Privacy and Security Terms

Article I, Business Contact Information

This Article applies if Supplier or IBM Processes the other's BCI.

1.1 IBM and Supplier may Process the other's BCI wherever they do business in connection with Supplier's delivery of Services and Deliverables.

1.2 A party:

(a) will not use or disclose the other party's BCI for any other purpose (for clarity, neither party will Sell the other's BCI or use or disclose the other's BCI for any marketing purpose without the other party's prior written consent, and where required, the prior written consent of affected Data Subjects), and

(b) will delete, modify, correct, return, provide information about the Processing of, restrict the Processing of, or take any other reasonably requested action in respect of the other's BCI, promptly on written request from the other party.

1.3 The parties are not entering a joint Controller relationship regarding each other's BCI and no provision of the Transaction Document will be interpreted or construed as indicating any intent to establish a joint Controller relationship.

1.4 The IBM Privacy Statement at https://www.ibm.com/privacy/ contains additional details on IBM's Processing of BCI.

1.5 Supplier has implemented and will maintain technical and organizational security measures to protect IBM's BCI against loss, destruction, alteration, accidental or unauthorized disclosure, accidental or unauthorized access, and unlawful Processing.

1.6 Supplier will promptly (and in no event any later than 48 hours) notify IBM after becoming aware of any Security Breach involving IBM's BCI. Supplier will provide such notification through the IBM Global Procurement Support Portal at https://www.ibm.com/procurement/procSupport. Supplier will provide IBM with reasonably requested information about such breach and the status of any Supplier remediation and restoration activities. By way of example, reasonably requested information may include logs demonstrating privileged, administrative, and other access to Devices, systems or applications, forensic images of Devices, systems or applications, and other similar items, to the extent relevant to the breach or Supplier's remediation and restoration activities.

1.7 Where Supplier is only Processing IBM's BCI, and has no access to any other data or materials of any kind or to any IBM Corporate System, this Article and Article X (Cooperation, Verification and Remediation) are the only Articles that apply to such Processing.

Article II, Technical and Organizational Measures, Data Security

This Article applies if Supplier Processes IBM Data, other than IBM's BCI. Supplier will comply with the requirements of this Article in providing all Services and Deliverables, and by doing so protect IBM Data against loss, destruction, alteration, accidental or unauthorized disclosure, accidental or unauthorized access, and unlawful forms of Processing. The requirements of this Article extend to all IT applications, platforms, and infrastructure that Supplier operates or manages in providing Deliverables and Services, including all development, testing, hosting, support, operations, and data center environments.

1. Data Use

1.1 Supplier may not add to the IBM Data or include with the IBM Data any other information or data, including any Personal Data, without IBM's prior written consent, and Supplier may not use IBM Data in any form, aggregated or otherwise, for any purpose other than providing Services and Deliverables (by way of example, Supplier is not permitted to use or reuse IBM Data to evaluate the effectiveness of or means of improving Supplier's offerings, for research and development to create new offerings, or to generate reports regarding Supplier's offerings). Unless expressly permitted in the Transaction Document, Supplier is prohibited from Selling IBM Data.

1.2 Supplier will not embed any web tracking technologies in the Deliverables or as part of the Services (such technologies include HTML5, local storage, third party tags or tokens, and web beacons) unless expressly permitted in the Transaction Document.

2. Third Party Requests and Confidentiality

2.1 Supplier will not disclose IBM Data to any third party, unless authorized in advance by IBM in writing. If a government, including any regulator, demands access to IBM Data (e.g., if the U.S. government serves a national security order on Supplier to obtain IBM Data), or if a disclosure of IBM Data is otherwise required by law, Supplier will notify IBM in writing of such demand or requirement and afford IBM a reasonable opportunity to challenge any disclosure (where law prohibits notification, Supplier will take the steps that it reasonably believes are appropriate to challenge the prohibition and disclosure of IBM Data through judicial action or other means).

2.2 Supplier assures IBM that: (a) only those of its employees who need access to IBM Data to provide Services or Deliverables will have that access, and then only to the extent necessary to provide those Services and Deliverables; and (b) it has bound its employees to confidentiality obligations that require those employees to only use and disclose IBM Data as these Terms permit.

3. Return or Deletion of IBM Data

3.1 Supplier will, at IBM's choice, either delete or return IBM Data to IBM upon termination or expiration of the Transaction Document, or earlier upon request from IBM. If IBM requires deletion, then Supplier will, consistent with Industry Best Practices, render the data unreadable and unable to be reassembled or reconstructed, and will certify the deletion to IBM. If IBM requires the return of IBM Data, then Supplier will do so on IBM's reasonable schedule and per IBM's reasonable written instructions.

Article III, Privacy

This Article applies if Supplier Processes IBM Personal Data.

1. Processing

1.1 IBM appoints Supplier as a Processor to Process IBM Personal Data for the sole purpose of providing the Deliverables and Services in accordance with IBM's instructions, including those contained in these Terms, the Transaction Document and the associated base agreement between the parties. If Supplier does not accommodate an instruction, IBM may terminate the affected part of the Services on written notice. If Supplier believes an instruction violates a data protection law, Supplier will so inform IBM promptly and within any time frame required by the law.

1.2 Supplier will comply with all data protection laws applicable to the Services and Deliverables.

1.3 An Exhibit to the Transaction Document, or the Transaction Document itself, sets out the following in respect of IBM Data:

(a) categories of Data Subjects;

(b) types of IBM Personal Data;

(c) Processing activities;

(d) duration of Processing; and

(e) a list of Subprocessors.

2. Technical and Organizational Measures

2.1 Supplier will implement and maintain the technical and organizational measures set forth in Article II (Technical and Organizational Measures, Data Security) and Article VIII (Technical and Organizational Measures, General Security), and by doing so ensure a level of security appropriate to the risk its Services and Deliverables present. Supplier certifies and understands the restrictions in Article II, this Article III, and Article VIII and will comply with them.

3. Data Subject Rights and Requests

3.1 Supplier will inform IBM promptly (on a schedule that allows IBM and any Other Controllers to fulfill their legal obligations) of any request from a Data Subject to exercise any Data Subject rights (e.g., rectification, deletion or blocking of data) regarding IBM Personal Data. Supplier will not answer any requests from Data Subjects unless it is legally required or instructed by IBM in writing to do so.

3.2 If IBM is obliged to provide information regarding IBM Personal Data to Other Controllers or other third-parties (e.g., Data Subjects or regulators), Supplier will assist IBM by providing information and taking other reasonable actions that IBM requests, on a schedule that allows IBM to timely respond to such Other Controllers or third-parties.

4. Subprocessors

4.1 Supplier will provide IBM with advance written notice before adding a new Subprocessor or expanding the scope of Processing by an existing Subprocessor, with such written notice identifying the name of the Subprocessor and describing the new or expanded scope of Processing. IBM may object to any such new Subprocessor or expanded scope on reasonable grounds at any time, and if

it does so, the parties will work together in good faith to address IBM's objection. Subject to IBM's right to so object at any time, Supplier may commission the new Subprocessor or expand the scope of Processing of the existing Subprocessor if IBM has not raised an objection within 30 Days of the date of Supplier's written notice.

4.2 Supplier will impose the data protection, security and certification obligations set out in these Terms on each approved Subprocessor prior to a Subprocessor Processing any IBM Data. Supplier is fully liable to IBM for performance of each Subprocessor's obligations.

5. Transborder Data Processing

As used below:

Adequate Country means a country providing an adequate level of data protection pursuant to a data protection law or the decision of a regulator.

Data Importer means either a Processor or a Subprocessor that is not established in an Adequate Country.

EU Standard Contractual Clauses ("EU SCCs") means the EU Standard Contractual Clauses (Commission Decision 2010/87/EC) with optional clauses removed, as officially published at https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/model-contracts-transferpersonal-data-third-countries_en.

Standard Contractual Clauses ("**SCCs**") means the contractual clauses required by applicable data protection laws for the transfer of Personal Data to Processors that are not established in Adequate Countries.

5.1 Supplier will not transfer or disclose (including by remote access) any IBM Personal Data across borders without IBM's prior written consent. If IBM provides such consent, the parties will cooperate to ensure compliance with applicable data protection laws. If SCCs are required by those laws, Supplier will promptly enter into the SCCs upon IBM's request.

5.2 Regarding EU SCCs:

(a) If Supplier is not established in an Adequate Country: (i) Supplier is hereby entering into EU SCCs with IBM on Supplier's own behalf as a Data Importer; and (ii) Supplier will enter into written agreements with each approved Subprocessor that is a Data Importer, in accordance with Clause 11 of the EU SCCs, and will provide IBM with copies of those agreements upon request.

(b) If Supplier is established in an Adequate Country, then Supplier is hereby entering into EU SCCs with IBM on behalf of each Subprocessor that is a Data Importer. If Supplier is unable to do so for any such Subprocessor, then Supplier will provide IBM with the EU SCCs signed by that Subprocessor for IBM's countersignature prior to allowing the Subprocessor to Process any IBM Personal Data.

(c) The EU SCCs between IBM and Supplier will serve either as EU SCCs between a Controller and Processor or as a back-to-back written agreement between 'data importer' and 'sub-processor' in accordance with Clause 11 of the EU SCCs, as the facts require. In the event of any conflict between the EU SCCs and these Terms, the EU SCCs will prevail.

5.3 Other Controllers, such as Customers or affiliates, may request to become additional 'data exporters' in accordance with Clause 9(2) of the EU SCCs. Supplier is hereby agreeing on its own behalf and on behalf of its Subprocessors to any such request. IBM will inform Supplier of any

additional ‘data exporters’ and, in turn, Supplier will inform its Subprocessors that are Data Importers of those additional ‘data exporters’.

6. Assistance and Records

6.1 Taking into account the nature of Processing, Supplier will assist IBM by having appropriate technical and organizational measures to fulfill obligations associated with Data Subject requests and rights. Supplier will also assist IBM in ensuring compliance with obligations relating to the security of Processing, the notification and communication of a Security Breach and the creation of data protection impact assessments, including prior consultation with the responsible regulator, if required, taking into account the information available to Supplier.

6.2 Supplier will maintain an up-to-date record of the name and contact details of each Subprocessor, including each Subprocessor’s representative and data protection officer. Upon request, Supplier will provide this record to IBM on a schedule that allows IBM to timely respond to any demand from a Customer or other third-party.

This Article applies if Supplier has access to IBM Source Code. Supplier will comply with the requirements of this Article and by doing so protect IBM Source Code against loss, destruction, alteration, accidental or unauthorized disclosure, accidental or unauthorized access, and unlawful forms of Handling. The requirements of this Article extend to all IT applications, platforms, and infrastructure that Supplier operates or manages in providing Deliverables and Services and in Handling IBM Technology, including all development, testing, hosting, support, operations, and data center environments.

1. Security Requirements

As used below,

Prohibited Country means any country: (a) that the US Government has designated as a foreign adversary under the May 15, 2019 Executive Order on Securing the Information and Communications Technology and Services Supply Chain, (b) listed in accordance with Section 1654 of the U.S. National Defense Authorization Act of 2019, or (c) identified as a "Prohibited Country" in the Transaction Document.

1.1 Supplier will not distribute or place any IBM Source Code in escrow for the benefit of any third party.

1.2 Supplier will not permit any IBM Source Code to reside on servers located in a Prohibited Country. Supplier will not permit anyone, including its Personnel, located in a Prohibited Country or visiting a Prohibited Country (for the extent of any such visit), for any reason whatsoever, to access or use any IBM Source Code, regardless of where that IBM Source Code is located globally, and Supplier will not permit any development, testing, or other work to occur in a Prohibited Country that would require such access or use.

1.3 Supplier will not place or distribute IBM Source Code in any jurisdiction where law or interpretation of law requires disclosure of Source Code to any third party. If there is a change of law or interpretation of law in a jurisdiction where IBM Source Code is located that may cause Supplier to be required to disclose such Source Code to a third party, Supplier will immediately destroy or immediately remove such IBM Source Code from such jurisdiction, and will not place any additional IBM Source Code in such jurisdiction if such law or interpretation of law remains operative.

1.4 Supplier will not, directly or indirectly, take any action, including entering into any agreement, that would cause Supplier, IBM or any third-party to incur a disclosure obligation under Sections 1654 or 1655 of the U.S. National Defense Authorization Act of 2019. For clarity, except as may be expressly permitted in the Transaction Document or associated base agreement between the parties, Supplier is not permitted to disclose IBM Source Code to any third-party, under any circumstance, without IBM's prior written consent.

1.5 If IBM notifies Supplier, or a third party notifies either party that: (a) Supplier has allowed IBM Source Code to be brought into a Prohibited Country or any jurisdiction subject to Section 1.3 above, (b) Supplier has otherwise released, accessed, or used IBM Source Code in a manner not permitted by the Transaction Document or associated base or other agreement between the parties or (c) Supplier has violated Section 1.4 above, then without limiting IBM's rights to address such non-compliance at law or in equity or under the Transaction Document or associated base or other agreement between the parties: (i) if such notification is to Supplier, then Supplier will promptly share the notification with IBM; and (ii) Supplier, at IBM's reasonable direction, will investigate and

remediate the matter on the schedule that IBM reasonably determines (after consultation with Supplier).

1.6 If IBM reasonably believes that changes in Supplier's policies, procedures, controls, or practices with respect to Source Code access may be necessary to address cyber security, intellectual property theft or similar or related risks (including the risk that without such changes IBM might be restricted from selling to certain Customers or into certain markets or otherwise be unable to satisfy Customer security or supply chain requirements), then IBM may contact Supplier to discuss the actions necessary to address such risks, including changes to such policies, procedures, controls or practices. Upon IBM's request, Supplier will cooperate with IBM in evaluating whether such changes are necessary and in implementing appropriate, mutually agreed changes.

Article V, Secure Development

This Article applies if Supplier will provide its or third-party Source Code to IBM or will have access to IBM Source Code, or IBM will rebrand any of Supplier's Deliverables as an IBM product or service.

1. Security Readiness

1.1 Supplier will cooperate with IBM's internal processes that assess the security readiness of IBM products and services that are dependent upon any of Supplier's Deliverables, including by timely and fully responding to requests for information, whether through documents, other records, interviews of relevant Supplier Personnel, or the like.

2. ISO 20243 Certification

2.1 Supplier will obtain a certification of compliance with ISO 20243, Information technology, Open Trusted Technology Provider, TM Standard (O-TTPS), Mitigating maliciously tainted and counterfeit products (either a self-assessed certification or one based on the assessment of a reputable independent auditor). In the alternative, if Supplier requests in writing and IBM approves in writing, Supplier will obtain a certification of compliance with a substantially equivalent industry standard addressing secure development and supply chain practices (either a self-assessed certification or one based on the assessment of a reputable independent auditor, if and as IBM approves).

2.2 Supplier will obtain the certification of compliance with ISO 20243 or a substantially equivalent industry standard (if IBM approves in writing) by 180 Days after the effective date of the Transaction Document and then renew the certification every 12 months thereafter (with each renewal against the then most current version of the applicable standard, i.e., ISO 20243 or, where IBM has approved in writing, a substantially equivalent industry standard addressing secure development and supply chain practices).

2.3 Supplier will, upon request, promptly provide to IBM a copy of the certifications Supplier is obligated to obtain, per Sections 2.1 and 2.2 above.

3. Security Vulnerabilities

As used below,

Error Correction means bug fixes and revisions that correct errors or deficiencies, including Security Vulnerabilities, in Deliverables.

Mitigation means any known means of lessening or avoiding the risks of a Security Vulnerability.

Security Vulnerability means a state in the design, coding, development, implementation, testing, operation, support, maintenance, or management of a Deliverable that allows an attack by anyone that could result in unauthorized access or exploitation, including: (a) access to, controlling or disrupting operation of a system, (b) access to, deleting, altering or extracting data or (c) changes of identity, authorizations or permissions of users or administrators. A Security Vulnerability may exist regardless of whether a Common Vulnerabilities and Exposures (CVE) ID or any scoring or official classification is assigned to it.

3.1 Supplier represents and warrants that it will: (a) use Industry Best Practices to identify Security Vulnerabilities, including through continuous static and dynamic source code application security scanning, open source security scanning and system vulnerability scanning, and (b) comply with the requirements of these Terms to help prevent, detect and correct Security Vulnerabilities in Deliverables and in all IT applications, platforms, and infrastructure in and through which Supplier creates and provides Services and Deliverables.

3.2 If Supplier becomes aware of a Security Vulnerability in a Deliverable or any such IT application, platform, or infrastructure, Supplier will provide IBM with an Error Correction and Mitigations for all versions and releases of the Deliverables in accordance with the Severity Levels and time frames defined in the tables below:

Severity Level*
Emergency Security Vulnerability – is a Security Vulnerability that constitutes a severe and potentially global threat. IBM designates Emergency Security Vulnerabilities in its sole discretion, regardless of CVSS Base Score.
Critical – is a Security Vulnerability that has a CVSS Base Score from 9 to 10.0
High – is a Security Vulnerability that has a CVSS Base Score from 7.0 to 8.9
Medium – is a Security Vulnerability that has a CVSS Base Score from 4.0 to 6.9 **Low** – is a Security Vulnerability that has a CVSS Base Score from 0.0 to 3.9

Time Frames				
Emergency	***Critical***	***High***	***Medium***	***Low***
4 Days or less, as determined by IBM's Chief Information Security Office	30 Days	30 Days	90 Days	Per Industry Best Practices

* In any case where a Security Vulnerability does not have a readily assigned CVSS Base Score, Supplier will apply a Severity Level that is appropriate for the nature and circumstances of such vulnerability.

3.3 For a Security Vulnerability that has been publicly disclosed and for which Supplier has not yet provided any Error Correction or Mitigation to IBM, Supplier will implement any technically feasible additional security controls that may mitigate the risks of the vulnerability.

3.4 If IBM is dissatisfied with Supplier's response to any Security Vulnerability in a Deliverable or any application, platform, or infrastructure referenced above, then without prejudice to any other rights of IBM, Supplier will promptly arrange for IBM to discuss its concerns directly with a Supplier Vice President or equivalent executive that is responsible for delivery of the Error Correction.

3.5 Examples of Security Vulnerabilities include third-party code or end-of-service (EOS) open source code, where these types of code no longer receive security fixes.

Article VI, Corporate Systems' Access

This Article applies if Supplier employees will have access to any Corporate System.

1. General Terms

1.1 IBM will determine whether to authorize Supplier employees to access Corporate Systems. If IBM so authorizes, then Supplier will comply, and will cause its employees with such access to comply, with the requirements of this Article.

1.2 IBM will identify the means by which Supplier employees may access Corporate Systems, including whether such employees will access Corporate Systems through IBM or Supplier provided Devices.

1.3 Supplier employees may only access Corporate Systems, and may only use the Devices that IBM authorizes for that access, to provide Services. Supplier employees may not use the Devices that IBM so authorizes to provide services to any other person or entity, or to access any Supplier or third-party IT systems, networks, applications, websites, email tools, collaboration tools, or the like for or in connection with the Services.

1.4 For clarity, Supplier employees may not use the Devices that IBM authorizes to access Corporate Systems for any personal reason (e.g., Supplier employees may not store personal files such as music, videos, pictures or other like items on such Devices and cannot use the Internet from such Devices for personal reasons).

1.5 Supplier employees will not copy IBM Materials that are accessible through a Corporate System without IBM's prior written approval (and will never copy any IBM Materials to a portable storage device, such as a USB, an external hard drive, or other like items).

1.6 Upon request, Supplier will confirm, by employee name, the specific Corporate Systems which its employees are authorized to access, and have accessed, over any time period that IBM identifies.

1.7 Supplier will notify IBM within twenty-four (24) hours after any Supplier employee with access to any Corporate System is no longer: (a) employed by Supplier or (b) working on activities that require such access. Supplier will work with IBM to ensure that access for such former or current employees is immediately revoked.

1.8 Supplier will immediately report any actual or suspected security incidents (such as loss of an IBM or Supplier Device or unauthorized access to a Device or data, materials or other information of any kind) to IBM and cooperate with IBM in the investigation of such incidents.

1.9 Supplier may not permit any agent, independent contractor or subcontractor employee to access any Corporate System, without IBM's prior written consent; if IBM provides that consent, then Supplier will contractually commit those persons and their employers to comply with the requirements of this

Article as if those persons were Supplier employees, and will be responsible to IBM for all actions and omissions to act by any such person or employer with respect to such Corporate System access.

2. Device Software

2.1 Supplier will direct its employees to timely install all Device software that IBM requires to facilitate access to Corporate Systems in a secure manner. Neither Supplier nor its employees will interfere with the operations of that software or the security features that the software enables.

2.2 Supplier and its employees will adhere to the Device configuration rules that IBM sets and otherwise work with IBM to help ensure that the software functions as IBM intends. For example, Supplier will not override software website blocking or automated patching features.

2.3 Supplier employees may not share the Devices they use to access Corporate Systems, or their Device usernames, passwords, or the like, with any other person.

2.4 If IBM authorizes Supplier employees to access Corporate Systems using Supplier Devices, then Supplier will install and run an operating system on those Devices that IBM approves and will upgrade to a new version of that operating system or a new operating system within a reasonable time after IBM so instructs.

3. Oversight and Cooperation

3.1 IBM has the unqualified rights to monitor and remediate potential intrusion and other cyber security threats in whatever ways, from whatever locations, and using whatever means IBM believes is necessary or appropriate, without prior notice to Supplier or any Supplier employee or others. As examples of such rights, IBM may, at any time, (a) perform a security test on any Device, (b) monitor, recover through technical or other means and review communications (including emails from any email accounts), records, files, and other items stored in any Device or transmitted through any Corporate System, and (c) acquire a full forensic image of any Device. If IBM needs Supplier's cooperation to exercise its rights, Supplier will fully and timely satisfy IBM's requests for such cooperation (including, for example, requests to securely configure any Device, install monitoring or other software on any Device, share system level connection details, engage in incident response measures on any Device, and provide physical access to any Device for IBM to obtain a full forensic image or otherwise, and similar and related requests).

3.2 IBM may revoke access to Corporate Systems at any time, for any Supplier employee or all Supplier employees, without prior notice to Supplier or any Supplier employee or others, if IBM believes that doing so is necessary to protect IBM.

3.3 IBM's rights are not blocked, lessened, or restricted in any way by any provision of the Transaction Document, the associated base agreement between the parties, or any other agreement between the parties, including any provision that may require data, materials or other information of any kind to reside only in a select location or locations or that may require that only persons from a select location or locations access such data, materials or other information.

4. IBM Devices

4.1 IBM will retain title to all IBM Devices, with Supplier bearing the risk of loss of the Devices, including due to theft, vandalism, or negligence. Supplier will not make or permit any alterations to IBM Devices without IBM's prior written consent, with an alteration being any change to a Device, including any change to Device software, applications, security design, security configuration, or physical, mechanical, or electrical design.

4.2 Supplier will return all IBM Devices within 5 business days after the need for those Devices to provide Services ends, and if IBM requests, destroy all data, materials and other information of any kind on those Devices at the same time, without retaining any copy, by following Industry Best Practices to permanently erase all such data, materials and other information. Supplier will pack and return IBM

Devices in the same condition as delivered to Supplier, other than reasonable wear and tear, at its own expense to the location that IBM identifies. Supplier's failure to comply with any obligation in this Section 4.2 constitutes a material breach of the Transaction Document and associated base agreement and any related agreement between the parties, with the understanding that an agreement is "related" if access to any Corporate System facilitates Supplier's tasks or other activities under that agreement.

4.3 IBM will provide support for IBM Devices (including Device inspection and preventive and remedial maintenance). Supplier will promptly advise IBM of the need for remedial service.

4.4 For software programs that IBM owns or has the right to license, IBM grants Supplier a temporary right to use, store, and make sufficient copies to support its authorized use of IBM Devices. Supplier may not transfer programs to anyone, make copies of software license information, or disassemble, decompile, reverse engineer, or otherwise translate any program unless expressly permitted by applicable law without the possibility of contractual waiver.

5. Updates

5.1 Notwithstanding anything to the contrary in the Transaction Document or associated base agreement between the parties, upon written notice to Supplier and without the need for obtaining Supplier's consent, IBM may update, supplement, or otherwise amend this Article to address any requirement under applicable law or Customer obligation, to reflect any development in security best practices, or otherwise as IBM believes necessary to protect

Corporate Systems or IBM.

Article VII, Staff Augmentation

This Article applies where Supplier's employees will devote all of their working time to provide Services for IBM, will perform all of those Services on IBM premises, Customer premises or from their homes, and will only provide Services using IBM Devices to access Corporate Systems.

1. Access to Corporate Systems; IBM's Environments

1.1 Supplier may only perform Services by accessing Corporate Systems using Devices that IBM provides.

1.2 Supplier will comply with the terms set forth in Article VI (Corporate Systems' Access), for all access to Corporate Systems.

1.3 IBM provided Devices are the only Devices that Supplier and its employees may use to provide

Services and may only be used by Supplier and its employees to provide Services. For clarity, in no event may Supplier or its employees use any other devices to provide Services or use IBM Devices for any other Supplier customer or for any purpose other than providing Services to IBM.

1.4 Supplier employees using IBM Devices may share IBM Materials with each other and store such materials on the IBM Devices, but only to the limited extent that such sharing and storage is necessary to successfully perform Services.

1.5 Except with respect to such storage within the IBM Devices, in no event may Supplier or its employees remove any IBM Materials from the IBM repositories, environments, tools or infrastructure where they are retained by IBM.

1.6 For clarity, Supplier and its employees are not authorized to transfer any IBM Materials to any Supplier repositories, environments, tools, or infrastructure, or any other Supplier systems, platforms, networks or the like, without IBM's prior written consent.

1.7 Article VIII (Technical and Organizational Measures, General Security) does not apply to Supplier's Services where Supplier's employees will devote all of their working time to provide Services for IBM, will perform all of those Services on IBM premises, Customer premises or from their homes, and will only provide Services using IBM Devices to access Corporate Systems. Otherwise, Article VIII applies to Supplier's Services.

Article VIII, Technical and Organizational Measures, General Security

This Article applies if Supplier provides any Services or Deliverables to IBM, unless Supplier will only have access to IBM BCI in providing those Services and Deliverables (i.e., Supplier will not Process any other IBM Data or have access to any other IBM Materials or to any Corporate System) or Supplier provides all of its Services and Deliverables in a staff augmentation model pursuant to Article VII, including Section 1.7 thereof.

Supplier will comply with the requirements of this Article and by doing so protect: (a) IBM Materials against loss, destruction, alteration, accidental or unauthorized disclosure, and accidental or unauthorized access, (b) IBM Data from unlawful forms of Processing and (c) IBM Technology from unlawful forms of Handling. The requirements of this Article extend to all IT applications, platforms, and infrastructure that Supplier operates or manages in providing Deliverables and Services and in Handling IBM Technology, including all development, testing, hosting, support, operations, and data center environments.

1. Security Policies

1.1 Supplier will maintain and follow IT security policies and practices that are integral to Supplier's business, mandatory for all Supplier Personnel, and consistent with Industry Best Practices.

1.2 Supplier will review its IT security policies and practices at least annually and amend them as Supplier deems necessary to protect the IBM Materials.

1.3 Supplier will maintain and follow standard, mandatory employment verification requirements for all new employee hires, and extend such requirements to all Supplier Personnel and wholly-owned Supplier subsidiaries. Those requirements will include criminal background checks to the extent permitted by local laws, proof of identity validation, and additional checks that Supplier deems necessary. Supplier will periodically repeat and revalidate these requirements, as it deems necessary.

1.4 Supplier will provide security and privacy education to its employees annually and require all such employees to certify each year that they will comply with Supplier's ethical business conduct, confidentiality, and security policies, as set out in Supplier's code of conduct or similar documents. Supplier will provide additional policy and process training to persons with administrative access to any components of the Services, Deliverables or IBM Materials, with such training specific to their role and support of the Services, Deliverables and IBM Materials, and as necessary to maintain required compliance and certifications.

1.5 Supplier will design security and privacy measures to protect and maintain the availability of IBM Materials, including through its implementation, maintenance, and compliance with policies and procedures which require security and privacy by design, secure engineering, and secure operations, for all Services and Deliverables and for all Handling of IBM Technology.

2. Security Incidents

2.1 Supplier will maintain and follow documented incident response policies consistent with Industry Best Practices for computer security incident handling.

2.2 Supplier will investigate unauthorized access or unauthorized use of IBM Materials and will define and execute an appropriate response plan.

2.3 Supplier will promptly (and in no event any later than 48 hours) notify IBM after becoming aware of any Security Breach. Supplier will provide such notification through the IBM Global Procurement Support Portal at https://www.ibm.com/procurement/procSupport. Supplier will provide IBM with reasonably requested information about such breach and the status of any Supplier remediation and restoration activities. By way of example, reasonably requested information may include logs demonstrating privileged, administrative, and other access to Devices, systems or applications, forensic images of Devices, systems or applications, and other similar items, to the extent relevant to the breach or Supplier's remediation and restoration activities.

2.4 Supplier will provide IBM with reasonable assistance to satisfy any legal obligations (including obligations to notify regulators or Data Subjects) of IBM, IBM affiliates and Customers (and their customers and affiliates) in relation to a Security Breach.

2.5 Supplier will not inform or notify any third party about a Security Breach unless IBM approves doing so in writing or if required by law, and Supplier will notify IBM in writing prior to distributing any legally required notification to any third-party.

2.6 In case of a Security Breach which arises from Supplier's breach of any obligation under these Terms:

(a) Supplier will be responsible for any costs it incurs, as well as actual costs that IBM incurs, in providing notification of the Security Breach to applicable regulators, other government and relevant industry self-regulatory agencies, the media (if required by applicable law), Data Subjects, Customers, and others,

(b) if IBM requests, Supplier will establish and maintain at Supplier's own expense a call-center to respond to questions from Data Subjects about the Security Breach and its consequences, for 1 year after the date on which such Data Subjects were notified of the Security Breach, or as required by any applicable data protection law, whichever affords greater protection. IBM and Supplier will work together to create the scripts and other materials to be used by call-center staff when responding to inquiries. Alternatively, on written notice to Supplier, IBM may establish and maintain its own callcenter, in lieu of having Supplier establish a call-center, and Supplier will reimburse IBM the actual costs that IBM incurs in establishing and maintaining such call-center, and

(c) Supplier will reimburse IBM the actual costs that IBM incurs in providing credit monitoring and credit restoration services for 1 year after the date on which individuals affected by the breach who choose to register for such services were notified of the Security Breach, or as required by any applicable data protection law, whichever affords greater protection.

3. Physical Security and Entry Control (as used below, "Facility" means a physical location where Supplier hosts, processes or otherwise accesses IBM Materials).

3.1 Supplier will maintain appropriate physical entry controls, such as barriers, card-controlled entry points, surveillance cameras, and manned reception desks, to protect against unauthorized entry into Facilities.

3.2 Supplier will require authorized approval for access to Facilities and controlled areas within Facilities, including any temporary access, and will limit access by job role and business need. If Supplier grants temporary access, its authorized employee will escort any visitor while in the Facility and any controlled areas.

3.3 Supplier will implement physical access controls, including multi-factor access controls that are consistent with Industry Best Practices, to appropriately restrict entrance to controlled areas within Facilities, will log all entry attempts, and retain such logs for at least one year.

3.4 Supplier will revoke access to Facilities and controlled areas within Facilities upon (a) separation of an authorized Supplier employee or (b) the authorized Supplier employee no longer having a valid business need for access. Supplier will follow formal documented separation procedures that include prompt removal from access control lists and surrender of physical access badges.

3.5 Supplier will take precautions to protect all physical infrastructure used to support the Services and Deliverables and the Handling of IBM Technology against environmental threats, both naturally occurring and man-made, such as excessive ambient temperature, fire, flood, humidity, theft, and vandalism.

4. Access, Intervention, Transfer, and Separation Control

4.1 Supplier will maintain documented security architecture of networks that it manages in its operation of the Services, its provision of Deliverables and its Handing of IBM Technology. Supplier will separately review such network architecture, and employ measures to prevent unauthorized network connections to systems, applications, and network devices, for compliance with secure segmentation, isolation, and defense in-depth standards. Supplier may not use wireless technology in its hosting and operations of any Hosted Services; otherwise, Supplier may use wireless networking technology in its delivery of Services and Deliverables and in its Handing of IBM Technology, but Supplier will encrypt and require secure authentication for any such wireless networks.

4.2 Supplier will maintain measures that are designed to logically separate and prevent IBM Materials from being exposed to or accessed by unauthorized persons. Further, Supplier will maintain appropriate isolation of its production, non-production, and other environments, and, if IBM Materials are already present within or are transferred to a non-production environment (for example to reproduce an error), then Supplier will ensure that the security and privacy protections in the non-production environment are equal to those in the production environment.

4.3 Supplier will encrypt IBM Materials in transit and at rest (unless Supplier demonstrates to IBM's reasonable satisfaction that encrypting IBM Materials at rest is technically infeasible). Supplier will also encrypt all physical media, if any, such as media containing backup files. Supplier will maintain documented procedures for secure key generation, issuance, distribution, storage, rotation, revocation, recovery, backup, destruction, access, and use associated with data encryption. Supplier will ensure that the specific cryptographic methods used for such encryption align with Industry Best Practices (such as NIST SP 800-131a).

4.4 If Supplier requires access to IBM Materials, Supplier will restrict and limit such access to the least level required to provide and support the Services and Deliverables. Supplier will require that such access, including administrative access to any underlying components (i.e., privileged access), will be individual, role based, and subject to approval and regular validation by authorized Supplier

employees following segregation of duty principles. Supplier will maintain measures to identify and remove redundant and dormant accounts. Supplier will also revoke accounts with privileged access within twenty-four (24) hours after the account owner's separation or the request by IBM or any authorized Supplier employee, such as the account owner's manager.

4.5 Consistent with Industry Best Practices, Supplier will maintain technical measures enforcing timeout of inactive sessions, lockout of accounts after multiple sequential failed login attempts, strong password or passphrase authentication, and measures requiring secure transfer and storage of such passwords and passphrases. Additionally, Supplier will utilize multi-factor authentication for all non-console based privileged access to any IBM Materials.

4.6 Supplier will monitor use of privileged access and maintain security information and event management measures designed to: (a) identify unauthorized access and activity, (b) facilitate a timely and appropriate response to such access and activity, and (c) enable audits by Supplier, IBM (pursuant to its verification rights in these Terms and audit rights in the Transaction Document or associated base or other related agreement between the parties) and others of compliance with documented Supplier policy.

4.7 Supplier will retain logs in which it records, in compliance with Industry Best Practices, all administrative, user, or other access or activity to or with respect to systems used in providing Services or Deliverables and in Handling IBM Technology (and will provide those logs to IBM upon request). Supplier will maintain measures designed to protect against unauthorized access, modification, and accidental or deliberate destruction of such logs.

4.8 Supplier will maintain computing protections for systems that it owns or manages, including end-user systems, and that it uses in providing Services or Deliverables or in Handling IBM Technology, with such protections including: endpoint firewalls, full disk encryption, signature and non-signature based endpoint detection and response technologies to address malware and advanced persistent threats, time based screen locks, and endpoint management solutions that enforce security configuration and patching requirements. In addition, Supplier will implement technical and operational controls that ensure only known and trusted end-user systems are allowed to use Supplier networks.

4.9 Consistent with Industry Best Practices, Supplier will maintain protections for data center environments where IBM Material are present or processed, with such protections including intrusion detection and prevention and denial of service attack countermeasures and mitigation.

5. Service and Systems Integrity and Availability Control

5.1 Supplier will: (a) perform security and privacy risk assessments at least annually, (b) perform security testing and assess vulnerabilities, including automated system and application security scanning and manual ethical hacking, before production release and annually thereafter as it concerns Services and Deliverables and annually with respect to its Handling of IBM Technology, (c) enlist a qualified independent third-party to perform penetration testing consistent with Industry Best Practices at least annually, with such testing including both automated and manual testing, (d) perform automated management and routine verification of compliance with security configuration requirements for each component of the Services and Deliverables and with respect to its Handling of IBM Technology, and (e) remediate identified vulnerabilities or noncompliance with its security configuration requirements based on associated risk, exploitability, and impact. Supplier will take reasonable steps to avoid disruption of Services when performing its tests, assessments, scans, and execution of remediation activities. Upon IBM's request, Supplier will provide IBM with a written summary of Supplier's then-most recent penetration testing activities, which report will at a

minimum include the name of the offerings covered by the testing, the number of systems or applications in-scope for the testing, the dates of the testing, the methodology used in the testing, and a high-level summary of findings.

5.2 Supplier will maintain policies and procedures designed to manage risks associated with the application of changes to the Services or Deliverables or to the Handling of IBM Technology. Prior to implementing such a change, including to affected systems, networks, and underlying components, Supplier will document in a registered change request: (a) a description of and reason for the change, (b) implementation details and schedule, (c) a risk statement addressing impact to the Services and Deliverables, customers of the Services, or IBM Materials, (d) expected outcome, (e) rollback plan, and (f) approval by authorized Supplier employees.

5.3 Supplier will maintain an inventory of all IT assets it uses in operating the Services, providing Deliverables and in Handling IBM Technology. Supplier will continuously monitor and manage the health (including capacity) and availability of such IT assets, Services, Deliverables and IBM Technology, including the underlying components of such assets, Services, Deliverables and IBM Technology.

5.4 Supplier will build all systems that it uses in the development or operation of Services and Deliverables and in its Handling of IBM Technology from predefined system security images or security baselines, which satisfy Industry Best Practices, such as the Center for Internet Security (CIS) benchmarks.

5.5 Without limiting Supplier's obligations or IBM's rights under the Transaction Document or associated base agreement between the parties with respect to business continuity, Supplier will separately assess each Service and Deliverable and each IT system used in Handling IBM Technology for business and IT continuity and disaster recovery requirements pursuant to documented risk management guidelines. Supplier will ensure that each such Service, Deliverable and IT system has, to the extent warranted by such risk assessment, separately defined, documented, maintained, and annually validated business and IT continuity and disaster recovery plans consistent with Industry Best Practices. Supplier will ensure that such plans are designed to deliver the specific recovery times that are set forth in Section 5.6 below.

5.6 The specific recovery point objectives ("**RPO**") and recovery time objectives ("**RTO**") with respect to any Hosted Service are: 24 hours RPO and 24 hours RTO; nevertheless, Supplier will comply with any shorter duration RPO or RTO that IBM has committed to a Customer, promptly after IBM notifies Supplier in writing of such shorter duration RPO or RTO (an email constitutes a writing). As it concerns all other Services provided by Supplier to IBM, Supplier will ensure that its business continuity and disaster recovery plans are designed to deliver RPO and RTO that enable Supplier to remain in compliance with all of its obligations to IBM under the Transaction Document and associated base agreement between the parties, and these Terms, including its obligations to timely provide testing, support, and maintenance.

5.7 Supplier will maintain measures designed to assess, test, and apply security advisory patches to the Services and Deliverables and associated systems, networks, applications, and underlying components within the scope of those Services and Deliverables, as well as the systems, networks, applications, and underlying components used to Handle IBM Technology. Upon determining that a security advisory patch is applicable and appropriate, Supplier will implement the patch pursuant to documented severity and risk assessment guidelines. Supplier's implementation of security advisory patches will be subject to its change management policy.

5.8 If IBM has a reasonable basis for believing that hardware or software that Supplier provides to IBM may contain intrusive elements, such as spyware, malware, or malicious code, then Supplier will timely cooperate with IBM in investigating and remediating IBM's concerns.

6. Service Provisioning

6.1 Supplier will support "bring your own encryption", also known as "bring your own key", with respect to encryption of IBM Materials, unless Supplier demonstrates to IBM's reasonable satisfaction that such support is technically infeasible.

6.2 Supplier will support industry common methods of federated authentication for any IBM user or Customer accounts, with Supplier following Industry Best Practices in authenticating such IBM user or Customer accounts (such as by IBM centrally managed multi-factor Single Sign-On, using OpenID Connect or Security Assertion Markup Language).

7. Subcontractors. Without limiting Supplier's obligations or IBM's rights under the Transaction Document or associated base agreement between the parties with respect to the retention of subcontractors, Supplier will ensure that any subcontractor performing work for Supplier has instituted governance controls to comply with the requirements and obligations that these Terms place on Supplier.

8. Physical Media. Supplier will securely sanitize physical media intended for reuse prior to such reuse, and will destroy physical media not intended for reuse, consistent with Industry Best Practices for media sanitization.

Article IX, Hosted Services' Certifications and Reports

This Article applies if Supplier provides a Hosted Service to IBM.

1.1 Supplier will obtain the following certifications or reports within the time frames set forth below:

Certifications / Reports	Time Frame
With respect to Supplier's Hosted Services: Certification of compliance with ISO 27001, Information technology, Security techniques, Information security management systems, with such certification based on the assessment of a reputable independent auditor **Or** SOC 2 Type 2: A report by a reputable independent auditor demonstrating its review of Supplier's systems, controls and operations in accordance with a SOC 2 Type 2 (including, at a minimum, security, confidentiality, and availability)	Supplier will obtain the ISO 27001 certification by 120 Days after the effective date of the Transaction Document* or Assumption Date** and then renew the certification based on the assessment of a reputable independent auditor every 12 months thereafter (with each renewal against the then most current version of the standard) Supplier will obtain the SOC 2 Type 2 report by 240 Days after the effective date of the Transaction Document* or Assumption Date** and then obtain a new report by a reputable independent auditor demonstrating its review of Supplier's systems, controls and operations in accordance with a SOC 2 Type 2 (including, at a minimum, security, confidentiality, and availability) every 6 months thereafter * If, as of such effective date, Supplier provides a Hosted Service ** The date that Supplier assumes an obligation to provide a Hosted Service

1.2 If Supplier requests in writing, and IBM approves in writing, Supplier may obtain a substantially equivalent certification or report to those referenced above, with the understanding that the time frames set forth in the table above would apply unchanged with respect to the substantially equivalent certification or report.

1.3 Supplier will: (a) upon request, promptly provide to IBM a copy of each certification and report Supplier is obligated to obtain and (b) promptly resolve any internal control weaknesses noted during the SOC 2 or substantially equivalent (if IBM so approves) reviews.

1.4 Supplier will obtain any additional certification or report that IBM has committed to a Customer, provided that IBM first notifies Supplier in writing of such commitment and affords Supplier a sufficient time to do so (an email constitutes a writing). Supplier may seek assistance from IBM in funding the incremental costs of securing any such additional certification or report, where it is reasonable to do so (it would not be reasonable if such cost has already been factored into Supplier's fees). In those cases where it is reasonable for Supplier to seek funding assistance, Supplier's obligation to secure any additional certification or report will not begin until the parties have reached agreement on such assistance.

Article X, Cooperation, Verification and Remediation

This Article applies if Supplier provides any Services or Deliverables to IBM.

1. Supplier Cooperation

1.1 If IBM has reason to question whether any Services or Deliverables may have contributed, are contributing or will contribute to any cyber security concern, then Supplier will cooperate with any IBM inquiry regarding such concern, including by timely and fully responding to requests for information, whether through documents, other records, interviews of relevant Supplier Personnel, or the like.

1.2 The parties agree to: (a) furnish upon request to each other such further information, (b) execute and deliver to each other such other documents, and (c) do such other acts and things, all as the other party may reasonably request for the purpose of carrying out the intent of these Terms and the documents referred to in these Terms. For example, if IBM requests, Supplier will timely provide the privacy and security focused terms of its written contracts with Subprocessors and subcontractors, including, where Supplier has the right to do so, by granting access to the contracts themselves.

1.3 If IBM requests, Supplier will timely provide information on the countries where its Deliverables and the components of those Deliverables were manufactured, developed, or otherwise sourced.

2. Verification (as used below, "Facility" means a physical location where Supplier hosts, processes or otherwise accesses IBM Materials)

2.1 Supplier will maintain an auditable record demonstrating compliance with these Terms.

2.2 IBM, by itself or with an external auditor, may, upon 30 Days prior written notice to Supplier, verify Supplier's compliance with these Terms, including by accessing any Facility or Facilities for such purposes, though IBM will not access any data center where Supplier Processes IBM Data unless it has a good faith reason to believe that doing so would provide relevant information. Supplier will cooperate with IBM's verification, including by timely and fully responding to requests for information, whether through documents, other records, interviews of relevant Supplier Personnel, or the like. Supplier may offer proof of adherence to an approved code of conduct or industry certification or otherwise provide information to demonstrate compliance with these Terms, for IBM's consideration.

2.3 A verification will not occur more than once in any 12 month period, unless: (a) IBM is validating Supplier's remediation of concerns resulting from a previous verification during the 12 month period or (b) a Security Breach has arisen and IBM wishes to verify compliance with obligations relevant to the breach. In either case, IBM will provide the same 30 Days prior written notice as specified in Section 2.2 above, but the urgency of addressing a Security Breach may necessitate IBM conducting a verification on less than 30 Days prior written notice.

2.4 A regulator or other Controller may exercise the same rights as IBM in Sections 2.2 and 2.3, with the understanding that a regulator may exercise any additional rights it has under the law.

2.5 If IBM has a reasonable basis for concluding that Supplier is not compliant with any of these Terms (whether such basis arises from a verification under these Terms or otherwise), then Supplier will promptly remediate such non-compliance.

3. Anti-Counterfeiting Program

3.1 If Supplier's Deliverables include electronic components (e.g., hard disk drives, solid-state drives, memory, central processing units, logic devices or cables), Supplier will maintain and follow a documented counterfeit prevention program to, first and foremost, prevent Supplier from providing counterfeit components to IBM and, secondarily, promptly detect and remediate any case where Supplier mistakenly provides counterfeit components to IBM. Supplier will impose this same obligation to maintain and follow a documented counterfeit prevention program on all of its suppliers that provide electronic components that are included in Supplier's Deliverables to IBM.

4. Remediation

4.1 If Supplier fails to comply with any of its obligations under these Terms, and that failure causes a Security Breach, then Supplier will correct the failure in its performance and remediate the harmful effects of the Security Breach, with such performance and remediation at IBM's reasonable direction and schedule. IBM will have the right to participate in such remediation, as it believes appropriate or necessary. Supplier will be responsible for its costs and expenses in correcting its performance and for the remediation costs and expenses that the parties incur, and all such costs and expenses will be considered, as between the parties, to be direct damages, subject to any applicable cap on direct damages.

4.2 By way of example, remediation costs and expenses associated with a Security Breach could include those for detecting and investigating a Security Breach, determining responsibilities under applicable laws and regulations, providing breach notifications, establishing and maintaining call-centers, providing credit monitoring and credit restoration services, reloading data, correcting product defects (including through Source Code or other development), retaining third-parties to assist with the foregoing or other relevant activities, and other costs and expenses that are necessary to remediate the harmful effects of the Security Breach. For clarity, remediation costs and expenses would not include IBM's loss of profits, business, value, revenue, goodwill, or anticipated savings.