

P3MO G-Cloud 15 Lot 2B Supplier Terms

Version: 1.0

Supplier: P3MO Ltd

Framework: UK Government G-Cloud 15 (Lot 2b)

Overview

The Supplier Terms applicable to this Call-Off Contract comprise three key sections:

- Acceptable Use Policy (AUP)
 - Service Level Agreement (SLA)
 - Supplier Licence Terms
-

Acceptable Use Policy (AUP)

Status: For UK Government Customers – G-Cloud 15 Compliant

Version: 1.0

Applies to: All authorised users of the P3MO SaaS Platform

Scope: All access and use of the Service by Customer staff, contractors, partners, and any third parties granted access by the Customer.

1. Purpose

This Acceptable Use Policy sets out the rules governing access to and use of the P3MO SaaS platform ("the Service") by UK Government customers purchasing through G-Cloud 15. The intent is to:

- Protect the security and integrity of the Service
- Ensure compliance with the G-Cloud 15 Framework, UK law, and applicable government security standards
- Prevent misuse that may impact availability, confidentiality, or service quality

Use of the Service constitutes acceptance of this policy.

2. General Principles

Users must:

- Use the Service only for legitimate business purposes associated with the Customer organisation
- Comply with all UK laws, including the Computer Misuse Act 1990, UK GDPR, DPA 2018, and applicable information security policies
- Access the Service only with authorised credentials assigned to them

- Use the Service in accordance with the Customer's internal security policies (for example, local Acceptable Use Policy, behaviour policy)

3. Security Requirements

3.1 Authentication and Access Control

Users must:

- Keep their login credentials confidential
- Use Multi-Factor Authentication (MFA) if enabled
- Use only their assigned accounts (no shared accounts)
- Immediately report lost or compromised credentials

3.2 Data Classification and Handling

Users must:

- Only store data classified as OFFICIAL or lower (unless specifically agreed in writing)
- Ensure personal data is handled in accordance with UK GDPR
- Not upload sensitive or prohibited data (for example, special category data) unless contractually allowed

3.3 Device and Network Requirements

Users must:

- Access the Service from devices compliant with Customer IT security standards
- Not circumvent built-in security controls (for example, browser restrictions, session timeouts)

4. Prohibited Activities

The following activities are strictly prohibited.

4.1 Security Violations

- Attempting to gain unauthorised access to systems, accounts, or data
- Penetration testing or vulnerability scanning without prior written approval
- Introducing malware, scripts, or code designed to disrupt or degrade the platform
- Attempting to bypass security controls, rate limits, or monitoring

4.2 Misuse of the Service

Users must not use the Service to store, process, or transmit:

- Illegal content
- Offensive, extremist, or discriminatory material
- Content breaching intellectual property rights

Additional prohibitions include:

- Using the Service for non-business or personal commercial activity
- Overloading system resources (for example, excessive API calls, automated scraping)

4.3 Data Misuse

- Exporting or copying data without authorisation
- Using personal data for purposes not permitted under the Customer's lawful basis
- Sharing data with unauthorised individuals or third parties

5. Government-Specific Restrictions (G-Cloud 15)

In line with G-Cloud 15 and CCS requirements, users must not:

- Use the Service in a way that breaches the Call-Off Contract terms, Crown copyright, or CCS framework rules
- Introduce data with a classification level higher than permitted
- Enable overseas access to personal data unless explicitly approved within the contract or Data Processing Agreement
- Use the Service in a way that may compromise UK Government information assurance standards (for example, NCSC Cloud Security Principles)

6. Customer Responsibilities

The Customer organisation must:

- Maintain accurate and controlled user access lists
- Remove user access promptly upon role change or exit
- Provide users with appropriate security awareness training
- Ensure their internal policies align with this Acceptable Use Policy
- Report potential breaches to the Provider immediately

7. Monitoring and Logging

P3MO Ltd may:

- Monitor usage to ensure performance, security, and compliance
- Log user actions for audit, security, and forensic purposes
- Suspend or restrict access where there is suspected breach or misuse

All monitoring will comply with UK GDPR and contractual terms.

8. Incident Reporting

Users must immediately report any of the following:

- Suspected security breach
- Unauthorised access
- Data loss or corruption
- System misuse

Reports must be made to the Customer's Information Security Officer and to P3MO Support via the agreed channels.

9. Violations and Enforcement

In the event of a breach of this Acceptable Use Policy, P3MO Ltd may:

- Suspend or terminate user access
- Notify the Customer's security or compliance lead
- Implement service restrictions or protective measures
- Support the Customer's internal investigation
- Take action required by law or regulatory bodies (for example, ICO)

Repeated or serious violations may result in service suspension per the Call-Off Contract.

10. Changes to this Policy

P3MO Ltd may update this Acceptable Use Policy where:

- G-Cloud framework terms change
- Applicable UK law or regulation changes
- Security best practice evolves

The Customer will be notified of material changes with reasonable advance notice.

Service Level Agreement (SLA)

This Service Level Agreement ("SLA") is a policy governing the use of the P3MO Platform ("Service") by customers of P3MO Ltd ("Provider").

1. Service Commitment

P3MO Ltd will use commercially reasonable efforts to make the Service available 99.9% of the time in any given calendar month, excluding scheduled maintenance and circumstances beyond our reasonable control (as defined in Section 5 of this SLA).

2. Service Availability

2.1 Uptime Commitment

The Service will be available 99.9% of the time during each monthly billing cycle, measured on a 24/7 basis.

2.2 Scheduled Maintenance

We may schedule maintenance with prior notice of at least 48 hours. Scheduled maintenance windows will not exceed 4 hours per month and will typically occur during low-usage hours.

2.3 Emergency Maintenance

In cases of emergency maintenance, we will provide as much notice as is practicable and work to restore the service as quickly as possible.

3. Support Services

3.1 Support Hours

Support is available 09:00 to 17:00 GMT, Monday to Friday, excluding public holidays.

3.2 Contact Methods

Support can be reached via email at: support@p3mo.io

3.3 Response Times

Response times are defined in the Call-Off Contract Service Definition Document.

4. Service Credits

If uptime falls below the stated commitment, you may be eligible for a Service Credit.

Key Definitions

Term	Definition
Maximum Available Minutes	The total accumulated minutes during a month period, excluding limitations (as defined in Section 5 of this SLA)
Downtime	The total accumulated minutes that are part of Maximum Available Minutes during which there is no Connectivity
Uptime Percentage	Calculated using the formula: (Maximum Available Minutes – Downtime) ÷ Maximum Available Minutes × 100

Table 1: Service Credit Key Definitions

4.1 Requesting a Credit

You must request a credit by submitting a claim within 30 days of the suspected SLA violation. Your claim must include:

- Downtime details with timestamps
- Description of the issue
- Steps taken to notify P3MO

4.2 Limitations

Service Credits are the sole and exclusive remedy for any SLA violation.

5. Exclusions

This SLA does not apply to downtime or performance issues:

- Caused by factors outside of our reasonable control (for example, natural disasters, war, acts of terrorism, riots, government action, internet outages, or device failure)
- Resulting from your software or hardware, or related to third-party software or services not provided by P3MO

- Due to your misuse or breach of the Terms of Service
- For licences not paid for at the time of the incident
- Related to beta or trial services

6. Amendments and Termination

We reserve the right to amend this SLA at any time, with 30 days' written notice. Continued use of the Service following changes constitutes acceptance.

7. Entire Agreement

This SLA is part of your agreement with P3MO Ltd.

Supplier Licence Terms

1. Definitions

- **Supplier** means P3MO Ltd
- **Customer** means the UK public sector organisation entering the G-Cloud 15 Call-Off Contract
- **Users** means individuals authorised by the Customer to access the Service
- **Service** means the cloud software delivered via a SaaS model under G-Cloud 15 Lot 2b
- **Customer Data** means all data uploaded, generated, or processed by the Customer
- **Documentation** means online or written materials describing use of the Service

2. Grant of Licence

The Supplier grants the Customer a non-exclusive, non-transferable, revocable licence to:

- Access and use the Service for its internal business purposes
- Permit Users to access the Service in accordance with the Call-Off Contract
- Use Supplier-provided Documentation to support permitted use

This licence is granted solely for the duration of the Customer's G-Cloud 15 Call-Off Contract and is subject to the terms set out below. No rights are granted beyond those expressly provided.

3. Permitted Use

The Customer may:

- Use the Service to store, process, and manage data classified up to OFFICIAL
- Configure the Service within the limits of permitted customer-side configuration
- Export Customer Data using agreed export mechanisms
- Use training, support, and knowledge materials provided by the Supplier
- Allow employees, contractors, and authorised partners to access the Service for legitimate business purposes

4. Prohibited Use

The Customer must not:

- Attempt to reverse-engineer, decompile, or access the Service's underlying code
- Use the Service for unlawful, harmful, or discriminatory activities
- Upload malicious code or attempt to disrupt platform operations
- Circumvent user authentication, access controls, or security protections
- Use the Service to store material classified above OFFICIAL, unless agreed in writing
- Provide access to any person or entity not authorised under the Call-Off Contract
- Resell, lease, sublicense, or make the Service available to any third party except as permitted by CCS terms
- Conduct penetration testing without prior written approval

5. Intellectual Property Rights

- All intellectual property rights in the Service, platform architecture, code, documentation, and associated materials are owned by the Supplier
- No ownership rights transfer to the Customer
- The Customer retains full ownership of Customer Data at all times
- The Supplier may reuse anonymised, aggregated analytics for service improvement, provided such data cannot identify the Customer or individuals

6. User Accounts and Access Management

The Customer is responsible for:

- Managing and administering all User accounts
- Ensuring role-based access controls are applied appropriately

- Removing access for Users who change role or leave the organisation
- Ensuring Users comply with the Supplier's Acceptable Use Policy (AUP)

The Supplier may suspend access if there is reasonable evidence of misuse or risk to the Service.

7. Service Availability

Availability commitments are defined in the Service Level Agreement (SLA) provided with the Service Definition Document and incorporated into the Call-Off Contract.

Service credits may apply where availability falls below contracted levels.

8. Data Protection and Privacy

Both parties shall comply with:

- UK GDPR
- Data Protection Act 2018
- The Call-Off Contract Data Protection Schedule
- The Data Processing Agreement (DPA)

8.1 Supplier Responsibilities

The Supplier shall:

- Process Customer Data only for the purpose of providing the Service
- Implement appropriate technical and organisational security measures
- Maintain UK-based or approved data residency as stated in the Service Definition
- Ensure sub-processors meet equivalent security and contractual requirements
- Notify the Customer of any data breach without undue delay

8.2 Customer Responsibilities

The Customer shall:

- Ensure Customer Data provided to the Supplier is lawful and accurate
- Configure access controls correctly
- Notify Supplier of any data subject requests involving Supplier processing
- Secure endpoints used to access the Service

9. Customer Obligations

The Customer shall:

- Use the Service in accordance with these Licence Terms
- Comply with applicable laws and government policies (for example, NCSC guidance and local IT security policies)
- Prevent unauthorised or unlawful use
- Ensure adequate network and device security
- Not introduce harmful or disruptive technologies into the Service
- Maintain accurate contact and billing details where applicable

10. Supplier Obligations

The Supplier shall:

- Provide access to the Service in line with G-Cloud 15 requirements
- Maintain and update the platform as required for security and stability
- Provide support through agreed channels and hours
- Ensure the platform remains compliant with relevant security certifications (for example, ISO 27001, Cyber Essentials Plus)

11. Term, Suspension, and Termination

These Licence Terms apply for the duration of the G-Cloud Call-Off Contract.

The Supplier may suspend access where there is:

- A serious security risk
- Suspected misuse
- Breach of legal or contractual obligations

Upon termination:

- Customer access ceases
- Customer Data will be made available for export for the period specified in the Service Definition
- The Supplier will securely delete Customer Data in accordance with the DPA

12. Warranties

The Supplier warrants that:

- The Service will operate materially in accordance with the Documentation

- It will deliver the Service with reasonable skill and care
- It has taken reasonable steps to ensure the Service is free from harmful code

The Supplier does not warrant that:

- The Service will be error-free or uninterrupted
- The Service will meet all Customer-specific requirements not expressly agreed

13. Liability

Liability is governed by the G-Cloud 15 Call-Off Contract Terms, including:

- Caps on liability
- Exclusions of indirect or consequential loss
- Carve-outs for data protection, fraud, and wilful misconduct

These terms override any conflicting Supplier liability statements.

14. Audit and Assurance

The Customer may request:

- Security documentation
- Certification evidence
- Penetration testing summaries
- Audit responses as permitted under the Call-Off Contract

The Customer may conduct audits in accordance with CCS rules provided reasonable notice is given.

15. Changes to the Licence Terms

The Supplier may update these terms where:

- Required by law
- Required by G-Cloud framework changes
- Required for security improvements

Material changes will be communicated to the Customer with reasonable advance notice.

16. Governing Law

These Licence Terms are governed by:

- The laws of England and Wales
 - The mandatory terms of the G-Cloud 15 Call-Off Contract
-

Document Information

Document Version: 1.0

Last Updated: 9 December 2025

Language: English (UK)

Classification: For UK Government Customers – G-Cloud 15 Compliant

This document has been formatted for WCAG 2.2 AA accessibility compliance with proper heading hierarchy, semantic list structures, structured tables, and clear navigation aids.