity to Current.

Required ISO 27001 Controls	
5.1	7.2.2 Information security awareness, education and training
5.2	14.2.6 Secure development environment
5.3	14.2.7 Outsourced development

Additional Enhanced Software Development Requirements	
5.4	Third party shall have a designated application security representative that acts as the primary liaison between Third Party and Current in matters related to secure application development, ensuring that Third Party development teams meet all Current requirements for secure application development, and provides to Current, upon demand, evidence of compliance with requirements listed in this section.
5.5	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 Current application owner. These risk factors shall be determined prior to the initiation of code development.
5.6	Documented security requirements shall be formally defined for all new development of applications including projects involving significant changes to existing applications with the Current designation of "Critical" and/or "External facing". These requirements shall be developed in collaboration with the Current application owner and other key stakeholders as necessary. All secure design requirements shall be documented and maintained with the broader set of application requirements.
5.7	Software development teams shall use Current-provided version control processes and tools.
5.8	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.
5.9	Static Application Security Testing (SAST) is required for all applications that are coded in programing language(s) supported by the Current solution. The list of languages is available from Current Cybersecurity & Technology Risk. If the application source code is not supported by the Current-provided solution, then SAST is not required, and only manual code review is necessary.
5.10	All confirmed high/critical vulnerabilities found during manual and automated (SAST) code review, shall be corrected prior to release to Current (to include deployment to production). SAST shall be performed utilizing the Current-provided solution. If coding is paused or halted, then SAST does not need to be performed until coding is resumed.
5.11	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 Current, to include deployment to production. DAST shall be performed utilizing the Current provided solution.
5.12	Security design review shall be incorporated to verify required security features and functionality.
5.13	A threat model is required for all applications that are developed for Current.

6. SYSTEM AND DATA AVAILABILITY

Applicability: Third Party Processes Current Highly Confidential Information, Confidential Information, Controlled Data, or Sensitive Personal Data that has high availability requirements or the Third Party's service/application has high availability requirements as defined by Current.

Required ISO 27001 Controls	
6.1	12.1.1 Documented operating procedures
6.2	12.1.3 Capacity management
6.3	12.3.1 Information backup
6.4	17.1.1 Planning information security continuity
6.5	17.1.2 Implementing information security continuity
6.6	17.1.3 Verify, review and evaluate information security continuity

	Additional System and Data Availability Requirements
6.7	Third party shall maintain a Disaster Recovery Plan (DRP) for all locations and applications used to provide services to Current. 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 Current. 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.
6.8	If Third Party provides a SaaS service, Third Party shall provide Current with geographically resilient hosting options. Third Party shall have more than one provider for each service for which there is a service delivery dependency.

7. SOFTWARE AS A SERVICE (SaaS) SECURITY

Applicability: Third Party hosts a cloud computing application that Processes Current Highly Confidential Information, Confidential Information, Controlled Data, or Sensitive Personal Data

Software as a Service Security Requirements	
7.1	SaaS provider is accountable for maintaining compliance with relevant regulations and legal requirements for its services.
7.2	SaaS provider shall provide documentation to tenants regarding the following: a. Roles and responsibilities matrix between cloud service provider and Current for each platform/service offering (e.g. incident response, infrastructure support, access management, etc.). Methods for maintaining segregation of duties within the cloud service offering shall also be included. b. Scenarios in which the cloud service provider may access tenant data and metadata. c. Installation, configuration, and use of products/services/features. d. Known issues with products/services of the cloud offering. e. Transport routes of data between systems and governing procedures for data migration to and from cloud service offering(s). f. How system (e.g. network, storage, memory, I/O, etc.) oversubscription is maintained and under what circumstances/scenarios.

	g. List of Third Parties that have access to Current Confidential Information or manage aspects of the application, database, server operating system, etc.
7.3	Configuration of the SaaS shall adhere to a minimum baseline of security configuration settings for role, scope and location of the services.
7.4	SaaS provider that directly provides services to Current is solely accountable for the platform and infrastructure security. If the provider uses other cloud or Third-Party service vendors, the provider is accountable for ensuring the security arrangement meets Current contractual requirements.
7.5	Integration of the primary SaaS with Current resources shall leverage Current pre-approved integration architecture pattern(s).
7.6	Interaction between two SaaS applications shall be channeled through Current approved security control points.
7.7	All service endpoints shall be signed by a trust authority or there must be another mechanism of establishing trust available.
7.8	SaaS provider shall ensure data portability among different cloud services by supporting standardized file format, import/export functionality, etc.
7.9	SaaS provider shall support standard based identity protocols and enforcement such as OpenID Connect (OIDC), Security Assertion Markup Language (SAML) and OAuth2 for propagating and enforcing identity controls through SaaS and Application Programing Interfaces (API).
7.10	SaaS provider shall have the capability to support tenant-generated and stored encryption keys.
7.11	Access to management consoles for entitlement and policy management shall be secure and restricted through Role Based Access Control (RBAC) and be based on the least privilege principle. Credential(s) for privileged accounts, including root or administrator accounts, shall be vaulted and multi factor authentication shall be implemented.
7.12	Upon request, SaaS provider shall inform Current of application user access that has been provisioned and de- provisioned for the Current account.
7.13	SaaS provider shall have the capability to provide secure data disposal at Current's request and ensure data is not recoverable by any computer forensic means.
7.14	SaaS provider shall triage threats and security related events in multi-tenant environments on a global scale and ensure timely and thorough incident management.
7.15	SaaS providers shall demonstrate compliance with information security and confidentiality, service definitions, and service level agreements. SaaS provider reports, records, and services shall undergo audit and review at planned intervals to govern and maintain compliance with the service delivery agreements.
7.16	SaaS provider shall use dedicated secure networks to provide management access to cloud service infrastructure that is separate from the customer (tenant) production infrastructure.
7.17	SaaS provider shall permit tenants to perform independent vulnerability assessments of the customer (tenant) production infrastructure.
7.18	SaaS provider shall allow tenants to opt-out of having their data/metadata accessed via inspection technologies.
7.19	SaaS provider shall have an option for customers to opt-in or opt-out of specific features in SaaS releases.
7.20	SaaS provider shall have the capability to logically segment and recover data for a specific customer in the case of a failure or data loss.
7.21	SaaS provider logging and monitoring framework shall allow isolation of an incident to specific tenants. Upon request, SaaS provider shall provide Current with platform management logs, application logs, API activity logs.
7.22	Upon request, SaaS provider shall have the capability to restrict the storage of customer data to specific countries or geographic locations.

8. PLATFORM AS A SERVICE (PaaS) SECURITY

Applicability: Third Party provides a cloud computing platform that allows Current to develop, run, and manage applications and these applications or company providing the PaaS Processes Current Highly Confidential Information, Confidential Information, Controlled Data, or Sensitive Personal Data.

Platform as a Service Security Requirements	
8.1	PaaS provider shall have the capability to integrate with Current supported identity solutions for access to the PaaS administration portal.
8.2	PaaS provider shall have a granular RBAC model to distinguish varying levels of access to PaaS components and applications.
8.3	PaaS provider administration portal and interactive access to the PaaS provider API shall require multi-factor authentication.
8.4	All access to the PaaS administrative portal and PaaS provider API shall utilize HTTPS/TLS.
8.5	PaaS provider shall support a "zero downtime" deployment model.
8.6	Upon request, PaaS provider shall have the ability for application, system, and API logs to be sent to the Current Digital Log Aggregation Tool.
8.7	Application workload and data storage shall be isolated at the tenant or application level.
8.8	PaaS provider shall allow and facilitate Current initiated network security scans and application penetration testing.
8.9	PaaS provider shall have systems in place to detect and respond to customer abuse on the platform.
8.10	PaaS provider shall have systems in place to receive and process abuse reports from customers and Third Parties in a timely fashion.
8.11	Hypervisor software shall be kept up to date with relevant patches.

9. VIRTUALIZATION SECURITY

Applicability: Third Party leverages virtualization, is responsible for the management of the virtual machine image and/or hypervisor, and Processes Current Highly Confidential Information, Confidential Information, Controlled Data, or Sensitive Personal Data.

Virtualization Security Requirements	
9.1	Maintain effective policies, guidelines, and processes to govern and control Virtual Machine (VM) lifecycle management, including self-service and automated scripts / DevOps tools.
9.2	Control the creation, storage, use, retirement and destruction of VM images with a formal change management process and tools and approve additions only when necessary.
9.3	Keep a small number of known-good and timely patched images of a guest operating system separately and use them for fast recovery and restoration of systems to the desired baseline.
9.4	Discover virtual systems, including dormant VMs and the applications running on them, regularly.
9.5	Use virtualization products with management solutions to examine, patch, and apply security configuration changes to VMs.
9.6	Maintain policies to restrict storage of VM images and snapshots. If it is necessary to store images and snapshots, proper authorization, such as secondary level of approval, shall be obtained and corresponding monitoring and control processes shall be established.
9.7	Control the backup, archiving, distribution, and restart of VMs with effective policies, guidelines, and processes such as suitably tagging the VM based on sensitivity / risk level.
9.8	Create a controlled environment to apply security patches and control policies to an offline or dormant VM.
9.9	Regularly monitor virtual appliances that provide critical infrastructure, management, and security services.
9.10	Ensure proper hardening and protection of VM instances through VM guest hardening.

9.11	Encrypt VM images to prevent unauthorized modification.
9.12	Augment VM operating systems with built-in security measures, leveraging third-party security technology, such as discovery and monitoring tools, to provide layered security controls.
9.13	Monitor virtual networks and data traffic similarly to physical networks.
9.14	Implement mechanisms to minimize resource contention such as staggering the scanning of VMs on the same physical server, using agentless deployment of anti-virus software, implementing distributed storage resources, and implementing a workload affinity policy.
9.15	Define and implement a standard operating procedure that detects VMs that are throttled due to resource exhaustion and puts a remedy in place instantly.
9.16	Harden the hypervisor's configuration to reduce areas of vulnerability (e.g. disabling memory sharing between VMs running within the same hypervisor hosts).
9.17	Disconnect unused physical hardware devices and disable clipboard or file-sharing services.
9.18	Conduct self-integrity checks upon boot-up using hypervisor integrity monitoring technology to confirm if the hypervisor has been compromised.
9.19	Monitor for signs of compromise by analyzing hypervisor logs on an ongoing basis.
9.20	Subscribe to your hypervisor vendor's security bulletins/alerts and implement security updates within 30 days of release by the vendor.
9.21	Implement and maintain effective hypervisor patch management practices.
9.22	Restrict access to the virtualization layer, including hypervisor management software and APIs through firewalls that restrict console access.
9.23	Follow the principles of least privilege by limiting the number of user accounts, including privileged accounts, requiring direct access to the hypervisor host.
9.24	Integrate hypervisor user accounts with robust credential management and multi factor authentication systems to enforce security policies.
9.25	Disable remote management of hypervisors. If this is not possible, provide access over a secure network connection and use multi-factor authentication. Close idle/inactive connections to prevent abuse of management/client.
9.26	Deploy a separate "management LAN" to manage access to hypervisors.
9.27	Apply strong authentication techniques where possible to self-service portals, preferably securing both the client and server side of cloud computing against potential attacks.

10. DATA CENTER SECURITY

Applicability: Third Party provides data center facility services.

Required ISO 27001 Controls	
10.1	11.1.4 Protecting against external and environmental threats
10.2	11.1.6 Delivery and loading areas
10.3	11.2.1 Equipment siting and protection
10.4	11.2.2 Supporting utilities
10.5	11.2.4 Equipment maintenance
10.6	17.2.1 Availability of information processing facilities

Data Center Security Requirements	
10.7	Data center walls shall be resistant to fire or explosions.
10.8	Data centers with glass windows are not allowed unless shatter proof and impact resistant barriers are in place.
10.9	Physical data center access rights shall be reviewed at a minimum quarterly using a documented process.
10.10	All data centers 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 center, 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 Current. 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 datacenter 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 center 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 center floor area.
10.16	Assets containing Current Confidential Information shall be caged off physically from the rest of the data center. 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 center parking area shall have physical obstacles in place to reduce risk of vehicle or car bomb penetrating exterior walls.
10.20	All data center 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 centers 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 center shall conform to the interior security requirements for entrance to the data center. 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 center 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 center 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 center 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 center 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 center 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 center 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 Current 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 labeled. 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 Current 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 centers shall have a disaster recovery plan for the facility and environmental that at least identifies and mitigates risks to Current 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 center sites. The plan shall be shared with Current to ensure Current can coordinate with its own DRP.
10.42	Data centers shall conduct an electrical blackout test, at least annually, to validate continue functionality through an operational interruption. Additionally, the data center shall participate and support Current DRP and associated testing.
10.43	All Current equipment shall be completely network segregated from non-Current parts of the data center.

11. DIRECT NETWORK CONNECTIVITY TO Current

SECURITY Applicability: Third Party has a Trusted Third-Party

Direct Network Connectivity Security Requirements	
11.1	Third party shall use only Current managed network devices to connect to the Trusted Third Party connection. Current requires out of band connectivity to the remote device for administration.
11.2	Third party shall implement a firewall between the third-party parent network and the Trusted Third Party network. The firewall shall be managed by Current and configured to allow only the connections authorized by Current.
11.3	Current conducts periodic scans on all Current IP addresses. If Current notifies the third party of any confirmed high or critical vulnerability found, the third party shall remediate the confirmed vulnerability

	The Trusted third party shall ensure that nothing will be placed in line to limit the ability for Current to perform vulnerability scanning of the Trusted Third Party network.
11.4	All internet traffic shall be directed to a Current managed external proxy.
11.5	Remote access to the Trusted Third Party network is only allowed through the Current Virtual Private Network (VPN) hub infrastructure with two-factor authentication.
11.6	Current 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 Current approved Third Party Workers and approved Current employees. The Third Party shall also maintain a listing of all individuals that have access to equipment.
11.7	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 Current network. The business network of the Third Party shall not share any layer-2 switches or network devices with Current except for the terminating firewall.
11.8	Third Party shall ensure that all wireless deployments on Trusted Third Party networks follow the Current Third Party network change request process and are configured/managed by Current.
11.9	All unused switch ports shall be disabled on network equipment. In addition, all new connection requests shall be submitted to Current.

12. PRODUCT SECURITY

Applicability: Third Party provides any Products (as defined below) under the Contract Document that include executable binary code.

Secure Software Development Requirements	
12.1	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.
12.2	Supplier shall implement processes to ensure malware protection measures are implemented for the Products development environment and relevant assets.
12.3	The Supplier shall have a process to ensure the systems used in Products development environment(s) are properly and timely patched.

12.4	Supplier shall include cybersecurity guidance in the Product documentation provided to Current. 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) the Products shall not provide access to that service or capability using a default account/password; (ii) the 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) the Products shall not provide access to that service or capability using a “Backdoor” account or password;

	(iv) the Products' associated authentication and password change processes shall be implemented with an appropriately secure cryptographic level; and (v) Current shall be able to change any passwords supported by the Products.
12.5	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.
12.6	In the event that 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).
12.7	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.
12.8	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 Current unless prior approval is obtained from Current.

Cybersecurity Vulnerabilities, Assessment and Reporting Requirements	
12.9	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 Current 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 Current and any Cybersecurity Vulnerability with a fix to Current at current.compliance@ge.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 Current, 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 Current in its investigation of a Cybersecurity Vulnerability, whether discovered by Supplier, Current, or a third party, which shall include providing Current a detailed description of the Cybersecurity Vulnerability, the remediation plan, and any other information Current reasonably may request concerning the Cybersecurity Vulnerability, as soon as such information can be collected or otherwise becomes available. Current or Current'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 Current promptly.

Physical Security and Distribution Integrity	
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 Current's components' environment only to personnel cleared by both supplier and Current; (ii) the use of tamper evident seals on media and containers, to detect unauthorized access to protected products (e.g. tamper evident labels or seals, which self- destruct and leave a residue sticker if removed); and (iii) tamper-resistant production (e.g. digital signatures for software and corresponding hardware mechanisms).

Additional Representations and Warranties and Insurance	
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 Current or used as a component of or in relation to any Products provided under the Agreement, except with the prior written authorization of Current; 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 Current shall not cause Current or Current's intellectual property rights to be subject to the terms or conditions of a Copyleft License, or require Current to fulfil 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 Current's other rights and remedies under this Agreement or otherwise at law or in equity, Supplier shall provide Current, 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.

13. SECURITY CONTROL APPLICABILITY MATRIX

Applicability	Minimum Security	Enhanced Security	Software Development	Enhanced Software Development	System & Data Availability	Software as a Service Security	Platform as a Service Security	Virtualization Security	Data Center Security	Direct Network Connectivity to Current Security	Product Security
Processes Current Confidential Data or Personal Data	X										
Processes Current Highly Confidential, Controlled Data or supports one or multiple critical business	X	X									
Direct Network Connectivity to Current										X	
Stores Physical Documentation	X	X									
Providing Data Center Services									X		
Services or Data that require high availability as defined by Current					X						
Develops software specific to Current's needs or hosts applications that Process with Current Data with no direct network connectivity to Current			X								
Develops software specific to Current's needs or hosts applications that interact with Current Data with direct network connectivity to Current				X							

Applicability	Minimum Security	Enhanced Security	Software Development	Enhanced Software Development	System & Data Availability	Software as a Service Security	Platform as a Service Security	Virtualization Security	Data Center Security	Direct Network Connectivity to Current Security	Product Security
SaaS services Processing Current Data						X					
PaaS services Processing Current Data							X				
Infrastructure as a Service Processing Current Data								X	X		
Cloud Service Provider responsible for governance of virtual machine images or hypervisor								X			
Provides a digital component to be utilized in a Current Product											X

14. 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 Current 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.

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

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

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

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 Current 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 Current 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 Current, or from Current to a Third Party. The correction of any existing critical or high vulnerabilities must be conducted prior to transfer or included in the work order for the new Third Party to correct within the applicable remediation timeframe.

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