UK G-Cloud 15 Framework Agreement

AWS EMEA SARL, UK Branch - Supplier Terms

January 2026

Submitted By:

AWS EMEA SARL, UK Branch

aws-ukps-frameworks@amazon.com

Supplier Terms

1. The Supplier Terms that shall be incorporated to a Call-Off Contract under the Framework are as listed below. Any definitions used in this document shall have the same meaning as set out in Joint Schedule 1 (Definitions), unless otherwise defined.

2. The Buyer acknowledges that these Supplier Terms may be updated from time to time.
3. Should the Buyer choose to (i) purchase products or Services that are not offered on the Platform, or (ii) consume Services outside of the Terms stated in the Order Form, such products and services are not subject to the terms of the Framework Agreement, Call-Off Contract or these Supplier Terms and instead are governed exclusively by the terms of the Amazon Web Services on-line click through Customer Agreement (https://aws.amazon.com/agreement/) (as updated from time to time). Buyers acknowledge that Supplier is unable to and has no responsibility to monitor Buyer accounts or limiting Buyers to stay within the Framework Agreement terms. This is solely a Buyer responsibility.

4. For the avoidance of doubt, the Supplier provides cloud computing services only. No physical goods are supplied under the Framework Agreement. Accordingly, Clause 3.2 (Goods) of the General Terms shall not apply to Call-Off Contracts awarded under the Framework Agreement.

Supplier Standard Terms

5. The Supplier Standard Terms are:
   - The Supplier Acceptable Use Policy listed below:

     AWS Acceptable Use Policy: https://aws.amazon.com/aup/

   - The Supplier Data Processing Agreement listed below:
     a. AWS Data Processing Addendum: https://d1.awsstatic.com/legal/aws-dpa/aws-dpa.pdf; and
     b. UK GDPR Addendum to the AWS Data Processing Addendum: https://d1.awsstatic.com/legal/aws-dpa/aws-uk-gdpr-dpa.pdf
   - The Supplier Specific Shared Responsibility Model set out in Appendix 1 to these Supplier Terms.

Supplier Service Specific Terms

6. The Supplier Service Specific Terms are:
   - The Supplier SLA listed below:

     AWS Service Level Agreements (SLAs): https://aws.amazon.com/legal/service-level-agreements/

   - The Supplier Licence Terms listed below:
     a. AWS Intellectual Property License: https://aws.amazon.com/legal/aws-ip-license-terms/;
     b. AWS Service Terms to the extent that the service terms relate to the Cloud Product that is being provided under the Contract: https://aws.amazon.com/service-terms/ ; and
     c. AWS Enterprise Support Additional Terms and Conditions set out in Appendix 2 to these Supplier Terms.

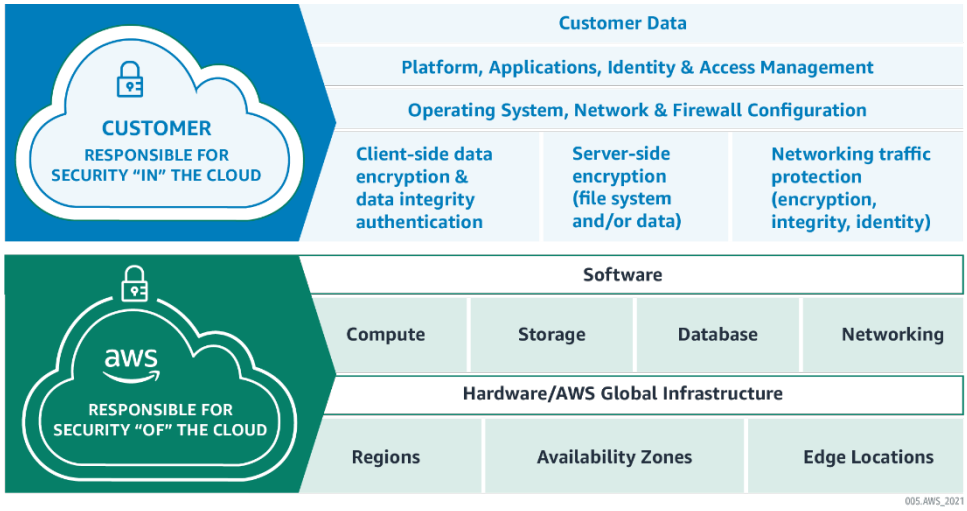
Appendix 1

Supplier Specific Shared Responsibility Model

1. Security and compliance is a shared responsibility between AWS and the Customer ("Buyer"). This shared responsibility model can help relieve Buyer's operational burdens as AWS operates, manages and controls the components from the host operating system and virtualisation layer down to the physical security of the facilities in which the service operates. Buyer controls how it architects and secures its applications and data in the AWS Cloud. As shown in the image below, this differentiation of responsibility is commonly referred to as Security "of" the Cloud versus Security "in" the Cloud. Further information is available on the AWS Compliance site (https://aws.amazon.com/compliance/shared-responsibility-model/).

2. This shared responsibility model supplements the AWS Customer Agreement available at http://aws.amazon.com/agreement, as updated from time to time between Customer and AWS, or other agreement between Customer and AWS governing Customer's use of the Services (the "Agreement"). The following clauses of the AWS Customer Agreement apply as between AWS and a Buyer: Clause 1 (AWS Responsibilities); Clause 2 (Your Responsibilities); Clause 4 (Suspension); Clause 6 (Proprietary Rights); Clause 8 (Disclaimers); Clause 10 (Modifications to the Agreement) and Clause 12 (Definitions).

3. AWS shall not be required to perform the Agreement in any way that does not align with this shared responsibility model.



4. **AWS responsibility "Security of the Cloud":** AWS is responsible for protecting the infrastructure that runs all of the services offered in the AWS Cloud. This infrastructure is composed of the hardware, software, networking, and facilities that run AWS services. AWS operates, manages, and controls the infrastructure components that customers build upon.

5. **Customer responsibility "Security in the Cloud":** Buyer assumes responsibility and management of the guest operating system (including updates and security patches), other associated application software as well as the configuration of the AWS provided security group firewall. Buyer responsibility will be determined by the AWS services that Buyer selects. This determines the amount of configuration work Buyer must perform as part of its security responsibilities. Buyer will review and comply with the AWS Documentation (https://docs.aws.amazon.com/ and https://docs.aws.amazon.com/security/).

6. Under the shared responsibility model, Buyer has the responsibility to ensure the protection and security of its data and content. AWS provides tools and service offerings to assist Buyer. AWS strongly recommends that Buyer uses AWS services such as Key Management Service, CloudTrail, Security Hub and GuardDuty to ensure that Buyer is in compliance with its own data protection obligations and Data Protection Legislation.

7. Buyer is responsible for all activities that occur under its account, regardless of whether the activities are authorised by Buyer or undertaken by Buyer, its employees or a third party. AWS is not responsible for unauthorised access to Buyer accounts. Buyer must ensure that its data and content and the use of Buyer data and content or the AWS services will not violate AWS policies including the AWS Acceptable Use Policy, AWS Privacy Notice and AWS service terms, or any applicable law. Buyer is solely responsible for the development, content, operation, maintenance, and use of its data and content.

8. Buyer is responsible for properly configuring and using AWS services and otherwise taking appropriate action to secure, protect and backup Buyer accounts, data and content in a manner that will provide appropriate security and protection, which might include use of encryption to protect Buyer data and content from unauthorised access, and routinely archiving Buyer data and content. AWS log-in credentials and private keys generated by the services are for Buyer internal use only and Buyer cannot sell, transfer or sublicense them to anyone else, except that Buyer may disclose its private key to agents and subcontractors performing work on Buyer's behalf. Buyer, not AWS, is responsible for their users' use of Buyer data and content and use of AWS services.

9. **Security Standards:** AWS has implemented and will maintain the technical and organizational measures described in the Security Standards. In particular, AWS has implemented and will maintain the following technical and organizational measures:

    a) security of the AWS Network as set out in Section 1.1 of the Security Standards;
    b) physical security of the facilities as set out in Section 1.2 of the Security Standards;
    c) measures to control access rights for authorized personnel to the AWS Network as set out in Section 1.3 of the Security Standards; and
    d) processes for regularly testing, assessing and evaluating the effectiveness of the technical and organizational measures implemented by AWS as described in Section 2 of the Security Standards.

10. **Minimum architecture requirements:** Customer agrees and acknowledges that it will issue all necessary instructions via the AWS console, and take all other necessary actions, to implement at least the minimum architecture requirements specified in Annex 2 (Minimum architecture requirements).

11. Notice:

(a) To You. We may provide any notice to you under this Agreement by:

(i) posting a notice on the AWS Site; or

(ii) sending a message to the email address then associated with your account.

Notices we provide by posting on the AWS Site will be effective upon posting and notices we provide by email will be effective when we send the email. It is your responsibility to keep your email address current. You will be deemed to have received any email sent to the email address then associated with your account when we send the email, whether or not you actually receive the email.

(b) To Us. To give us notice under this Agreement, you must contact AWS by facsimile transmission or personal delivery, overnight courier or registered or certified mail to the facsimile number 352 2789 0057 or mailing address, 38 Avenue John F. Kennedy, L-1855, Luxembourg, as applicable, for Amazon Web Services EMEA SARL. We may update the facsimile number or address for notices to us by posting a notice on the AWS Site. Notices provided by personal delivery will be effective immediately. Notices provided by facsimile transmission or overnight courier will be effective one business day after they are sent. Notices provided registered or certified mail will be effective three business days after they are sent.

12. **Definitions:** Unless otherwise defined in the Agreement, all capitalized terms used in this shared responsibility model, including the annexes to the shared responsibility model, will have the meanings given to them below:

"AWS Content" means APIs, WSDLs, sample code, software libraries, command line tools, proofs of concept, templates, advice, information, programs (including credit programs) and any other Content made available by us and our affiliates related to use of the Services or on the AWS Site and other related technology (including any of the foregoing that are provided by our personnel). AWS Content does not include the Services or Third-Party Content.

"AWS Network" means the servers, networking equipment, and host software systems (for example, virtual firewalls) that are within AWS's control and are used to provide the Services.

"AWS Region" means the location(s) where Customer Data will be processed within the AWS Network.

"AWS Site" means http://aws.amazon.com (and any successor or related locations designated by us), as may be updated by us from time to time.

"Content" means software (including machine images), data, text, audio, video, or images.

"Security Standards" means the security standards appended to this shared responsibility model at Annex 1.

13. **Definition alignment:** The capitalized terms used in this shared responsibility model, including those used in the annexes to the shared responsibility model, and set out in the table below shall be construed as follows to align to the definitions in the G-Cloud 15 Framework Agreement and Call-Off Contract:

Addendum definition	**Interpretation**
Agreement	shall mean the Call Off Contract governing use of AWS services under the G-Cloud 15 Framework Agreement or the AWS Customer Agreement available at http://aws.amazon.com/agreement as updated from time to time between Customer and AWS.
AWS, we, us, or **our**	shall mean the Supplier.
Customer	shall mean the Buyer.
Customer Content	shall mean Buyer Content.
Customer Data	shall include Buyer Personal Data uploaded to the Services under Buyer's accounts.
Service(s)	shall have the meaning set out in Schedule 1 (Definitions) of the Agreement.

Annex 1

Security Standards

Capitalized terms not otherwise defined in this annex have the meanings assigned to them in the Agreement.

1. Information Security Program. AWS will maintain an information security program designed to (a) enable Customer to secure Customer Content against accidental or unlawful loss, access, or disclosure, (b) identify reasonably foreseeable risks to the security and availability of the AWS Network, and (c) minimize physical and logical security risks to the AWS Network, including through regular risk assessment and testing. AWS will designate one or more employees to coordinate and be accountable for the information security program. AWS's information security program will include the following measures:

1.1 Logical Security.

1.1.1 Access Controls. AWS will make the AWS Network accessible only to authorized personnel, and only as necessary to maintain and provide the Services. AWS will maintain access controls and policies to manage authorizations for access to the AWS Network from each network connection and user, including through the use of firewalls or functionally equivalent technology and authentication controls. AWS will maintain access controls designed to (i) restrict unauthorized access to data, and (ii) segregate each customer's data from other customers' data.

1.1.2 Restricted User Access. AWS will (i) provision and restrict user access to the AWS Network in accordance with least privilege principles based on personnel job functions, (ii) require review and approval prior to provisioning access to the AWS Network above least privileged principles, including administrator accounts, (iii) require at least quarterly review of AWS Network access privileges and, where necessary, revoke AWS Network access privileges in a timely manner, and (iv) require two-factor authentication for access to the AWS Network from remote locations.

1.1.3 Vulnerability Assessments. AWS will perform regular external vulnerability assessments and penetration testing of the AWS Network, and will investigate identified issues and track them to resolution in a timely manner.

1.1.4 Application Security. Before publicly launching new Services or significant new features of Services, AWS will perform application security reviews designed to identify, mitigate, and remediate security risks.

1.1.5 Change Management. AWS will maintain controls designed to log, authorize, test, approve, and document changes to existing AWS Network resources, and will document change details within its change management or deployment tools. AWS will test changes according to its change management standards prior to migration to production. AWS will maintain processes designed to detect unauthorized changes to the AWS Network and track identified issues to a resolution.

1.1.6 Data Integrity. AWS will maintain controls designed to provide data integrity during transmission, storage, and processing within the AWS Network. The Services include controls that enable Customer to delete Customer Content from the AWS Network.

1.1.7 Business Continuity and Disaster Recovery. AWS will maintain a formal risk management program designed to support the continuity of its critical business functions ("**Business Continuity Program**"). The Business Continuity Program includes processes and procedures for identification of, response to, and recovery from, events that could prevent or materially impair AWS's provision of the Services (a "**BCP Event**"). The Business Continuity Program includes a three-phased approach that AWS will follow to manage BCP Events:

(i) Activation and Notification Phase. As AWS identifies issues likely to result in a BCP Event, AWS will escalate, validate and investigate those issues. During this phase, AWS will analyze the root cause of the BCP Event.

(ii) Recovery Phase. AWS assigns responsibility to the appropriate teams to take steps to restore normal system functionality or stabilize the affected Services.

(iii) Reconstitution Phase. AWS leadership reviews actions taken and confirms that the recovery effort is complete and the affected portions of the Services and AWS Network have been restored. Following such confirmation, AWS conducts a post-mortem analysis of the BCP Event.

1.1.8 Incident Management. AWS will maintain corrective action plans and incident response plans to respond to potential security threats to the AWS Network. AWS incident response plans will have defined processes to detect, mitigate, investigate, and report security incidents. The AWS incident response plans include incident verification, attack analysis, containment, data collection, and problem remediation. AWS will maintain an AWS Security Bulletin (as of the Effective Date, http://aws.amazon.com/security/security-bulletins/) which publishes and communicates security related information that may affect the Services and provides guidance to mitigate the risks identified.

1.1.9 Storage Media Decommissioning. AWS will maintain a media decommissioning process that is conducted prior to final disposal of storage media used to store Customer Content. Prior to final disposal, storage media that was used to store Customer Content will be degaussed, erased, purged, physically destroyed, or otherwise sanitized in accordance with industry standard practices designed to ensure that the Customer Content cannot be retrieved from the applicable type of storage media.

1.2 Physical Security.

1.2.1 Access Controls. AWS will (i) implement and maintain physical safeguards designed to prevent unauthorized physical access, damage, or interference to the AWS Network, (ii) use appropriate control devices to restrict physical access to the AWS Network to only authorized personnel who have a legitimate business need for such access, (iii) monitor physical access to the AWS Network using intrusion detection systems designed to monitor, detect, and alert appropriate personnel of security incidents, (iv) log and regularly audit physical access to the AWS Network, and (v) perform periodic reviews to validate adherence with these standards.

1.2.2 Availability. AWS will (i) implement redundant systems for the AWS Network designed to minimize the effect of a malfunction on the AWS Network, (ii) design the AWS Network to anticipate and tolerate hardware failures, and (iii) implement automated processes designed to move customer data traffic away from the affected area in the case of hardware failure.

1.3 AWS Employees.

1.3.1 Employee Security Training. AWS will implement and maintain employee security training programs regarding AWS information security requirements. The security awareness training programs will be reviewed and updated at least annually.

1.3.2 Background Checks. Where permitted by law, and to the extent available from applicable governmental authorities, AWS will require that each employee undergo a background investigation that is reasonable and appropriate for that employee's position and level of access to the AWS Network.

2. Continued Evaluation. AWS will conduct periodic reviews of the information security program for the AWS Network. AWS will update or alter its information security program as necessary to respond to new security risks and to take advantage of new technologies.

3. Security Event Notification. If AWS knows of a breach of the security measures described in these Security Standards that resulted in either (a) any unlawful access to any Customer Content stored on AWS's equipment or in AWS's facilities, or (b) any unauthorized access to such equipment or facilities, where in either case such access results in loss, disclosure, or alteration of Customer Content (each a "**Security Event**"), AWS will promptly (i) notify Customer of the Security Event, and (ii) take reasonable steps to mitigate the effects and to minimize any damage resulting from the Security Event.

Annex 2

Minimum Architecture Requirements

Each reference in this Annex 2 to specific Services includes equivalent alternative or replacement Service(s) that AWS makes available. At all times Customer will comply with all of the following:

1. **Encryption.** Encrypt all Customer Content in transit and at rest, using Strong Cryptography with associated key management processes and procedures. "**Strong Cryptography**" has the meaning given in Payment Card Industry (PCI) Data Security Standard (DSS) and Payment Application Data Security Standard (PA-DSS) Glossary of Terms, Abbreviations, and Acronyms, Version 3.2 (as updated from time to time).

2. **Security Architecture.**

   2.1. Promptly address any security and privacy events as notified at http://aws.amazon.com/security/security-bulletins/, except those categorized as "Informational".
   2.2. Monitor and evaluate software running in its AWS Enterprise Accounts for known and new vulnerabilities and take the steps necessary to address such vulnerabilities.

3. **Access Management.**

   3.1 Use multi-factor authentication to control access to root account credentials and not use root account credentials beyond initial account configuration, except in using Services for which AWS Identity and Access Management (IAM) is not available.
   3.2 Require each user to have unique security credentials that are rotated at least quarterly.
   3.3 Use multifactor authentication or federated credentials for all authentications and grant users and groups only the minimum privileges necessary.
   3.4 Restrict permissions in Security Groups and Access Control Lists to only those users required for Customer's use of the Services.
   3.5 Restrict permitted source and destination authorizations to only those required for Customer's use of the Services.
   3.6 Apply resource-based policies to limit access to Services only to authorized parties.

4. **Backup and Redundancy.**

   4.1 Back up Customer Content in accordance with industry-standard security configurations.
   4.2 Store all Customer Content redundantly in more than one AWS Region.

Appendix 2

AWS Enterprise Support Additional Terms and Conditions

THE FOLLOWING AWS ENTERPRISE SUPPORT TERMS AND CONDITIONS SHALL APPLY TO EACH CALL-OFF CONTRACT ISSUED UNDER THE FRAMEWORK AGREEMENT WHERE THE BUYER HAS SUBSCRIBED TO ENTERPRISE – LEVEL AWS SUPPORT.

AWS ENTERPRISE SUPPORT ADDITIONAL SUPPLIER TERMS

The following is included as additional Supplier Terms where Buyer has executed a Call-Off Contract to procure Enterprise-level AWS Support, including where Enterprise Support is included in the offering (e.g. AWS Managed Services). Enterprise-level AWS Support provides Buyer with one-on-one technical support services to help Buyers business utilize the products and features provided by Amazon Web Services.

To subscribe for Enterprise-level AWS Support following execution of the Call-Off Contract, Supplier requires the AWS account numbers that Buyer intends to enroll to enable this service. Buyer will notify the account ID(s) to Supplier at aws-ukps-frameworks@amazon.com.

AWS ACCOUNTS

These additional terms and conditions will cover the account(s) notified to Supplier at aws-ukps-frameworks@amazon.com and other all accounts linked to the account(s) listed above via consolidated billing, provided that all such linked accounts are opened by Buyer or Buyers employees using email addresses issued by Buyer, for use by Buyer or Buyers employees:

1. Accounts may be added to or removed by mutual agreement of the parties (which agreement may be made via email.)

2. For those accounts notified to Supplier, Supplier will provide AWS Support at the Enterprise subscription level to Buyer in accordance with the terms and Enterprise-level pricing located on the site and the AWS Support Service Terms at http://aws.amazon.com/serviceterms/ .

3. Buyer will be billed for AWS Support on a monthly basis and payments for AWS Support are non-refundable. If Buyer cancels their subscription within 30 days of sign-up Buyer will see a minimum subscription charge on their next bill.

[Remainder of Page Intentionally Left Blank]