



Cyberfort



The Bunker
PART OF THE CYBERFORT GROUP

G-Cloud 15

Standard Terms & Conditions
Cloud Hosting Managed Services



1. Standard Terms & Conditions

The below Standard Terms and Conditions are applicable to the supply of the G-Cloud Framework and would form the Services to be supplied under the Call-Off Contract with the Customer/Buyer.

If you ultimately decide to purchase the Service(s) described with Cyberfort, then all terms and conditions will only be pursuant to a final and definitive written agreement between the Customer/Buyer and Cyberfort (including any amendments, if applicable).

For the avoidance of doubt, the final agreement will replace any other suggested terms and conditions.

Notwithstanding anything to the contrary, Cyberfort makes no representations, warranties, or covenants (including without limitation as to any products, services, service levels, third-party products or services or interoperability) separate from, in contravention of, or in addition to those contained in the final agreement, and any purported representation, warranty or covenant in this information document shall be of no force or effect.

Any information provided in below regarding the Service is for informational purposes only and is subject to change.

2. Managed Services

1. Additional definitions

The following capitalised terms shall have the following meanings:

Bandwidth	means the telecommunications bandwidth capacity provided to the Customer as part of the Services;
Building	means the Cyberfort premises where the Services will be provided as specified in the Order Form or SOW;
Commencement Date	means the earlier of (i) the date on which user acceptance testing as set out in the Schedule to the Order Form is completed and (ii) the date on which the Customer first uses the Services
Customer Equipment	means the equipment either belonging to the Customer or to a Customer Representative, which is installed in the Building;
Customer Representative	means an employee, director or agent of the Customer or any other third party for whom the Customer is responsible or deemed responsible pursuant to this MRA;
Customer Space	means the Equipment Room, Equipment Cage, Racking or Equipment Cabinet (as applicable);
Cyberfort Access Policy	means the Cyberfort Access Policy set out in Annex 1;
Equipment Cabinet	means an equipment cabinet used by Customers for the installation and operation of the Customer Equipment;
Equipment Cage	means a caged area used by the Customer for the installation and operation of the Customer Equipment;
Equipment Room	a room used by the Customer for the installation and operation of Customer Equipment;
Racking	means racking used by Customers for the installation and operation of Customer Equipment;
Service Credits	has the meaning given to it in the Service Level Agreement set out in Appendix 2;
Technical Infrastructure	any equipment hardware, software and/or cabling (other than the Customer Equipment), in or outside the Equipment Room(s), the Equipment Cage(s), Equipment Cabinet(s) and/or Racking.

2. Provision of Service



- 2.1 Cyberfort shall provide the Services, including the Bandwidth and the Customer Space, as described in the applicable Order Form or SOW in accordance with the MRA. The Service Levels set out in Appendix 2 shall apply to Cyberfort's provision of the Services under the MRA.
- 2.2 The Services will commence when the parties sign the Order Form and/or SOW and will remain in effect until terminated by either party giving the other three (3) months' notice in writing, to expire on or after the third anniversary of the Commencement Date, or otherwise in accordance with the terms of the MRA.

3. Use of Customer Space

- 3.1 Subject to the provisions of this paragraph 3, Cyberfort permits the Customer to install, locate and operate the Customer Equipment within the Customer Space in relation to the purchased Services and for no other purpose.
- 3.2 The MRA does not create any right of occupation or tenancy in relation to the Building and the Customer's occupation is by way of personal license only.
- 3.3 Cyberfort shall retain control of the Customer Space. The Customer shall have no right of exclusive possession, shall have no right at any time to prohibit entry to the Customer Space by Cyberfort. The Customer shall have no legal interest in the Customer Space, which shall remain vested in Cyberfort at all times.
- 3.4 Upon written notification to the Customer and where reasonably practicable in consultation with the Customer, Cyberfort shall have the right at any time for the duration of the MRA to relocate, at its cost, the Customer Equipment to another location within the Building. Any such relocation shall be carried out by Cyberfort as swiftly as reasonably practicable causing the minimum interference reasonably possible to the functioning of the Customer Equipment.
- 3.5 The Customer will have sole responsibility for the accuracy and completeness of Customer Material and Data and shall ensure that Customer Material and Data do not contain anything which is defamatory, offensive or abusive or of an obscene or menacing character, or which constitutes a violation or infringement of the rights (including without limitation Intellectual Property Rights) of any person or which is illegal or which constitutes a breach of any relevant regulations or codes of practice.

4. Maintenance of the Technical Infrastructure

- 4.1 Cyberfort may from time to time carry out preventative maintenance on the Technical Infrastructure.
- 4.2 Subject to paragraph 4.3, Cyberfort shall not carry out maintenance or other work to the Technical Infrastructure which may cause any interruption to the Services unless it has given at least seven days prior written notice to the Customer that it intends to do so.
- 4.3 If in Cyberfort's reasonable opinion an emergency situation exists whether due to applicable safety, security, statutory requirements or otherwise, Cyberfort may carry out essential maintenance activities to the Technical Infrastructure or make changes to the Services (which do not materially affect the provision of the Services) without giving notice pursuant to this paragraph 4 and Cyberfort will notify the Customer as soon as reasonably practicable thereafter.
- 4.4 Cyberfort conducts scheduled maintenance to improve the monitoring, security and stability of Cyberfort cloud services. When maintenance is executed within the scheduled maintenance window brief outages may occur. The scheduled maintenance windows for Cyberfort cloud services are confined to Tuesdays and Fridays, 18:00PM to 20:00PM GMT.
- 4.5 Cyberfort shall have no liability to the Customer for interruptions to the Services due to changes to the Service or maintenance activities carried out or pursuant to Appendix 2.



5. Customer Equipment

- 5.1 Installation of all Customer Equipment in the Customer Space shall be at the cost and risk of the Customer.
- 5.2 Prior to any installation of Customer Equipment within the Customer Space the Customer shall first produce to Cyberfort for approval in its absolute discretion:
 - (a) details and specifications of such Customer Equipment
 - (b) plans and specifications showing the proposed layout of the Customer Equipment;
 - (c) all as more particularly described in the Order Form and/or SOW together with such other information as Cyberfort shall reasonably require from time to time.
- 5.3 No such installation shall take place without Cyberfort's approval. Cyberfort shall be permitted to charge the Customer a reasonable administration fee for the provision of its approval under this paragraph.
- 5.4 The Customer shall notify Cyberfort if it intends to make any further changes to the Customer Equipment within the Customer Space and shall provide Cyberfort with updates to the documents and information.
- 5.5 The Customer shall not without the prior written consent of Cyberfort make any modification, alteration or addition to the Customer Equipment within the Customer Space which results in material changes to the floor loading, heat output, power consumption and environmental conditions. Cyberfort may as a condition of giving any such consent require changes in the floor, air conditioning and power supply and/or the Services.
- 5.6 The Customer shall not permit any person other than Cyberfort to make any connection or disconnection of the Customer Equipment to the power supply within the Building.
- 5.7 The Customer shall ensure that all Customer Equipment brought into the Building by the Customer is certified for the intended purposes and complies with relevant national and international standards and is constructed in such a way that failure and/or damage will not harm other equipment or the operation of that equipment or endanger any personnel. The Customer is responsible for maintaining the equipment in line with these standards.
- 5.8 If any interference occurs between the Customer Equipment and the equipment of any third party within the Building, Cyberfort shall deal with such interference in its absolute discretion and the Customer shall comply with all instructions given by Cyberfort (including but without prejudice to the foregoing provisions instructions to disconnect part or parts of the Customer Equipment). In the case of an emergency, Cyberfort may, without incurring any liability to the Customer or to Customer Representatives, disconnect part or parts of the Customer Equipment itself.
- 5.9 The MRA shall not create or vest any rights in Cyberfort with respect to Customer Equipment and Cyberfort is not entitled to use such Customer Equipment for its own purposes.

6. Customer Access

- 6.1 Cyberfort shall allow the Customer and authorised Customer Representatives (as applicable) access to the Building at any time in accordance with the Cyberfort Access Policy, provided that Cyberfort may refuse entry to all or part of the Building by any person if (in its absolute discretion) Cyberfort believes it necessary or prudent, either for security purposes, for other purposes connected with the management and running of the Building, or if the Customer is in breach of the MRA.

7. Insurance

- 7.1 The Customer undertakes to Cyberfort that it has and shall maintain public and third party liability insurance providing cover of at least five (5) million pounds sterling per event or series of events, and shall as soon as reasonably practicable following the Cyberfort's request provide proof that the insurance policies are current and validly maintained.
- 7.2 The Customer shall be solely responsible for insuring the Customer Equipment or procuring that it is insured against any and all risks, including losses that may occur to it, its business or its clients as a result of any failure of the Services.

8. Service Charges

- 8.1 Charges for the Services will start on the Commencement Date.

9. Additional Services and Charges

- 9.1 Should the Customer request additional time, over and above the agreed Support Level or System Setup and Standard Integration, the Customer will be charged at the following Standard Hourly Rates*, invoiced in 15-minute increments.

Service Type	Business Hours 09.00 – 17.00	Scheduled out of business hours 17.00 – 09.00 & Weekends	Unscheduled, Emergency and Public & Bank Holidays
Remote Hands	£100 P/h	£200 P/h	£300 P/h
Specialist Technical	£150 P/h	£300 P/h	£450 P/h
Project Management	£100 P/h	£200 P/h	£300 P/h
Administration Fee	£100 P/h	£200 P/h	£300 P/h

*Standard Hourly rates are subject to annual review in accordance with the MRA. These rates are current on the Commencement Date of the MRA.

- The Standard Hourly Rate shall apply during business working hours of 09.00 to 17.00.
- Scheduled out of business working hours will be charged at the overtime rate at TWO times the Standard Hourly Rate.
- Public and Bank Holidays as well as unscheduled out of business working hours will be charged at the overtime rate at THREE times the Standard Hourly Rate.

10. Customer Visits

For security purposes, in a high-security environment, a security officer must accompany all customers needing access to their equipment, while on site.

All visits must be booked in advance, thereby allowing time to allocate a security escort. The following notice is required:

For visits during Business Hours a notice period of 24 hours is required For visits out of Business Hours a notice period of 48 hours is required

Should an emergency event occur that requires a customer to have access to their equipment



outside of Business hours we will make every effort to accommodate them, subject to operational limitations and assessed on a case-by-case basis.

Service Type	Business Hours 09.00 – 17.00	Scheduled out of business hours 17.00 – 09.00 & Weekends	Unscheduled, Emergency and Public & Bank Holidays
Security Escort	£15 P/h	£15 P/h	£50 P/h

Please note these charges are subject to change as per the MRA and are current at the Commencement Date of the MRA.

11. Effect of Termination

- 11.1 Forthwith upon termination of this agreement:
 - 11.1.1 Cyberfort may cease to provide the Services;
 - 11.1.2 all outstanding sums shall be paid to Cyberfort by the Customer and any sums paid in advance to Cyberfort shall be non-refundable;
 - 11.1.3 Cyberfort shall permit the Customer access to the Customer Space and the Customer shall promptly remove at its own risk and cost the entire Customer Equipment belonging to the Customer or any applicable third parties. The Customer shall continue to pay all applicable Service Charges until the date upon which Cyberfort is satisfied that all Customer Equipment is removed;
 - 11.1.4 the Customer shall restore or pay to Cyberfort on demand the cost of restoring the Customer Space used by the Customer to the same condition in which it existed at the Commencement Date and to the reasonable satisfaction of Cyberfort.
- 11.2 If the Customer fails to comply with its obligations in paragraph 11.1.3 within 1 month of the termination date, Cyberfort shall be entitled in its sole discretion at the Customer's expense to remove the Customer Equipment from the Customer Space and deliver the same to the Customer at the address given in the MRA or place the Customer Equipment in storage and restore the Customer Space to the satisfaction of Cyberfort. Cyberfort shall be entitled in its sole discretion to engage the services of third party contractors to carry out the activities described in this paragraph 11.2.
- 11.3 The Customer shall indemnify Cyberfort and keep Cyberfort indemnified against all costs, actions, claims, damages, proceedings and expenses incurred by Cyberfort in connection with the activities described in this paragraph 11 and such sums shall be reimbursed to Cyberfort by the Customer on demand.
- 11.4 Notwithstanding termination, the Customer shall continue to be liable to pay a sum equivalent to the monthly Services Charges otherwise payable under this SOW/Order Form and the MRA in respect of any Customer Equipment which has not been removed from the Building, such sum to be calculated on a daily rate from the date of termination up to the date when the Customer Equipment is removed.
- 11.5 Cyberfort reserves the right to exercise a lien over the Customer Equipment in respect of any unpaid Service Charges beyond the termination date and shall be entitled to sell the Customer Equipment if it remains in the Building after the expiry of one (1) month from the termination date in order to recoup any unpaid Service Charges.



Annex 1

CYBERFORT ACCESS POLICY

1. Notwithstanding any provision of the MRA, Cyberfort may refuse entry to all or part of the Building by any person if (in its absolute discretion) Cyberfort believes it necessary or prudent, either for security purposes or for other purposes connected with the management and running of the Building
2. Subject to paragraph 1, an authorised Customer (or where relevant, an authorised Customer representative) will be entitled to enter the Building for the purpose of inspecting the Customer Equipment and to carry out all necessary maintenance and repair to the Customer Equipment if it complies with the following:
 - (a) it gives Cyberfort at least 24 hours prior notice for access during Business Hours and 48 hours' notice for access out of Business Hours (as defined in the Order Form), provided, however if the Customer requires immediate access to the Building, Cyberfort shall use its reasonable endeavours to accommodate the request, subject to operational limitations and assessed on a case-by-case basis; and
 - (b) specifies the identity of the personnel who wish to enter the Building and the purpose of their visit.
3. Any person seeking to enter the Building will not be permitted entry unless, on arrival, that person provides proof of his or her identity and submits such other documents as set out from time to time, including, in respect of any Customer representatives, written authority of the Customer permitting that Customer representative access to the Customer Space.
4. Any persons entering the Building on behalf of the Customer or the Customer Representative will at all times be accompanied by a representative of Cyberfort or a security guard, at the Customer's cost.
5. Cyberfort reserves the right to extract Customer Equipment from the Customer Space to allow the Customer or any Customer Representative access to such Customer Equipment where entry to such Customer Space is prevented, or reasonably withheld by Cyberfort for any reason.
6. The Customer shall ensure that its Customer representatives:
 - (a) follow Cyberfort's instructions with respect to access to the Building including but not limited to the instructions described in the Cyberfort Access Policy and all health and safety regulations;
 - (b) do not cause any change to or interfere with the Customer Space, the Building or the equipment of any other third party customers of Cyberfort; and
 - (c) do nothing to cause the Customer Space and the Building to be in anything other than a clean and tidy condition.
7. The Customer may not bring any goods, furniture or equipment into the Building without the prior written consent of Cyberfort (such consent to be in the absolute discretion of Cyberfort). If such consent is given, the Customer shall give 24 hours prior written notice (unless Cyberfort directs otherwise) of its intention to deliver such goods, furniture or equipment to the Building. All deliveries shall take place between the hours of 09H00 and 17H00 UK time and in accordance with Cyberfort's instructions and this Cyberfort Access Policy.
8. The Customer shall not operate any equipment that may constitute a safety hazard. Any activity causing dust particles is prohibited. Dust particles may trigger the fire alarm.
9. Camera equipment, including mobile telephones with cameras are not allowed into the Building.
10. All irregularities and alarms must be reported to the Service Desk.

Appendix 2 – Service Level Agreement

1. Definitions:

For the purposes of this Service Level Agreement the following additional definitions shall apply:

Agreement	means this Service Level Agreement
Availability	in relation to the Core Services is defined as: $\frac{\text{Service Cover Time} - \text{Total Unavailability}}{\text{Service Cover Time}} \times 100 \quad [\%]$ where:
Core Services	means the core hosting services described in the Order Form or SOW
Emergency Maintenance	means Cyberfort needs to provide immediate maintenance to equipment in the Building that may result in an outage on Customer hardware
End Time	has the meaning given to it in paragraph 7.2.
Planned Maintenance	means where Cyberfort needs to provide maintenance to equipment in the Building that may result in an outage on Customer Equipment and Cyberfort shall, where practicable, use its reasonable endeavours to provide a minimum of seven days' notice for such maintenance.
Measurement Period	shall mean a period of one calendar month, save that the first such period after the commencement of the Services (First Measurement Period) shall run until the end of the first full calendar month after commencement of the Services.
Scheduled Maintenance	shall mean where Cyberfort needs to provide maintenance to equipment in the Building that may result in an outage on Customer Equipment on a regular basis. In the case of Scheduled Maintenance, Cyberfort shall, where reasonably practicable, provide notice for such maintenance.
Service Cover Time	shall mean the total number of minutes comprised in the relevant Measurement Period (or First Measurement Period)
Service Levels	shall have the meaning given to them in paragraph 3 of this Agreement.
Standard Operating Procedure (SOP)	shall mean the documented set of instructions detailing standardised processes and procedures used to perform routine activities.
Start Time	has the meaning given in paragraph 7.1.
Total Unavailability	is defined as the total time in minutes between the Start Time and the End Time (rounded up to the nearest whole minute) in the relevant Measurement Period (or First Measurement Period) during which the Core Services were inoperable or unusable as determined in

accordance with the unavailability computation calculated pursuant to paragraph 7 of this Agreement.

2. Subject to any express provisions of the Agreement, Cyberfort shall maintain the Service Levels for each of the Core Services as set out in paragraph 3 of this Agreement. If, in any one event, more than one of the Core Services fails, the Unavailability Computation will be based on only the longest duration of any of these Core Services in that said event.

3. **Core Services and Service Levels shall mean:**

Core Service	Measurement Period	First Measurement Period
Power	A service level of 100% for power to the data centre	A service level of 100% for power to the data centre
Connectivity	A service level of 99.5% for connectivity to the network port on the data centre	A service level of 95% for connectivity to the network port on the data centre
Climate	An average temperature of between 23°C and 27°C across the data centre	An average temperature of between 23°C and 27°C across the data centre
Fire Detection	A service level of 100% to the data centre floors	A service level of 100% to the data centre floors
Security	Security systems will operate on a 24/7/365 basis and will operate to 100% capability	Security systems will operate on a 24/7/365 basis and will operate to 100% capability

4. **Exclusions from Service Levels**

- 4.1 The parties agree that, notwithstanding any other provision in this Agreement, Cyberfort will not be responsible for failure to provide the Core Services or failure to meet the Service Levels to the extent that the failure is due to:
- (a) Force Majeure;
 - (b) for any failure, incorrectly configured or operated hardware or software in relation to the Customer Equipment, overload of system capacities, servers, networks, telecommunication lines and connections and other electronic and mechanical equipment or any other default in respect thereof (except to the extent that such default is directly caused by Cyberfort's breach of the Contract);
 - (c) any failure by the Customer to comply with any of its duties or obligations set out in this Agreement or the MRA;
 - (d) any act or omission of any of the Customer's contractors, agents and suppliers (other than Cyberfort);
 - (e) Scheduled Maintenance, Planned Maintenance or Emergency Maintenance which makes any of the Core Services inoperable, unusable or cause any outages;
 - (f) equipment, connectivity, interruption of power supplies or other utility of service (whether partial or total) and environmental conditions on the Customer's site;
 - (g) unauthorised changes by the Customer;
 - (h) the Services fall outside of the Term of the MRA or the applicable SOW/Order Form.

- (i) governmental or regulatory restrictions; exchange rulings, court or tribunal orders or other human intervention;
- (j) any other circumstances or matters other than matters for which Cyberfort is directly responsible pursuant to this Agreement.
- (k) In the event of an exclusion as set out in paragraph 4.1, the parties acknowledge and agree that the outages caused by these events will not be included in the Unavailability Computation and the Service Credits will not apply, nor will the Customer be entitled to bring any claims for damages, losses, costs and/or expenses incurred or suffered which arise from any failure to provide the Service.

5. Response and Target Times

In the event a failure concerning one of the Core Services is detected by Cyberfort or reported by the Customer, Cyberfort shall use reasonable endeavours to rectify the affected Core Service within the following Target Times:

Fault	Response Times	Target Times to Resolve
Failure of Core Service	PROMPT response from time of event notification and assignment of Trouble Ticket number.	Within 1 hour of Cyberfort's response.

6. Fault Escalation Path

If the Fault cannot be resolved within the Target Time specified above, the fault escalation path for the Customer shall be as follows:

ACTION	Position	Escalation Time for Fault	Telephone	Fax / E-mail
Initial Notification	Alarm raised - NOC notified of fault – On site Technician	Trouble Ticket raised	Documented in SOP	Documented in SOP
Level 1 escalation	On call Senior Technician notified	Promptly	Documented in SOP	Documented in SOP
Level 2 escalation	On call Senior Manager notified	Escalated if Fault not resolved within 60 minutes of Level 1 escalation	Documented in SOP	Documented in SOP

7. Unavailability Computation

7.1 A Core Service will be deemed unavailable from either:

- a) the time that the Customer reports the Core Service is below the Service Level; or
- b) the time that Cyberfort discovers that the Core Service is below the Service Level (the “**Start Time**” as applicable).

7.2 A Core Service will be deemed available again from when the Core Service is either

- a) above the Service Level, based on the reasonable opinion of Cyberfort; or
- b) where the End Time falls into another Measurement Period the End Time will

be deemed to be the last day within the same Measurement Period as the Start Time. (the “**End Time**” as applicable)

8. Service Credits

- 8.1 Cyberfort shall pay to the Customer Service Credits in accordance with this Agreement where the achieved performance levels of certain Services fail to meet certain of the respective Service Levels.
- 8.2 The parties agree that:
 - 8.2.1 Service Credits are a reasonable and genuine pre-estimate of the loss to the Customer for failure to meet the relevant Service Levels for which Service Credits are specified and will be considered by the parties to constitute liquidated damages; and
 - 8.2.2 where Service Credits are provided for as a remedy for failure to meet a particular Service Level, the payment of Service Credits by Cyberfort to the Customer will constitute the sole and exclusive remedy of the Customer for the failure of Cyberfort to provide the Services.
- 8.3 In any event, Cyberfort's maximum liability for Service Credits under the Agreement shall be 100% of the Charges payable in respect of the Services for the relevant Measurement Period in which Service Credits are calculated and applied.
- 8.4 No Service Credits shall be carried forward from one calendar month to another in circumstances where the amount of Service Credits would but for the provisions of paragraph 8.3 exceed 100% of the Charges payable in respect of the Services for such period and/or in any other circumstances.
- 8.5 Subject to paragraphs 8.3 and 8.4 of this Agreement, the Service Credits shall be calculated as follows: For each FULL percentage point (1%) by which the Availability in a Measurement Period is reduced below the target Availability (or First Measurement Period Availability where applicable), a Service Credit shall be due to the Customer equal to 5% of the Fees payable by the Customer in respect of the Services for such Measurement Period.
- 8.6 If the Customer is entitled to any Service Credits, the Customer must write to Cyberfort within seven days after the end of any Measurement Period to claim the Service Credits in respect of such Measurement Period.
- 8.7 Service Credits will not be given where the Customer is in arrears of payment to Cyberfort.
- 8.8 Service Credits can only be claimed by the Customer for any Core Service failure to their specific racking.
- 8.9 The Customer is not entitled to claim any Service Credits on behalf of any of its clients for any consequential interruption or failure of any third-party services provided by the Customer.

9. Breaches to Service Level

- 9.1 The following list of circumstances will constitute a material breach and the Customer may, without prejudice to its other rights under the MRA, have the right to terminate the MRA immediately in whole or in part by giving Cyberfort notice in writing:
 - 9.1.1 if the Availability falls below 70% in the First Measurement Period after the Commencement Date; or
 - 9.1.2 if the Availability falls below 80% during any Measurement Period after the Commencement Date; or
 - 9.1.3 if the Availability falls below an average of 90% in any three consecutive Measurement Periods.



10. Third Party Service Level Agreements

- 10.1 The Parties acknowledge that if Cyberfort contracts with third-party suppliers for the purposes of providing non-standard services, Cyberfort shall be subject to such third-party's service level agreement. Accordingly, Cyberfort shall only be liable to the Customer for response times and service credits pursuant to this appendix to the extent that the third-party supplier is liable to Cyberfort for response times and service credits for the relevant parts of the service.