Cloud Services Agreement for G-Cloud 13

G-Cloud 13: In the event of conflicting terms, the order of precedence specified in the G-Cloud 13 Framework Agreement shall apply. The CSA and applicable Attachments and Transaction Documents are incorporated into each Call-Off Contract for the G-Cloud 13 Framework Agreement. Where "IBM" is used in TDs, the DSP or DPA, it shall mean "Supplier" and where "Client" is used in TDs, the DSP or DPA, it shall mean "Buyer". "Supplier Terms" shall mean the Agreement as defined herein.

The Agreement: This Cloud Services Agreement (CSA) and applicable Attachments and Transaction Documents are the agreement regarding each transaction under this CSA (together, the Agreement) under which Buyer may order Supplier Cloud Services which have been made available at GOV.UK Digital Marketplace.

Transaction Documents: Transaction Documents (TDs) detail the specifics of transactions, such as charges and a description of and information about the Supplier Cloud Services. Examples of TDs include statements of work, service descriptions, ordering documents and invoices. There may be more than one TD applicable to a transaction.

Attachments: Documents identified as Attachments provide supplemental terms that apply across certain types of transactions such as a solution attachment.

Any conflicting terms in an Attachment or TD that override terms of this CSA will be identified in the TD or Attachment accepted by the Buyer and only apply to the specific transaction.

1. Cloud Services

a.	**Supplier Cloud Services**	• Supplier Cloud Services are "as a service" Supplier offerings that Supplier makes available via a network, such as software as a service, platform as a service, or infrastructure as a service. • Each Supplier Cloud Service is described in a TD. • Supplier Cloud Services are designed to be available 24/7, subject to maintenance. Supplier will provide advance notice of scheduled maintenance. • Technical support and service level commitments, if any, are specified in an Attachment or TD.
b.	**Non-Supplier Services**	• Supplier may offer third party Cloud Services, or Supplier Cloud Services may enable access to third party Cloud Services (Non-Supplier Services). • A TD will identify any applicable third-party terms that govern Buyer's use of Non-Supplier Services. Use of Non-Supplier Services constitutes Buyer's agreement with the third-party terms. • Supplier is not a party to any third-party terms and is not responsible for Non-Supplier Services.
c.	**Order Acceptance**	• Buyer accepts the applicable Attachment or TD for Cloud Services by ordering, enrolling, using, or making a payment. • Supplier accepts Buyer's order by confirming the order or enabling access.
d.	**What Supplier Provides**	• Supplier provides the facilities, personnel, equipment, software, and other resources necessary for Supplier to provide Supplier Cloud Services. • Supplier provides generally available user guides and documentation to support Buyer's use of Supplier Cloud Services.
e.	**Enabling Software**	• Enabling Software is software that Buyer downloads to Buyer systems that facilitates the use of a Cloud Service and will be identified in a TD. • Enabling Software is not part of the Cloud Service and Buyer may use Enabling Software only in connection with use of the Cloud Service in accordance with any licensing terms specified in a TD. • The licensing terms will specify applicable warranties, if any. **Otherwise, Enabling Software is provided as is, without warranties of any kind.**
f.	**What Buyer Provides**	• Buyer will provide hardware, software, and connectivity to access and use the Cloud Services, including any required Buyer-specific URL addresses and associated certificates.
g.	**Right to Use and Buyer Responsibilities**	• Buyer's authorised users may access Cloud Services only to the extent of authorisations Buyer acquires.

- Buyer is responsible for the use of Cloud Services by any user who accesses the Cloud Services with Buyer's account credentials.

h. Acceptable Use Terms

- Cloud Services may not be used for unlawful, harmful, obscene, offensive, or fraudulent Content or activity. Examples of prohibited activities are advocating or causing harm, interfering with, or violating the integrity or security of a network or system, evading filters, sending unsolicited, abusive, or deceptive messages, introducing viruses or harmful code, or violating third party rights.
- Buyer may not use Cloud Services if failure or interruption of the Cloud Services could lead to death, serious bodily injury, or property or environmental damage.
- Buyer may not:
  - (1) reverse engineer any portion of a Cloud Service;
  - (2) assign or resell direct access to a Cloud Service to a third party outside Buyer's Enterprise; or
  - (3) combine a Cloud Service with Buyer's value add to create a Buyer branded solution that Buyer markets to its end user customers unless otherwise agreed by Supplier in writing.

i. Preview Cloud Services

- Cloud Services or features of Cloud Services are considered "preview" when Supplier makes such services or features available at no charge, with limited or pre-release functionality, or for a limited time to try available functionality. Examples of preview Cloud Services include beta, trial, no-charge, or preview-designated Cloud Services.
- Any preview Cloud Service is excluded from available service level agreements and may not be supported.
- Supplier may change or discontinue a preview Cloud Service at any time and without notice.
- Supplier is not obligated to release preview Cloud Services or make an equivalent service generally available.

2. Content and Data Protection

a. Content Buyer Provides

- Content consists of all data, software, and information that Buyer or its authorised users provides, authorises access to, or inputs to Supplier Cloud Services.
- Buyer grants the rights and permissions to Supplier, its affiliates, and contractors of either, to use, provide, store, and otherwise process Content solely for the purpose of providing the Supplier Cloud Services.
- Use of the Supplier Cloud Services will not affect Buyer's ownership or license rights in Content.

b. Use of Content

- Supplier, its affiliates, and contractors of either, will access and use the Content solely for the purpose of providing and managing the Supplier Cloud Service.
- Supplier will treat Content as confidential by only disclosing to Supplier employees and contractors to the extent necessary to provide the Supplier Cloud Services.

c. Buyer Responsibilities

- Buyer is responsible for obtaining all necessary rights and permissions to permit processing of Content in the Supplier Cloud Services.
- Buyer will make disclosures and obtain consent required by law before Buyer provides, authorises access, or inputs individuals' information, including personal or other regulated data, for processing in the Supplier Cloud Services.
- If any Content could be subject to governmental regulation or may require security measures beyond those specified by Supplier for the Supplier Cloud Services, Buyer will not provide, allow access to, or input the Content for processing in the Supplier Cloud Services unless specifically permitted in the applicable TD or unless Supplier has first agreed in writing to implement additional security and other measures.

d. Data Protection

- Supplier Data Security and Privacy Principles (DSP), apply for standard Supplier Cloud Services that are generally available. The current version of the DSP is included as **Appendix A** and new versions can be found at http://www.ibm.com/cloud/data-security
- Specific security features and functions of a Supplier Cloud Service will be described in the applicable Attachment or TD.

- Buyer is responsible for selecting, ordering, enabling, and using available data protection features appropriate to support Buyer's use of the Cloud Services.
- Buyer is responsible for assessing the suitability of the Cloud Services for the Content and Buyer's intended use. Buyer acknowledges that the Cloud Services used meet Buyer's requirements and processing instructions required to comply with applicable laws.

e. Supplier 's Data Processing Addendum

- Supplier 's Data Processing Addendum (DPA) can be found at http://ibm.com/dpa, the current version of the DPA is included as **Appendix B**.
- Each Supplier Cloud Service has a DPA Exhibit that specifies how Supplier will process Buyer's data. The applicable DPA Exhibit is included by reference in the TD.
- The DPA and applicable DPA Exhibit(s) apply to personal data contained in Content, if and to the extent: i) the European General Data Protection Regulation (EU/2016/679); or ii) other data protection laws identified at http://www.ibm.com/dpa/dpl apply.
- Upon request by either party, Supplier, Buyer, or affiliates of either, will enter into additional agreements as required by law in the prescribed form for the protection of regulated personal data included in Content. The parties agree (and will ensure that their respective affiliates agree) that such additional agreements will be subject to the terms of the Agreement.

f. Removal of Content

- For Supplier Cloud Services with self-managed features, Buyer can remove Content at any time. Otherwise, Supplier will return or remove Content from Supplier computing resources upon the expiration or cancellation of the Supplier Cloud Services, or earlier upon Buyer's request.
- Supplier may charge for certain activities performed at Buyer's request (such as delivering Content in a specific format).
- Supplier does not archive Content; however, some Content may remain in the Supplier Cloud Services backup files until expiration of such files as governed by Supplier 's backup retention practices.

3. Changes and Withdrawal of Cloud Services

a. Supplier Right to Change Cloud Services

- At any time and at Supplier 's discretion, Supplier may change:
  (1) the Supplier Cloud Services, including the corresponding published descriptions; and
  (2) the DSP and other published data security and privacy documentation for the Supplier Cloud Services.
- The intent of any change to the above will be to:
  (1) make available additional features and functionality;
  (2) improve and clarify existing commitments; or
  (3) maintain alignment to current adopted operational and security standards or applicable laws.
- The intent is not to degrade the security or data protection features or functionality of the Supplier Cloud Services.
- Changes to the published descriptions, DSP, or published other documents as specified above, will be effective when published or on the specified effective date.
- Any changes that do not meet conditions specified above will only take effect, and Buyer accepts, upon:
  (1) a new order;
  (2) the term renewal date for the Cloud Services that automatically renew; or
  (3) notification from Supplier of the change effective date for ongoing services that do not have a specified term.

b. Withdrawal of a Cloud Service

- Supplier may withdraw a Supplier Cloud Services on 12 months' notice.
- Supplier will continue to provide withdrawn Supplier Cloud Service for the remainder of Buyer's unexpired term or work with Buyer to migrate to another generally available Supplier offering.
- Non-Supplier Services may be discontinued at any time if the third party discontinues, or Supplier no longer makes available such services.

4. Warranties

a. Supplier Warrants

- Supplier warrants that it provides Supplier Cloud Services or other Supplier services using commercially reasonable care and skill and as described in the applicable TD.
- These warranties end when the Supplier Cloud Services or other Supplier services end.
- **These warranties are the exclusive warranties from Supplier and replace all other warranties, including the implied warranties or conditions of satisfactory quality, merchantability, non-infringement, and fitness for a particular purpose.**

b. Warranty Limitations

- **Supplier does not warrant uninterrupted or error-free operation of the Supplier Cloud Services.**
- **Supplier does not warrant it will correct all defects.**
- **While Supplier endeavours to provide security measures to keep all data secure, Supplier does not warrant Supplier can prevent all third-party disruptions or unauthorised third-party access.**
- **Supplier warranties will not apply if there has been misuse, modification, damage not caused by Supplier, or failure to comply with written instructions provided by Supplier.**
- **Supplier makes preview Cloud Services or Non-Supplier Services under the Agreement as-is, without warranties of any kind. Third parties may provide their own warranties to Buyer for Non-Supplier Services.**

5. Charges, Taxes, and Payment

a. Charges

- Buyer agrees to pay all applicable charges specified in a TD and charges for use in excess of authorisations.
- Charges are exclusive of any customs or other duty, tax, and similar levies imposed by any authority resulting from Buyer's acquisitions under the Agreement and will be invoiced in addition to such charges.
- Amounts are due upon receipt of the invoice and payable within 30 days of the invoice date to an account specified by Supplier and late payment fees may apply.
- Prepaid services must be used within the applicable period.
- Supplier does not give credits or refunds for any prepaid, one-time charges, or other charges already due or paid, except as provided in the Agreement.
- If Supplier commits to pricing as specified in a TD, Supplier will not change such pricing during the specified term. If there is not a specified commitment, then Supplier may change pricing on thirty days' notice.

b. Withholding Taxes

- Buyer agrees to:
  (1) pay withholding tax directly to the appropriate government entity where required by law;
  (2) furnish a tax certificate evidencing such payment to Supplier;
  (3) pay Supplier only the net proceeds after tax; and
  (4) fully cooperate with Supplier in seeking a waiver or reduction of such taxes and promptly complete and file all relevant documents.

c. Invoicing

- Supplier will invoice:
  (1) recurring charges at the beginning of the selected billing frequency term;
  (2) overage and usage charges in arrears; and
  (3) one-time charges upon Supplier 's acceptance of an order.

6. Liability and Indemnity

a. Liability for Damages

- Supplier 's entire liability for all claims related to the Agreement will not exceed the amount of any actual direct damages incurred by Buyer up to 125% of the amounts paid (if recurring charges, up to 12 months' charges apply) for the service that is the subject of the claim, regardless of the basis of the claim.
- **Supplier will not be liable for special, incidental, exemplary, indirect, or consequential damages, or lost profits, business, value, revenue, goodwill, or anticipated savings.**
- These limitations apply collectively to Supplier, its affiliates, contractors, and suppliers.

b. What Damages are Not Limited

- The following amounts are not subject to the above cap:
  (1) third party payments referred to in the Infringement Claims subsection below; and
  (2) damages that cannot be limited under applicable law.

c. Infringement Claims

- If a third party asserts a claim against Buyer that the Supplier Cloud Service infringes a patent or copyright, Supplier will defend Buyer against that claim and pay amounts finally awarded by a court against Buyer or included in a settlement approved by Supplier.
- To obtain Supplier's defense against and payment of infringement claims, Buyer must promptly:
  (1) notify Supplier in writing of the claim;
  (2) supply information requested by Supplier; and
  (3) allow Supplier to control, and reasonably cooperate in, the defense and settlement, including mitigation efforts.
- Supplier 's defense and payment obligations for infringement claims extend to claims based on Open-Source Code that Supplier selects and embeds in the Supplier Cloud Services. Open-Source Code is software code licensed from a third party meeting the Open-Source Definition defined at https://opensource.org/osd.

d. Claims Not Covered

- Supplier has no responsibility for claims based on:
  (1) non-Supplier products and services, including Non-Supplier Services;
  (2) items not provided by Supplier; or
  (3) any violation of law or third-party rights caused by Content, materials, designs, or specifications.

7. Term and Termination

a. Term of a Cloud Service

- The term begins on the date Supplier notifies Buyer that Buyer can access the Cloud Services.
- The ordering TD will specify whether the Cloud Services renew automatically, proceed on a continuous use basis, or terminate at the end of the term.
- For automatic renewal, unless Buyer provides written notice of non-renewal to Supplier or the Supplier Business Partner involved in the Cloud Services at least 30 days prior to the term expiration date, the Cloud Services will automatically renew for the specified term.
- For continuous use, the Cloud Services will continue to be available on a month-to-month basis until Buyer provides 30 days written termination notice to Supplier or the Supplier Business Partner involved in the Cloud Services. The Cloud Services will remain available until the end of the calendar month after the 30-day period.

b. Suspension of a Supplier Cloud Service

- Supplier may suspend or limit, to the extent necessary, Buyer's use of a Supplier Cloud Service if Supplier reasonably determines there is a:
  (1) material breach of Buyer's obligations;
  (2) security breach;
  (3) violation of law; or
  (4) breach of the Acceptable Use Terms.
- Supplier will provide notice prior to a suspension as commercially reasonable.

- If the cause of a suspension can reasonably be remedied, Supplier will provide notice of the actions Buyer must take to reinstate the Supplier Cloud Services. If Buyer fails to take such actions within a reasonable time, Supplier may terminate the Supplier Cloud Services.

c. Termination of Cloud Services

- Buyer may terminate the Supplier Cloud Services on 30 days' notice:
  (1) at the written recommendation of a government or regulatory agency following a change in either applicable law or the Supplier Cloud Services;
  (2) if a change to the Supplier Cloud Services causes Buyer to be noncompliant with applicable laws; or
  (3) if Supplier notifies Buyer of a change to the Supplier Cloud Services that has a material adverse effect on Buyer's use of the Supplier Cloud Services, provided that Supplier will have 90 days to work with Buyer to minimise such effect.
- In the event of any such Buyer termination above or a similar termination of a Non-Supplier Service, Supplier shall refund a portion of any prepaid amounts for the applicable Cloud Service for the period after the date of termination.
- Buyer may terminate the Supplier Cloud Services for material breach of Supplier 's obligations by giving notice and reasonable time to comply.
- If the Cloud Services are terminated for any other reason, Buyer will pay to Supplier, on the date of termination, the total amounts due per the Agreement.
- Upon termination, Supplier may assist Buyer in transitioning Content to an alternative technology for an additional charge and under separately agreed terms.

d. Termination of this CSA

- Either party may terminate this CSA:
  (1) without cause on at least 30 days' notice to the other after expiration or termination of its obligations under the Agreement; or
  (2) immediately for cause if the other is in material breach of the Agreement, provided the one who is not complying is given notice and reasonable time to comply.
- Any terms that by their nature extend beyond the Agreement termination remain in effect until fulfilled and apply to successors and assignees.
- Termination of this CSA does not terminate TDs, and provisions of this CSA as they relate to such TDs remain in effect until fulfilled or otherwise terminated in accordance with their terms.
- Failure to pay is a material breach.

8. Governing Laws and Geographic Scope

a. Compliance with Laws

- Each party is responsible for complying with:
  (1) laws and regulations applicable to its business and Content; and
  (2) import, export and economic sanction laws and regulations, including defense trade control regime of any jurisdiction, including the International Traffic in Arms Regulations and those of the United States that prohibit or restrict the export, re-export, or transfer of products, technology, services, or data, directly or indirectly, to or for certain countries, end uses or end users.

b. Applicable Laws

- Both parties agree to the application of the laws of England, without regard to conflict of law principles.
- The rights and obligations of each party are valid only in the country of Buyer's business address.
- If Buyer or any user exports or imports Content or uses any portion of the Cloud Services outside the country of Buyer's business address, Supplier will not serve as the exporter or importer, except as required by data protection laws.
- If any provision of the Agreement is invalid or unenforceable, the remaining provisions remain in full force and effect.
- Nothing in the Agreement affects statutory rights of consumers that cannot be waived or limited by contract.
- The United Nations Convention on Contracts for the International Sale of Goods does not apply to transactions under the Agreement.

9. General

a. Supplier 's Role

- Supplier is an independent contractor, not Buyer's agent, joint venturer, partner, or fiduciary.
- Supplier does not undertake to perform any of Buyer's regulatory obligations or assume any responsibility for Buyer's business or operations, and Buyer is responsible for its use of Cloud Services.
- Supplier is acting as an information technology provider only.
- Supplier 's direction, suggested usage, or guidance or use of the Cloud Services do not constitute medical, clinical, legal, accounting, or other licensed professional advice. Buyer and its authorised users are responsible for the use of the Cloud Services within any professional practice and should obtain their own expert advice.
- Each party is responsible for determining the assignment of its and its affiliates personnel, and their respective contractors, and for their direction, control, and compensation.

---

b. CSA Changes

- Supplier may change this CSA by providing Buyer at least three months' notice.
- CSA changes are not retroactive. They will only apply as of the effective date to:
  (1) new orders;
  (2) continuous Cloud Services that do not expire; and
  (3) renewals.
- For transactions with a defined renewable contract period stated in a TD, Buyer may request that Supplier defer the change effective date until the end of the current contract period.
- Buyer accepts changes by placing new orders, continuing use after the change effective date, or allowing transactions to renew after receipt of the change notice.
- Except as provided in this section and the Changes and Withdrawal of Cloud Services section above, all other changes to the Agreement must be in writing accepted by both parties.

---

c. Business Conduct

- Supplier maintains a robust set of business conduct and related guidelines covering conflicts of interest, market abuse, anti-bribery and corruption, and fraud.
- Supplier and its personnel comply with such policies and require contractors to have similar policies.

---

d. Business Contact and Account Usage Information

- Supplier, its affiliates, and contractors of either require use of business contact information and certain account usage information. This information is not Content.
- Business contact information is used to communicate and manage business dealings with the Buyer. Examples of business contact information include name, business telephone, address, email, and user ID.
- Account usage information is required to enable, provide, manage, support, administer, and improve Cloud Services. Examples of account usage information include digital information gathered using tracking technologies, such as cookies and web beacons during use of the Supplier Cloud Services.
- The Supplier Privacy Statement at https://www.ibm.com/privacy/ provides additional details with respect to Supplier 's collection, use, and handling of business contact and account usage information.
- When Buyer provides information to Supplier and notice to, or consent by, the individuals is required for such processing, Buyer will notify individuals and obtain consent.

---

e. Supplier Business Partners

- Supplier Business Partners who use or make available Cloud Services are independent from Supplier and unilaterally determine their prices and terms. Supplier is not responsible for their actions, omissions, statements, or offerings.
- If Supplier notifies Buyer their current Supplier Business Partner will no longer resell Cloud Services, Buyer may select to acquire auto renewing or continuous use Cloud Services directly from Supplier or from another authorised Supplier Business Partner.

---

f. Assignment

- Neither party may assign the Agreement, in whole or in part, without the prior written consent of the other.
- Supplier may assign rights to receive payments. Supplier will remain responsible to perform its obligations.

- Assignments by Supplier in conjunction with the sale of the portion of Supplier 's business that includes the Cloud Services is not restricted.
- Supplier may share this Agreement and related documents in conjunction with any assignment.

g. Enterprise Companies

- This CSA applies to Supplier and Buyer (accepting this CSA) and their respective Enterprise companies that provide or acquire Cloud Services under this CSA.
- The parties shall coordinate the activities of their own Enterprise companies under the CSA.
- Enterprise companies include:
  (1) companies within the same country that Buyer or Supplier control (by owning greater than 50% of the voting shares); and
  (2) any other entity that controls, is controlled by, or is under common control with Buyer or Supplier and has signed a participation agreement.

h. Notices and Administration

- All notices under the Agreement must be in writing and sent to the business address specified for the Agreement unless a party designates in writing a different address.
- The parties consent to the use of electronic means and facsimile transmissions for communications as a signed writing.
- Any reproduction of the Agreement made by reliable means is considered an original.
- The Agreement supersedes any course of dealing, discussions, or representations between the parties.
- Where approval, acceptance, consent, access, cooperation, or similar action by either party is required, such action will not be unreasonably delayed or withheld.

i. Cause of Action

- No right or cause of action for any third party is created by the Agreement or any transaction under it.
- Neither party will bring a legal action arising out of or related to the Agreement more than two years after the cause of action arose.
- Neither party is responsible for failure to fulfil its non-monetary obligations due to causes beyond its control.
- Each party will allow the other reasonable opportunity to comply before it claims the other has not met its obligations.

j. Global Resources

- Supplier may use personnel and resources in locations worldwide, including contractors, to support the delivery of Supplier Cloud Services.
- Buyer's use of the Cloud Services may result in the transfer of Content, including personal data, across country borders.
- A list of countries where Content may be transferred and processed for a Supplier Cloud Service is included in the applicable TD.
- Supplier is responsible for the obligations under the Agreement even if Supplier uses a contractor and will have appropriate agreements in place to enable Supplier to meet its obligations for the Supplier Cloud Services.

k. Other Services

- Supplier may offer additional customisation, configuration, or other services to support Cloud Services, as detailed in a TD.

Data Security and Privacy Principles

1. Definitions

Capitalized terms used herein have the meanings given below or if not defined below, the meanings given in the applicable written contract between IBM and Client for the IBM Services.

Client – is the entity to which IBM is providing the IBM Services under an IBM Services Document.

Components – are the application, platform, or infrastructure elements of an IBM Service that IBM operates and manages.

Content – consists of all data, software, and information that Client or its authorized users provide, authorize access to, or input to IBM Services.

DSP – is this IBM Data Security and Privacy Principles document.

IBM Cloud Services – are "as a service" IBM offerings that IBM makes available via a network, such as software as a service, platform as a service, or infrastructure as a service.

IBM Services Document – is a Transaction Document and any other document that is incorporated into a written contract between IBM and a Client and that addresses details of a specific IBM Service.

IBM Services – are (a) IBM Cloud Services, (b) other IBM service offerings, including infrastructure or application service offerings that IBM delivers and dedicates to or customizes for a Client, and (c) any other services, including consulting, maintenance, or support, that IBM provides to a Client.

Security Incident – is an unauthorized access and unauthorized use of Content.

Transaction Document – is a document that details the specifics of transactions, such as charges and a description of and information about an IBM Cloud Service. Examples of Transaction Documents include statements of work, service descriptions, ordering documents and invoices for an IBM Cloud Service. There may be more than one Transaction Document applicable to a transaction.

2. Overview

The technical and organizational measures provided in this DSP apply to IBM Services (including any Components) only where IBM has expressly agreed to comply with the DSP in a written contract between IBM and Client. For clarity, those measures do not apply where Client is responsible for security and privacy or as specified below or in an IBM Services Document.

a. Client is responsible for determining whether an IBM Service is suitable for Client's use and implementing and managing security and privacy measures for components that IBM does not provide or manage within the IBM Services. Examples of Client responsibilities for IBM Services include: (1) the security of systems and applications built or deployed by the Client upon an infrastructure as a service or platform as a service offering or upon infrastructure, Components or software that IBM manages for a Client, and (2) Client end-user access control and application level security configuration for a software as a service offering that IBM manages for a Client or an application service offering that IBM delivers to a Client.

b. Client acknowledges that IBM may modify this DSP from time to time at IBM's sole discretion and such modifications will replace prior versions as of the date that IBM publishes the modified version. Notwithstanding anything to the contrary in any written contract between IBM and Client, the intent of any modification will be to: (1) improve or clarify existing commitments, (2) enable IBM to appropriately prioritize its security focus to address evolving data and cybersecurity threats and issues, (3) maintain alignment to current adopted standards and applicable laws, or (4) provide additional features and functionality. Modifications will not degrade the security or data protection features or functionality of IBM Services.

c. In the event of any conflict between this DSP and an IBM Services Document, the IBM Services Document will prevail and if the conflicting terms are in a Transaction Document, they will be identified as overriding the terms of this DSP and will only apply to the specific transaction.

3. Data Protection

a. IBM will treat all Content as confidential by not disclosing Content except to IBM employees, contractors, and suppliers (including subprocessors), and only to the extent necessary to deliver the IBM Services.

b. Security and privacy measures for each IBM Service are implemented in accordance with IBM's security and privacy by design practices to protect Content processed by an IBM Service, and to maintain the availability of such Content pursuant to the applicable written contract between IBM and Client, including applicable IBM Services Documents.

c. Additional security and privacy information specific to an IBM Service may be available in the relevant IBM Services Document or other standard documentation to aid in Client's initial and ongoing assessment of an IBM Service's suitability for Client's use. Such information may include evidence of stated certifications and accreditations, information related to

such certifications and accreditations, data sheets, FAQs, and other generally available documentation. IBM will direct Client to available standard documentation if asked to complete Client-preferred security or privacy questionnaires.

4. Security Policies

a. IBM will maintain and follow written IT security policies and practices that are integral to IBM's business and mandatory for all IBM employees. The IBM Chief Information Security Officer will maintain responsibility and executive oversight for such policies, including formal governance and revision management, employee education, and compliance enforcement.

b. IBM will review its IT security policies at least annually and amend such policies as IBM deems reasonable to maintain protection of IBM Services and Content.

c. IBM will maintain and follow its standard mandatory employment verification requirements for all new hires and will extend such requirements to wholly owned IBM subsidiaries. In accordance with IBM internal processes and procedures, these requirements will be periodically reviewed and include, but may not be limited to, criminal background checks, proof of identity validation, and additional checks as deemed necessary by IBM. Each IBM company is responsible for implementing these requirements in its hiring process as applicable and permitted under local law.

d. IBM employees will complete IBM's security and privacy education annually and certify each year that they will comply with IBM's ethical business conduct, confidentiality, and security policies, as set out in IBM's Business Conduct Guidelines. Additional training will be provided to any persons granted privileged access to Compon ents that is specific to their role within IBM's operation and support of the IBM Services, and as required to maintain compliance and accreditations stated in any relevant IBM Services Document.

5. Compliance

a. For standard (non-custom) IBM Cloud Services, the measures implemented and maintained by IBM within each IBM Cloud Service will be subject to annual certification of compliance with ISO 27001 or SSAE SOC 2, or both, unless stated otherwise in an IBM Services Document.

b. Additionally, IBM will maintain compliance and accreditation for the IBM Services as defined in an IBM Services Document.

c. Upon request, IBM will provide evidence of the compliance and accreditation required by 5a. and 5b., such as certificates, attestations, or reports resulting from accredited independent third-party audits (accredited independent third-party audits will occur at the frequency required by the relevant standard).

d. IBM is responsible for these data security and privacy measures even if IBM uses a contractor or supplier (including subprocessors) in the delivery or support of an IBM Service.

6. Security Incidents

a. IBM will maintain and follow documented incident response policies consistent with National Institute of Standards and Technology, United States Department of Commerce (NIST) guidelines or equivalent industry standards for computer security incident handling and will comply with the data breach notification terms of the applicable written contract between IBM and Client.

b. IBM will investigate Security Incidents of which IBM becomes aware, and, within the scope of the IBM Services, IBM will define and execute an appropriate response plan. Client may notify IBM of a suspected vulnerability or incident by submitting a request through the incident reporting process sp ecific to the IBM Service (as referenced in an IBM Services Document) or, in the absence of such process, by submitting a technical support request.

c. IBM will notify Client without undue delay upon confirmation of a Security Incident that is known or reasonably suspected by IBM to affect Client. IBM will provide Client with reasonably requested information about such Security Incident and the status of any IBM remediation and restoration activities.

7. Physical Security and Entry Control

a. IBM 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 IBM managed facilities (data centers) used to host the IBM Services. Auxiliary entry points into such data centers, such as delivery areas and loading docks, will be controlled and isolated from computing resources.

b. Access to IBM-managed data centers and controlled areas within those data centers will be limited by job role and subject to authorized approval. Such access will be logged, and such logs will be retained for not less than one year. IBM will revoke access to IBM-managed data centers upon separation of an authorized employee. IBM will follow formal documented separation procedures that include prompt removal from access control lists and surrender of physical access badges.

c. Any person granted temporary permission to enter an IBM-managed data center facility or a controlled area within such a data center will be registered upon entering the premises, must provide proof of identity upon registration, and will be escorted by authorized personnel. Any temporary authorization to enter, including deliveries, will be scheduled in advance and require approval by authorized personnel.

d. IBM will take precautions to protect the physical infrastructure of IBM managed data center facilities against environmental threats, both naturally occurring and man-made, such as excessive ambient temperature, fire, flood, humidity, theft, and vandalism.

8. Access, Intervention, Transfer and Separation Control

a. IBM will maintain a documented security architecture for Components. IBM will separately review such security architecture, including measures designed to prevent unauthorized network connections to systems, applications and network devices, for compliance with its secure segmentation, isolation, and defense-in-depth standards prior to implementation.

b. IBM may use wireless networking technology in its maintenance and support of the IBM Services and associated Components. Such wireless networks, if any, will be encrypted and require secure authentication and will not provide direct access to IBM Cloud Services networks. IBM Cloud Services networks do not use wireless networking technology.

c. IBM will maintain measures for an IBM Service that are designed to logically separate and prevent Content from being exposed to or accessed by unauthorized persons. IBM will maintain appropriate isolation of its production and non-production environments, and, if Content is transferred to a non-production environment, for example to reproduce an error at Client's request, security and privacy protections in the non-production environment will be equivalent to those in production.

d. IBM will encrypt Content not intended for public or unauthenticated viewing when transferring Content over public networks and enable use of a cryptographic protocol, such as HTTPS, SFTP, or FTPS, for Client's secure transfer of Content to and from the IBM Services over public networks.

e. IBM will encrypt Content at rest if and as specified in an IBM Services Document. If an IBM Service includes management of cryptographic keys, IBM will maintain documented procedures for secure key generation, issuance, distribution, storage, rotation, revocation, recovery, backup, destruction, access, and use.

f. If IBM requires access to Content to provide the IBM Services, and if such access is managed by IBM, IBM will restrict access to the minimum level required. Such access, including administrative access to any underlying Components (privileged access), will be individual, role-based, and subject to approval and regular validation by authorized IBM personnel following the principles of segregation of duties. IBM will maintain measures to identify and remove redundant and dormant accounts with privileged access and will promptly revoke such access upon the account owner's separation or upon the request of authorized IBM personnel, such as the account owner's manager.

g. Consistent with industry standard practices, and to the extent natively supported by each Component, IBM will maintain technical measures enforcing timeout of inactive sessions, lockout of accounts after multiple sequential failed login attempts, strong password or passphrase authentication, password change frequency, and secure transfer and storage of such passwords and passphrases.

h. IBM will monitor use of privileged access and maintain security information and event management measures designed to: (1) identify unauthorized access and activity, (2) facilitate a timely and appropriate response, and (3) enable internal and independent third-party audits of compliance with documented IBM policy.

i. Logs in which privileged access and activity are recorded will be retained in compliance with IBM's worldwide records management plan. IBM will maintain measures designed to protect against unauthorized access, modification, and accidental or deliberate destruction of such logs.

j. To the extent supported by native device or operating system functionality, IBM will maintain computing protections for its end-user systems that include, but may not be limited to, endpoint firewalls, full disk encryption, signature-based malware detection and removal, time-based screen locks, and endpoint management solutions that enforce security configuration and patching requirements.

k. IBM will securely sanitize physical media intended for reuse prior to such reuse, and will destroy physical media not intended for reuse, consistent with NIST guidelines for media sanitization.

9. Service Integrity and Availability Control

a. IBM will: (1) perform security and privacy risk assessments of the IBM Services at least annually, (2) perform security testing and vulnerability assessments of the IBM Services before production release and at least annually thereafter, (3) enlist a qualified independent third party, IBM X-Force™ or, if specified in an IBM Services Document, another qualified testing service to perform penetration testing of the IBM Cloud Services, at least annually, (4) perform automated vulnerability scanning of underlying Components of the IBM Services against industry security configuration best practices, (5) remediate identified vulnerabilities from security testing and scanning, based on associated risk,

exploitability, and impact, and (6) take reasonable steps to avoid disruption to the IBM Services when performing its tests, assessments, scans, and execution of remediation activities.

b. IBM will maintain measures designed to assess, test, and apply security advisory patches to the IBM Services and associated systems, networks, applications, and underlying Components within the scope of the IBM Services. Upon determining that a security advisory patch is applicable and appropriate, IBM will implement the patch pursuant to documented severity and risk assessment guidelines, based on Common Vulnerability Scoring System ratings of patches, when available. Implementation of security advisory patches will be subject to IBM change management policy.

c. IBM will maintain policies and procedures designed to manage risks associated with the application of changes to IBM Services. Prior to implementation, changes to an IBM Service, including its systems, networks, and underlying Components, will be documented in a registered change request that includes a description of and reason for the change, implementation details and schedule, a risk statement addressing impact to the IBM Service and its clients, expected outcome, rollback plan, and documented approval by authorized personnel.

d. IBM will maintain an inventory of all information technology assets used in its operation of IBM Services. IBM will continuously monitor and manage the health, including capacity, and availability of IBM Services and underlying Components.

e. Each IBM Service will be separately assessed for business continuity and disaster recovery requirements through appropriate business impact analysis and risk assessments intended to identify and prioritize critical business functions. Each IBM Service will have, to the extent warranted by such risk assessments, separately defined, documented, maintained, and annually validated business continuity and disaster recovery plans consistent with industry standard practices. Recovery point and time objectives for an IBM Service, if provided for in the relevant IBM Services Document, will be established with consideration given to the IBM Service's architecture and intended use. Physical media intended for off-site storage, if any, such as media containing backup files, will be encrypted prior to transport.

Data Processing Addendum

This Data Processing Addendum (DPA) and its applicable DPA Exhibits apply to the Processing of Personal Data by IBM on behalf of Client (Client Personal Data) subject to the General Data Protection Regulation 2016/679 (GDPR) or any other data protection laws identified at http://www.ibm.com/dpa/dpl (together 'Data Protection Laws') in order to provide services (Services) pursuant to the Agreement between Client and IBM. DPA Exhibits for each Service will be provided in the applicable Transaction Document (TD). This DPA is incorporated into the Agreement. Capitalized terms used and not defined herein have the meanings given them in the applicable Data Protection Laws. In the event of conflict, the DPA Exhibit prevails over the DPA which prevails over the rest of the Agreement.

1. Processing

1.1 Client is: (a) a Controller of Client Personal Data; or (b) acting as Processor on behalf of other Controllers and has been instructed by and obtained the authorization of the relevant Controller(s) to agree to the Processing of Client Personal Data by IBM as Client's subprocessor as set out in this DPA. Client appoints IBM as Processor to Process Client Personal Data. If there are other Controllers, Client will identify and inform IBM of any such other Controllers prior to providing their Personal Data, in accordance with the DPA Exhibit.

1.2 A list of categories of Data Subjects, types of Client Personal Data, Special Categories of Personal Data and the processing activities is set out in the applicable DPA Exhibit for a Service. The duration of the Processing corresponds to the duration of the Service, unless otherwise stated in the DPA Exhibit. The purpose and subject matter of the Processing is the provision of the Service as described in the Agreement.

1.3 IBM will Process Client Personal Data according to Client's documented instructions. The scope of Client's instructions for the Processing of Client Personal Data is defined by the Agreement, and, if applicable, Client's and its authorized users' use and configuration of the features of the Service. Client may provide further legally required instructions regarding the Processing of Client Personal Data (Additional Instructions) as described in Section 10.2. If IBM notifies Client that an Additional Instruction is not feasible, the parties shall work together to find an alternative. If IBM notifies the Client that neither the Additional Instruction nor an alternative is feasible, Client may terminate the affected Service, in accordance with any applicable terms of the Agreement. If IBM believes an instruction violates the Data Protection Laws, IBM will immediately inform Client, and may suspend the performance of such instruction until Client has modified or confirmed its lawfulness in documented form.

1.4 Client shall serve as a single point of contact for IBM. As other Controllers may have certain direct rights against IBM, Client undertakes to exercise all such rights on their behalf and to obtain all necessary permissions from the other Controllers. IBM shall be discharged of its obligation to inform or notify another Controller when IBM has provided such information or notice to Client. Similarly, IBM will serve as a single point of contact for Client with respect to its obligations as a Processor under this DPA.

1.5 IBM will comply with all Data Protection Laws in respect of the Services applicable to IBM as Processor. IBM is not responsible for determining the requirements of laws or regulations applicable to Client's business, or that a Service meets the requirements of any such applicable laws or regulations. As between the parties, Client is responsible for the lawfulness of the Processing of the Client Personal Data. Client will not use the Services in a manner that would violate applicable Data Protection Laws.

2. Technical and organizational measures

2.1 Client and IBM agree that IBM will implement and maintain the technical and organizational measures set forth in the applicable DPA Exhibit (TOMs) which ensure a level of security appropriate to the risk for IBM's scope of responsibility. TOMs are subject to technical progress and further development. Accordingly, IBM reserves the right to modify the TOMs provided that the functionality and security of the Services are not degraded.

3. Data Subject Rights and Requests

3.1 IBM will inform Client of requests from Data Subjects exercising their Data Subject rights (e.g., including but not limited to rectification, deletion and blocking of data) addressed directly to IBM regarding Client Personal Data. Client shall be responsible to handle such requests of Data Subjects. IBM will reasonably assist Client in handling such Data Subject requests in accordance with Section 10.2.

3.2 If a Data Subject brings a claim directly against IBM for a violation of their Data Subject rights, Client will reimburse IBM for any cost, charge, damages, expenses or loss arising from such a claim, to the extent that IBM has notified Client about the claim and given Client the opportunity to cooperate with IBM in the defense and settlement of the claim. Subject to the terms of the Agreement, Client may claim from IBM damages resulting from Data Subject claims for a violation of their Data Subject rights caused by IBM's breach of its obligations under this DPA and the respective DPA Exhibit.

4. Third Party Requests and Confidentiality

4.1 IBM will not disclose Client Personal Data to any third party, unless authorized by the Client or required by law. If a government or Supervisory Authority demands access to Client Personal Data, IBM will notify Client prior to disclosure, unless such notification is prohibited by law.

4.2 IBM requires all of its personnel authorized to Process Client Personal Data to commit themselves to confidentiality and not Process such Client Personal Data for any other purposes, except on instructions from Client or unless required by applicable law.

5. Audit

5.1 IBM shall allow for, and contribute to, audits, including inspections, conducted by the Client or another auditor mandated by the Client in accordance with the following procedures:

a. Upon Client's written request, IBM will provide Client or its mandated auditor with the most recent certifications and/or summary audit report(s), which IBM has procured to regularly test, assess and evaluate the effectiveness of the TOMs, to the extent set out in the DPA Exhibit.

b. IBM will reasonably cooperate with Client by providing available additional information concerning the TOMs, to help Client better understand such TOMs.

c. If further information is needed by Client to comply with its own or other Controllers audit obligations or a competent Supervisory Authority's request, Client will inform IBM in writing to enable IBM to provide such information or to grant access to it.

d. To the extent it is not possible to otherwise satisfy an audit right mandated by applicable law or expressly agreed by the Parties, only legally mandated entities (such as a governmental regulatory agency having oversight of Client's operations), the Client or its mandated auditor may conduct an onsite visit of the IBM facilities used to provide the Service, during normal business hours and only in a manner that causes minimal disruption to IBM's business, subject to coordinating the timing of such visit and in accordance with any audit procedures described in the DPA Exhibit in order to reduce any risk to IBM's other customers.

Any other auditor mandated by the Client shall not be a direct competitor of IBM with regard to the Services and shall be bound to an obligation of confidentiality.

5.2 Each party will bear its own costs in respect of paragraphs a. and b. of Section 5.1, otherwise Section 10.2 applies accordingly.

6. Return or Deletion of Client Personal Data

6.1 Upon termination or expiration of the Agreement IBM will either delete or return Client Personal Data in its possession as set out in the respective DPA Exhibit, unless otherwise required by applicable law.

7. Subprocessors

7.1 Client authorizes the engagement of other Processors to Process Client Personal Data (Subprocessors). A list of the current Subprocessors is set out in the respective DPA Exhibit. IBM will notify Client in advance of any addition or replacement of the Subprocessors as set out in the respective DPA Exhibit. Within 30 days after IBM's notification of the intended change, Client can object to the addition of a Subprocessor on the basis that such addition would cause Client to violate applicable legal requirements. Client's objection shall be in writing and include Client's specific reasons for its objection and options to mitigate, if any. If Client does not object within such period, the respective Subprocessor may be commissioned to Process Client Personal Data. IBM shall impose substantially similar but no less protective data protection obligations as set out in this DPA on any approved Subprocessor prior to the Subprocessor initiating any Processing of Client Personal Data.

7.2 If Client legitimately objects to the addition of a Subprocessor and IBM cannot reasonably accommodate Client's objection, IBM will notify Client. Client may terminate the affected Services as set out in the Agreement, otherwise the parties shall cooperate to find a feasible solution in accordance with the dispute resolution process.

8. Transborder Data Processing

8.1 In the case of a transfer of Client Personal Data to a country not providing an adequate level of protection pursuant to the Data Protection Laws (Non-Adequate Country), the parties shall cooperate to ensure compliance with the applicable Data Protection Laws as set out in the following Sections or at the Data Protection Laws at http://www.ibm.com/dpa/dpl. If Client believes the measures are not sufficient to satisfy the legal requirements, Client shall notify IBM and the parties shall work together to find an alternative.

8.2 By entering into the Agreement, Client and IBM are entering into EU Standard Contractual Clauses as set out in the applicable DPA Exhibit (EU SCC) if Client, IBM, or both are located in a Non-Adequate Country. If the EU SCC are not required because both parties are located in a country considered adequate by the Data Protection Laws, but during the Service the country where IBM or Client is located becomes a Non-Adequate Country, the EU SCC will apply.

The parties acknowledge that the applicable module of the EU SCC will be determined by their role as Controller and/or Processor under the circumstances of each case and are responsible for determining the correct role undertaken in order to fulfil the appropriate obligations under the applicable module.

8.3 Client agrees that the EU SCC, including any claims arising from them, are subject to the terms set forth in the Agreement, including the limitations of liability. In case of conflict, the EU SCC shall prevail.

8.4 IBM will enter into the EU SCC with each Subprocessor located in a Non-Adequate Country as listed in the respective DPA Exhibit.

9. Personal Data Breach

9.1 IBM will notify Client without undue delay after becoming aware of a Personal Data Breach with respect to the Services. IBM will promptly investigate the Personal Data Breach if it occurred on IBM infrastructure or in another area IBM is responsible for and will assist Client as set out in Section 10.

10. Assistance

10.1 IBM will assist Client by technical and organizational measures for the fulfillment of Client's obligation to comply with the rights of Data Subjects and in ensuring compliance with Clients obligations relating to the security of Processing, the notification and communication of a Personal Data Breach and the Data Protection Impact Assessment, including prior consultation with the responsible Supervisory Authority, if required, taking into account the nature of the processing and the information available to IBM.

10.2 Client will make a written request for any assistance referred to in this DPA. IBM may charge Client no more than a reasonable charge to perform such assistance or an Additional Instruction, such charges to be set forth in a quote and agreed in writing by the parties, or as set forth in an applicable change control provision of the Agreement. If Client does not agree to the quote, the parties agree to reasonably cooperate to find a feasible solution in accordance with the dispute resolution process.