Baker Hughes

Third Party Information Security Requirements

Date: 23 November 2021

Table of Contents

Introduction

The Baker Hughes (hereinafter referred to as BH) Third Party Information Security Requirements document outlines the security requirements applicable to BH Third Parties, including suppliers and joint ventures. The security requirements outlined herein, are applicable to Third Parties that Process BH Confidential Information, have access to a BH 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 BH, specifically guided by the type of BH information the Third-Party Processes, network connection, services provided by the Third Party, and data availability requirements.
BH reserves the right to update this document from time to time.

1) Business Information

Applicability

This is a default domain applicable to all third parties who are being assessed.

General Controls	
1.1	No material claims or judgments against the Third Party
1.2	Third Party not suffered a data loss or security breach within the last 3 years
1.3	Third parties subcontractors not suffered any data loss or security breach within the last 3 years

2) Policy, Procedure, Process (PPP)

Applicability

This is a default domain applicable to all third parties who are being assessed.

General Controls	
2.1	Third Party must document, develop and maintain the following policies and procedures up-to-date which has to be aligned with industry preferred standards.
	a) Vulnerability Management plan.
	b) Information Security Policy & Privacy policy.
	c) CISO/CIO to oversee and manage cybersecurity program.
	d) Data protection program which maintains enforcement and monitoring procedures to ensure compliance with Privacy obligations.
	e) Network Security Plan/Program.
	f) Business Continuity and Disaster Recovery
	g) Incident Management plan/Program
	h) Operational Change Management/Change Control policy or program
	i) Physical security program
	j) Human Resource policies
	k) Asset Management program
	l) Acceptable Usage policy

2.2	Third Party shall have an internal password policy with complexity or length requirements?
2.3	Third Party shall perform an annual information security reviews over the environment(s) that process and/or stored Baker Hughes data Examples of information security reviews include, but are not limited to SSAE 16, SOC 2 Type 2, ISAE 4302, PCI, ISO27001 Certification. Note: The assessment can be performed by an external party or an internal team. If an internal team is leveraged then the team must be independent, qualified and staffed with dedicated members. If the team does not meet all of these aspects please answer "No" and indicate which aspects are not met in the Comments section.
2.4	Third party shall maintain an Industry Standard certification such as IEC Standard Framework, ISO 27002 Framework, SOC2 or SOC 3, HITRUST Certification.

3) Human Resources (HR)

Applicability

This is a default domain applicable to all third parties who are being assessed.

General Controls	
3.1	Confidentiality/NDA to be signed with External parties having access to BH Data. Employees, Contractors and Sub contractors to sign a NDA, Acceptable Disclosures during onboarding to reflect the Supplier needs for protection of Data
3.2	Screening of Employees
3.3	Information Security Awareness Education and Training
3.4	Secure Development & Testing Awareness Education and Training
3.5	Third Party shall implement a process to ensure the access of an employee, contractor, or temporary worker leaves the Supplier organization will be revoked with 24 hours of their termination date

4) Business Continuity and Disaster Recovery (BCDR)

Applicability

This Domain will be applicable when the vendor is not replaceable or if the vendor services are not available for a period of time which will impact Baker Hughes Core business or business

General Controls	
4.1	Implementing information security continuity
4.2	Planning information security continuity, Implementing information security continuity
4.3	Information backup
4.4	Verify, review and evaluate information security continuity
4.5	Availability of information processing facilities
4.6	Verify, review and evaluate information security continuity

5) Data Center (DC)

Applicability

This Domain will be applicable whenever the vendor is providing a solution using a Cloud services or Web based services, Application hosted by vendor or any datacenter related services that are provided by vendor.

General Controls	
5.1	Data Centre has to be Certified by Either SOC/HITRUST/ISO
5.2	Protecting against external and environmental threats
5.3	Delivery and loading areas
5.4	Supporting utilities
5.5	Equipment maintenance
5.6	Availability of information processing facilities
5.7	Equipment siting and protection
5.8	Alarms to be triggered if door left open more than 60 seconds
5.9	Data centre doors to generate log with timestamp, room and badge id
5.10	All door logs, check in process logs to be retained for one year
5.11	Critical infrastructure (e.g. network, storage, power supply) should be monitored to ensure that potentially disruptive events are identified and remediated immediately
5.12	Badge readers used on all entry points to ensure physical access is restricted to authorized personnel?
5.13	Process to be defined for visitors to follow a check in process on all entry points
5.14	CCTV to monitor and archived as per industry standards
5.15	Prevention of unplanned interruption services
5.16	Documented operating procedures
5.17	Third Party shall define a process for carrying out backup activities including offsite long-term storage and for reviewing and responding to unsuccessful backups.

6) Network Security (NS)

Applicability

This Domain will be applicable when the vendor is maintaining a network connection with BH or if the vendor services are provided through Cloud.

General Controls	
6.1	Network Security has to be mapped to industry standards
6.2	Vulnerability management process to be implemented
6.3	Network controls/Architecture to be created for Baker Hughes engagement
6.4	Information security policy for supplier relationships
6.5	Wireless Security (disabling SSID broadcasting, MFA implementation)
6.6	Security of network services
6.7	Segregation in networks
6.8	Root/administrator access to the management console shall require multi-factor authentication
6.9	Disconnecting unused hardware and disabling file sharing services.
6.10	Detect unauthorized devices in supplier network real time

6.11	Access to networks and network services
6.12	User access provisioning/ Least privilege access to sensitive information
6.13	User registration and de-registration
6.14	Physical access to Baker Hughes Managed network equipment limited to Baker Hughes approved third-party
6.15	Restricting Remote Administration from Public Networks and Multifactor authentication to access network third party organization remotely
6.16	Documented Customer network connection approval
6.17	Access control policy
6.18	Information access restriction
6.19	Documented process of reassign ownership of non-service accounts
6.20	Virtualization/VM Lifecycle and Hypervisor Lifecycle Policy
6.21	Hypervisor Patch management
6.22	Monitor for signs of compromise by analysing hypervisor logs on an ongoing basis.
6.23	Disable remote management of hypervisors when required
6.24	Regularly monitor virtual appliances that provide critical infrastructure, management, and security services
6.25	Define and implement a standard operating procedure that detects VMs that are throttled due to resource exhaustion and provisions additional resources dynamically
6.26	Controlling VM images with a formal Change management process
6.27	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.
6.28	Create a controlled environment to apply security patches and control policies to an offline or dormant VM
6.29	Third Party shall ensure proper hardening and protection of VM instances through VM guest hardening
6.30	Third Party shall 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
6.31	Electronic messaging
6.32	Securing application services on public networks
6.33	Protecting application services transactions
6.34	All logs to be merged together manually or by SIEM in a single form for granular analysis. (e.g., app logs, firewall logs, IDS logs, physical access logs, etc.
6.35	Event logging
6.36	Administrator and operator logs
6.37	Documented process to periodically review and monitor security logs, event logs and errors at application and system level
6.38	Third party shall implement a process that differentiate "Enhanced Screening" and "Limited High Privileged Access" processes for a "special HPA team" to support systems and data that Baker Hughes assessed to be "Critical and/or High Risk
6.39	Third party provider shall use dedicated secure networks, separate from customer production infrastructure, leveraged to provide management access to the cloud infrastructure
6.40	Third Party software shall be able to integrate with customer identity provider for user authentication
6.41	Third Party platform shall support the self-service registration and onboarding of Baker Hughes customers and partners identities to in scope digital properties through a governance process
6.42	Third Party platform shall support the management of consent and privacy clauses, as part of the self-service registration process?

6.43	Third Party platform shall implement a Centralized Policy Based Access Control (PBAC) solution with a governance process to protect customer data
6.44	Third Party shall have a patch management process which includes applying all relevant vendor rated critical patches and security updates within 30 days of release by the vendor
6.45	Third Party shall harden their hypervisor's configuration to reduce areas of vulnerability?
6.46	Third Party shall restrict, log, and monitor access their information security management systems
6.47	Third Party shall document and provide their timeframe for patching critical network vulnerabilities for perimeter firewalls

7) Incident Management (IM)

Applicability

This Domain will be applicable when the vendor is providing a software development solution or cloud services or has a network connection to Baker Hughes where the vendor might need to handle potential threats and ready to handle incidents.

General Controls	
7.1	Information Security Incident Management Responsibilities and procedures
7.2	Reporting information security events
7.3	Assessment of and decision on information security events
7.4	Response to information security incidents
7.5	Learning from information security incidents
7.6	Event Logging
7.7	Third party shall log all security events in production environment (firewalls connections, authentication requests, admin access, privilege escalations etc.)

8) Asset and Information Management (AIM)

Applicability

This Domain will be applicable when the vendor handling assets that are provided by Baker Hughes or providing services to Baker Hughes where they are handling sensitive information, confidential data, Highly Confidential data and PII Data.

General Controls	
8.1	Classification of information
8.2	Handling of assets
8.3	Information security awareness, education and training
8.4	Management of removable media
8.5	Physical media transfer
8.6	Securing application services on public networks
8.7	Protecting application services transactions
8.8	Electronic messaging
8.9	Secure disposal or re-use of equipment
8.10	Disposal of media

8.11	Process to reconcile hardware assets (Owner/asset tag) to ensure existence and to detect unauthorized devices at minimum annually
8.12	Process to verify the Return of Assets
8.13	Inventory of assets
8.14	TLS protocol has to be equal or greater than 1.2
8.15	Third Party shall store Hard Copies of confidential data only if it is locked in cabinet by their employees
8.16	Third Party shall implement a standard endpoint that shall be issued to employees and their security configuration shall be documented.
8.17	Third Party shall implement an anti-virus with the latest virus definitions/signatures installed on all desktops, laptops, and servers within third-party organizations environment.
8.18	Third Party shall encrypt tenant data at rest (on disk/storage) within their environment

9) Software Development (SD)

Applicability

This Domain will be applicable when the vendor is providing Software as a Service, Development services, Deployment service, Cloud Services which may or may not handle Confidential data, PII Data, Highly Confidential data etc.

General Controls	
9.1	Software or application development of Industry Standard framework frame works and secure code practices adhered
9.2	Secure development policy
9.3	Separation of development, testing and operational environment
9.4	Separates code repositories for production and Non production environment
9.5	Availability of information processing facilities
9.6	Verify, review and evaluate information security continuity
9.7	Information access restriction
9.8	Access control to program source code
9.9	System security testing
9.10	System acceptance testing
9.11	Management of technical vulnerabilities, i.e. risk assessment process, secure design/architecture review, source code review, security vulnerability testing, remediation of all high and critical vulnerabilities prior to moving code to production
9.12	Documented process in place to meet the agreed upon escrow arrangements per contractual requirements.
9.13	Baker Hughes secure coding standards for all programming languages being utilized
9.14	Secure Development Environment
9.15	SAST and DAST to be performed on the software developed for Baker Hughes
9.16	Outsourced development should be controlled and should made aware to Baker Hughes
9.17	Vulnerabilities should be remediated before Software/Application is provided to the BH
9.18	Third Party shall have a designated application security representative who acts as the primary liaison between Supplier and Baker Hughes to ensure that all requirements for secure application development are met
9.19	Third Party development team shall be provided with prevention and remediation training on the common vulnerabilities identified in the software they developed or assisted in developing
9.20	Third Party include any of following as part of annual product security assessments: Vulnerability scanning, Threat Modelling, Penetration testing, Annual Product Security Assessments

10) Change Management (CM)

Applicability

This Domain will be applicable if the vendor provides software services, Development patching, Cloud services which include software configurations to Baker Hughes

General Controls	
10.1	Change management policy
10.2	System change control procedures
10.3	Access to networks and network services
10.4	User access provisioning
10.5	User registration and de-registration
10.6	Software applications aligned to Baker Hughes, the change control process include an option for Baker Hughes to opt-in or opt-out of specific features in releases
10.7	Change management process shall include the following requirements • Testing is performed in an environment separate from production before implementation • Formal approvals are obtained before a change takes place • Version control is maintained for all software updates • A change request audit trail is maintained • The person who requests the change and the person who approves the changes are not the same (segregation of duties • Change management procedures must be followed during emergencies

11) Cloud Services (CS)

Applicability

This Domain will be applicable when the vendor is providing services though cloud platforms such as IaaS, SaaS, PaaS, IDaaS etc. .

General Controls	
11.1	PaaS and IaaS Cloud Services has subscribe to the Shared Responsibility Model, where clients are responsible for access control and provide logging and alert functions to Platform and Infrastructure products
11.2	Removal or adjustment of access rights when it is no longer needed in the business requirement
11.3	PaaS and IaaS Services provider to manage and store the identity of all personnel who have access to the IT infrastructure, including their level of access based on RBAC model
11.4	Controls are in place to prevent unauthorized access to your application, program, or object source code, and assure it is restricted to authorized personnel only.
11.5	Based on RBAC there should be timely DE provisioning, revocation, or modification of user access to the Suppliers systems, information assets, and data implemented upon any change in status of employees, contractors, customers, business partners, or involved third parties
11.6	PaaS and IaaS providers to provide open encryption methodologies (3.4ES, AES, etc.) to tenants in order for them to protect their data if it is required to move through public networks (e.g., the Internet)
11.7	PaaS and IaaS providers to utilize open encryption methodologies any time in the infrastructure components need to communicate with each other via public networks (e.g., Internet-based replication of data from one environment to another)

11.8	PaaS and IaaS providers to provide tenants with ongoing visibility and reporting of your operational Service Level Agreement (SLA) performance
11.9	PaaS and IaaS providers shall have systems in place to detect and respond to customer abuse on the platform.
11.10	PaaS and IaaS providers to conduct network penetration tests of your cloud service infrastructure regularly as prescribed by industry best practices and guidance.
11.11	SaaS provider to encrypt tenant data at rest (on disk/storage) within your environment.
11.12	SaaS provider to allow isolation of logs by tenant.
11.13	SaaS provider audit logs reviewed on a regular basis for security events (e.g., with automated tools)
11.14	SaaS provider shall support standards based identity protocols (e.g. OpenID Connect, OAuth2, etc.) leveraged for propagating and enforcing identity controls through the SaaS and associated API's.
11.15	SaaS provider shall allow Single Sign-On (SSO) available for SaaS applications included as part of the products or services contracted to Baker Hughes.
11.16	SaaS provider shall support tenant-generated encryption keys, tenant specific encryption keys, or permit tenants to encrypt data to an identity without access to a public key certificate (e.g. identity-based encryption)
11.17	SaaS provider shall conduct application penetration tests of your cloud infrastructure regularly as prescribed by industry best practices and guidance
11.18	SaaS provider shall have the ability to logically segment or encrypt customer data such that data may be produced for a single tenant only, without inadvertently accessing another tenant's data
11.19	SaaS provider's application workload and data storage shall be isolated at the tenant or application level
11.20	SaaS provider shall have the capability to recover data for a specific customer in the case of a failure or data loss
11.21	SaaS provider should implemented SaaS product backup or redundancy mechanisms, to ensure compliance with regulatory, statutory, contractual or business requirements
11.22	SaaS provider has to you publish a list of all APIs available in the service and indicate which are standard and which are customized as per Baker Hughes Requirements.
11.23	SaaS provider logging and monitoring framework allow isolation of an incident to specific tenants
11.24	SaaS provider shall permit Baker Hughes to opt-in or opt-out of certain features in application or platform releases
11.25	SaaS provider should provide tenants with separate environments for production and test processes (i.e. provision of a "Sandbox" for configuration testing)
11.26	SaaS provider shall provide Baker Hughes with the following documentation i) Roles and responsibilities matrix between Supplier organization and Baker Hughes for each platform/service offering (i.e. incident response, infrastructure support, access management, etc. Methods for maintaining segregation of duties within the cloud service offering ii) Scenarios in which the cloud service provider may access tenant data and metadata iii) Installation, configuration, and use of products/services/features iv) Known issues with certain products/services of the cloud offering v) Transport routes of data between systems and governing procedures for data migration to and from cloud service offering.
11.27	SaaS provider shall have a documented Recovery Time and Recovery Point SLA.
11.28	SaaS provider shall implement a Web Application Firewall (WAF) as part of the solution to protect the application and/ or API
11.29	SaaS provider shall mitigate web application vulnerabilities for not only limited to internet facing SaaS application

12) Payment Cardholder Industry (PCI)

Applicability

This Domain will be applicable when the vendor is not replaceable or if the vendor services are not available for a period of time which will impact Baker Hughes Core business or business

General Controls	
12.1	Third Party shall have an internal program to monitor compliance with PCI.
12.2	Third Party is required to conduct an onsite certification by a Qualified Security Assessor (QSA) as per their corresponding PCI level Annually.
12.3	Third Party has to complete a Self-Assessment Questionnaire from the PCI Council along with an Attestation of Compliance.
12.4	Third Party shall conduct quarterly network scans by an Approved Scanning Vendor (ASV).
12.5	If Third Parties shares Baker Hughes cardholder data with external parties the external parties are subjected to be PCI compliant.
12.6	Encryption Key management Life Cycle.

13) Trusted Connections (TC)

Applicability

This Domain will be applicable when the Supplier is maintaining a direct connection or maintaining an offshore development center for Baker Hughes within the Supplier's environment.

General Controls	
13.1	Third Party shall maintain a listing of approved individuals who have access to the Baker Hughes managed network equipment.
13.2	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 Baker Hughes network.
13.3	Third Party shall ensure that all wireless deployments on the trusted third party network follow the Baker Hughes third party network change request process and are they configured/managed by Baker Hughes.
13.4	All unused switch ports shall be disabled on network equipment. In addition, all new connection requests shall be submitted to Baker Hughes.
13.5	Third party shall implement a firewall between the third-party parent network and the Trusted Third Party network. The firewall shall be managed by Baker Hughes and configured to allow only the connections authorized by Baker Hughes.
13.6	If Baker Hughes has notified Supplier organization of high or critical vulnerabilities, have the vulnerabilities shall be remediated within 30 days of notification.
13.7	All internet traffic directed to a Baker Hughes managed external proxy
13.8	Third-party Shall describe the trusted third party network access controls for Baker Hughes trusted connections (for example, Virtual Private Networks, Multi-Factor Authentication, Service Accounts, or other).
13.9	Third Party shall not use a non-Baker Hughes managed network devices used to connect to a trusted third party connection
13.10	Third-party Supplier network shall share any layer-2 switches, or other network devices with Baker Hughes (with the exception of the firewall)?

13.11	Third-party Supplier shall conduct an web application vulnerability assessment or penetration test been performed on the application(s) that store, process, host, and/or transmit Baker Hughes data within the last 12 months by an external 3rd party

14) Workspace /Physical Security (WPS)

Applicability

This Domain will be applicable when the vendor is not replaceable or if the vendor services are not available for a period of time which will impact Baker Hughes Core business or business

General Controls	
14.1	Physical security perimeter
14.2	Securing offices, rooms and facilities
14.3	Physical entry controls
14.4	Clear screen policy
14.5	Clean desk policy

15) Third Parties (TP)

Applicability

This Domain will be applicable when the vendor is utilizing a third party to provide a service to Baker Hughes using a contracting or sub contracting services

General Controls	
15.1	Information and Communication technology supply chain
15.2	Information security policy for supplier relationships
15.3	Information and details about the outsourced work

16) GDPR (GD)

Applicability

This Domain will be applicable when the vendor handling PII data of European Union region or proving a services a service to or from European Union region.

General Controls	
16.1	Third Party shall have an documented policies and procedures for cross border data flows or transfers of Baker Hughes data either to the US from other countries or from the EU to other countries.
16.2	Third Party shall be required to be registered with one or more Data Protection Authorities
16.3	Third Party shall appoint a Data Protection Officer as Per GDPR requirement.
16.4	Third Party shall maintain a process to remove Personal Data based on the Right to be Forgotten if applicable to the services provided.
16.5	Client scoped data that is collected, transmitted, processed, or stored by company to be classified as either European Union covered Personal Data or Special Categories of Personal Data (e.g., Genetic data, biometric data, health data)

17) General Privacy (GP)

Applicability

This is a default domain applicable to all third parties who are being assessed.

General Controls	
17.1	Third Party shall collect client scoped data either directly from an individual on behalf of the client or provided to the Supplier directly by the client, Non-Public Personal Data, PII Data, PHI or Medical Information data and Data Consumer report information or Covered account under Identity Theft Red Flags etc. based on the agreed Scope of work and shall have relevant process and procedures to enable individuals to view, access, correct, amend, or delete inaccurate information.
17.2	Third Party shall provide conspicuous notice, in clear and plain language, about privacy policies and procedures related to client scoped data.
17.3	Third Party shall have a documented privacy policies and procedures that address choice and consent based on the statutory, regulatory, or contractual obligations to provide privacy protection for client-scoped privacy data.
17.4	Third Party shall have controls to ensure that the collection and usage of personal information is limited and in compliance with applicable law.
17.5	Third Party shall not disclose client scoped data to third parties.
17.6	Third Party shall not allow their third parties to collect, transmit, process, access, disclose, or retain client scoped data with regards to services provided to Baker Hughes.
17.7	Third Parties shall have a documented data protection program with administrative, technical, and physical and environmental safeguards for the protection of client-scoped data.
17.8	Third Party shall have a documented process to maintain accurate, complete, relevant and timely records of personal information for the purposes identified in the notice.
17.9	Third Party shall have a data protection function that maintains enforcement and monitoring procedures to address compliance for its privacy obligations for client-scoped privacy data.
17.10	Third party shall implement a Data anonymization when they are handling Highly confidential Baker Hughes Data and shall document the data anonymization procedure that is implemented