MANAGED SERVICES
SCHEDULE 2: SERVICE LEVEL AGREEMENT

CONTENTS

ARTICLE 1 - SERVICE ELEMENTS

1 General

1.1. Unless otherwise stated, the defined terms in this Service Level Agreement shall have the same meaning as set out elsewhere in the Agreement. References in this Service Level Agreement to the Primary Location and Secondary Location are to the definitions of said terms as set out in the Service Definition (where applicable).

1.2. The Service Provider will provide the Services in accordance with operational and support procedures defined and agreed with the Customer as part of the Implementation Services and documented in the Procedure Manual. The scope of the Procedure Manual and the applicable provisions of this Service Level Agreement are limited to the Services (including any related Hardware) as detailed in the Service Definition.

1.3. For the purposes of this Service Level Agreement, unless stated otherwise in the Service Definition, the Service Levels apply to both any dedicated Hardware and any Shared Service as set out in Article 3 of the Service Definition, whether owned by the Service Provider or Customer (collectively the "**Customer Environment**"). This Service Level Agreement will only apply to the Services as from the Services Commencement Date.

2 Hosting Services

Where specified in Article 4 of the Service Definition the Service Provider will undertake hosting of the Customer Environment in the Service Provider's Premises as specified in the Service Definition. This Service element will be available 24x7x365.

3 Operational Support

Where specified in Article 4 of the Service Definition the Service Provider will provide Operational Support to include: (i) monitoring the Customer Environment as specified in the Service Definition, (ii) acting on Alerts as described in Clause 7, and (iii) performing any external visual checks of any Customer owned Hardware on request by the Customer where the Customer Environment is hosted by the Service Provider. This Service element will be available 24x7x365.

4 Media Management & Offsite Storage

Where specified in Article 4 of the Service Definition all magnetic media associated with the backups outlined in Clause 6 will be retained by the Service Provider in secure storage separate from the Premises listed in the Service Definition, and only moved to another location when required for the Backup Schedule (as defined herein) or at specific Customer request. This Service element will be available 24x7x365.

5 CDP Service

5.1. Where the CDP Service is specified in Article 4 of the Service Definition, the Service Provider is responsible for ensuring that changes made to the Protected Data (as defined in the Service Definition) will be captured and replicated to the CDP Environment (as defined in the Service Definition). The Service element will be available 24x7x365.

5.2. Where specified in the Service Definition, selected backups of the Customer's Protected Data (or part thereof) on the CDP Environment will be taken offline to tape media by the Service Provider on an frequency as specified in Schedule 3: Pricing.

5.3. Unless specified otherwise in the Service Definition, the Customer is responsible for all data restoration activities at the Primary Location as well as for ensuring that all Customer infrastructure components including servers and storage are appropriately backed up, whether utilising any Backup Appliance(s) or VTL Appliance(s) or not (as deemed applicable by the Customer).

6 Online Backup Service

6.1. Where specified in Article 4 of the Service Definition backups of the Customer's data from the Customer Environment (whether to online storage such as disk media or offline storage such as tape media) will be carried out in accordance with a schedule agreed between the Customer and the Service Provider (the "**Backup Schedule**") and documented in the Procedure Manual.

6.2. The Service Provider will be responsible for the reporting and verification that backups are successfully taken in accordance with the Backup Schedule and that they meet the agreed criteria. This Clause 6 will apply to both the Online Backup Service as described in the Service Definition and any backups taken to offline storage such as tape media.

6.3. The Service Provider will be responsible for any data restoration activities required on the Customer Environment as specified in the Service Definition. Data restoration activities will be available between 08:00 and 18:00 Monday to Friday (excluding public holidays) except if the appropriate response as a result of a Critical Incident (as defined in Article 2 Clause 5) requires the Service Provider to make available data restoration activities outside of those hours.

6.4. For the avoidance of doubt data restore requests shall be treated as Incidents (excluding planned restore testing) and the Service Provider shall respond to each data restore request in accordance with the appropriate Response Time as detailed in Article 2 Clause 5. The Customer shall at its discretion determine the Assigned Severity for each data restore Incident.

7 Infrastructure Monitoring

7.1. Where specified in Article 4 of the Service Definition the Service Provider will provide Infrastructure Monitoring to highlight abnormal and/or exceptional conditions ("**Alerts**") and automatically respond and/or route them to the Service Provider's Service Desk. This Service element will be available 24x7x365.

7.2. Where an Alert results in or relates to an Incident the Service Provider will respond in accordance with the appropriate Response Time as detailed in Article 2 Clause 5. Application software Alerts will be routed to the Customer or appropriate third party providers via an agreed logging and escalation procedure or resolved via an agreed procedure, each as documented in the Procedure Manual.

7.3. For each Alert logged with the Service Provider Service Desk the Service Provider will perform the appropriate procedure as documented in the Procedure Manual or otherwise in accordance with Good Industry Practice. For Customer application issues the determination of appropriate actions will be dependent upon the availability of documented procedures provided by and agreed with the Customer.

8 Anti-Virus Management

8.1. Where specified in Article 4 of the Service Definition, the Service Provider will provide Anti-Virus Management for items of the Customer Environment for the technologies as specified in Article 4 of the Service Definition. This Service element will be available 24x7x365.

8.2. Virus definition database updates (where available) will be performed no less frequently than every twenty four (24) hours. All other updates which may require a restart or would otherwise impact Availability will be treated as a Patch and will be subject to Patch Management pursuant to Clause 9.

8.3. In addition to proactive scans of data and other information as it is added, changed and/or accessed via activity on each server instance, a regular comprehensive scan of memory and storage related to each server instance shall be performed by the Service Provider at a time and frequency, normally on a daily or weekly basis, as agreed with the Customer and documented in the Procedure Manual.

9 Patch Management

9.1. Where specified in Article 4 of the Service Definition, the Service Provider will provide Patch Management for Software within the Customer Environment and listed in the Service Definition as the responsibility of the Service Provider, subject to the Change Control Procedure as defined herein.

9.2. Patch Management to include the review, loading, and preparation activities for Software Patches will be performed during the Business Day except in the case of Emergency or approved Changes which will be managed in accordance with the Change Control Procedure. The application of Patches shall be completed in accordance with Clause 9.3 below.

9.3. Emergency Patches (as determined by the original software vendor) will be applied within twenty four (24) hours of the Patch being identified and made available to the Service Provider together with an emergency Change request from the Customer, or as otherwise agreed with the Customer. Preventative (non-mandatory) Software updates will be applied in accordance with a release schedule agreed between the Parties for such updates, normally on a quarterly basis, and documented in the Procedure Manual.

9.4. Subject to Clause 9.5 and availability of Software Version or Release upgrades from the original software vendor, the Service Provider will perform one (1) Software Version or Release upgrade every two (2) years per server, appliance or logical partition as an alternative to a regular Patch application as described in Clause 9.3.

9.5. The Service Provider and Customer shall work in good faith to agree the implementation approach and timeline for any Software Version or Release upgrade. The Service Provider reserves the right to levy additional one time charges where; (i) such Version or Release upgrade cannot be performed solely based on the original vendor supplied installation / upgrade instructions; (ii) the Service Provider is required to perform additional testing activities other than verifying successful installation and updates to the Software; or (iii) the Customer requires additional resources including Hardware to perform testing of applications, other third party software and/or business operations following the Software version or release upgrade.

9.6. For the avoidance of doubt the Service Provider is only obliged to provide Patch Management for software products still supported by the original software vendor. The Service Provider shall inform the Customer of any upcoming withdrawal of support by original software vendors during Service Reviews (as defined herein) and the Parties shall work together to agree the appropriate actions (if required) for ensuring the Customer Environment remains within original software vendor support.

10 Support and Management

Where specified in Article 4 of the Service Definition, and for the technologies specified in the Service Definition, the Service Provider will provide technical support and management for the Customer Environment. Support and Management will be available 08:00 to 18:00 Monday to Friday on Business Days except for resolving Critical incidents, which shall be on a 24x7x365 basis for specific environments where detailed in the Service Definition.

11 Hardware Maintenance

11.1. Where the Service Provider is responsible for the provision of Hardware Maintenance services for the Hardware owned by the Customer this will be subject to a separate contractual agreement between the Parties.

11.2. Hardware Maintenance for the Shared Service will be provided by the Service Provider with a four (4) hour response Service Level. This Service element will be available 24x7x365.

12 Disaster Recovery Services

12.1. Where the Service Provider is responsible for the provision of Disaster Recovery Services for Hardware owned by the Customer this will be subject to a separate contractual agreement between the Parties.

12.2. Where specified in Article 4 of the Service Definition, the invocation process for Disaster Recovery Services where Services utilise Server Provider owned Hardware will be defined and agreed for individual components as well as the total Customer Environment. This will include nominated Customer and Service Provider contacts together with appropriate escalation paths.

12.3. In the event of an Invocation the Service Provider will implement the agreed procedures as set out in the Procedure Manual to provide a Customer Environment for all servers and/or appliances for which the Disaster Recovery Services applies as described in the Service Definition. The Recovery Point Objectives and Recovery Time Objectives as determined by the Customer for individual servers may vary and will be documented in the Procedure Manual.

12.4. For the avoidance of doubt, measurement of the Recovery Point Objective is from the point of failure and measurement of the Recovery Time Objective is from the point at which recovery is initiated for each server based on the documented order of recovery. The Service Provider is only responsible for recovery of individual servers up to and including the Operating System. All other infrastructure and application support and management responsibilities are described in the Service Definition.

12.5. The Customer acknowledges that the ability of the Service Provider to identify when any documented Recovery Point Objective and Recovery Time Objective cannot be achieved is contingent upon the Service Provider being permitted by the Customer to perform test Invocations for all servers at least on an annual basis during the Schedule Term (or any extension thereof) and the Parties agreeing any identified service improvements via the Change Control Procedure or Variation Procedure (as applicable).

13 High Availability Services

13.1. Where specified in Article 4 of the Service Definition, the Role Swap (as defined in the Service Definition) process for High Availability Services will be defined and agreed both for individual components as well as for the total Customer Environment. This will include the nominated Customer and Service Provider contacts together with the appropriate escalation paths.

13.2. In the event of a Role Swap the Service Provider will implement the agreed procedures as set out in the Procedure Manual intended to provide a Customer Environment for all servers and/or appliances for which the High Availability Service applies as described in the Service Definition within a Recovery Point Objective of thirty (30) minutes and a Recovery Time Objective of two (2) hours. The achieved recovery point for individual servers may vary depending upon the nature of the failure and the time of day. The order of recovery for individual servers will be agreed and documented in the Procedure Manual.

13.3. For the avoidance of doubt, measurement of the Recovery Point Objective is from the point of failure and measurement of the Recovery Time Objective is from the point at which recovery is invoked for each server based on the documented order of recovery. The Service Provider is only responsible for recovery of individual servers up to and including the Operating System. All other infrastructure and application support and management responsibilities are described in the Service Definition.

13.4. The Customer acknowledges that the ability of the Service Provider to achieve the Recovery Point Objective and Recovery Time Objective as described in this Clause 13 is contingent upon:

a) each individual server being protected by high availability, clustering and/or data replication services with separate instances of a server maintained in different Service Provider Premises; and

b) the Service Provider being permitted by the Customer to perform test Role Swaps for all servers at least on an annual basis during the Schedule Term and address any identified service improvements via the Change Control Procedure.

14 Service Desk

The Service Provider provides a manned Network Operations Centre and Service Desk which is available 24x7x365 with no exclusions via the telephone number 0330 0940 400 or email address Service.Desk@bluechip.co.uk**.** With the exception of the reporting of Critical Incidents (as defined in Article 2 Clause 5), which shall always be reported to the Service Desk via telephone, the Customer can also choose at its own discretion to use the Service Provider's online portal for submitting any requests which would otherwise be submitted by it to the Service Desk.

15 Service Delivery Management

15.1. The Service Provider shall nominate a Service Delivery Manager as primary contact for matters relating to the delivery and performance of the Services and have the responsibilities as defined in the Service Definition.

15.2. The Customer Representative and the Service Delivery Manager will meet on a regular basis (the "**Service Review**") to an agreed schedule at location(s) within the United Kingdom, and/or using video conferencing facilities, as agreed between the Parties. During the Service Review the Parties will review the Service Reports (as defined herein) and the performance of the Services against the Service Levels described herein, and where applicable the Continuous Service Improvement Plan ("**CSIP**"). In the event the Service Provider has been unable to achieve one or more Service Levels for a period of two (2) consecutive months or more it shall also be obliged to present a plan to remedy the deficiencies in the Services (a "**Service Improvement Plan**") to the Customer at the Service Review.

15.3. During the Assessment Period (as defined herein) the performance of the Service Provider and Services may be regularly reviewed against any measures agreed in writing by the Parties (the "**Assessment Criteria**"). Where the Parties agree that the performance of the Service Provider and/or the Services does not meet the Assessment Criteria or at a minimum meet the measures stated in Article 2:

a) the Assessment Criteria may be updated by mutual consent of the Parties to adjust the measures used for the basis of reviews to reflect a change in Customer operations and/or requirements; and/or

b) a Change to the Services may be requested as detailed in the Variation Procedure to ensure that the measures used for the basis of reviews can be achieved.

Without prejudice to any rights and remedies of the Customer, in the event the Parties cannot reach agreement as to an appropriate action in accordance with this Clause 15.3 the Dispute Resolution Process as documented in the Master Services Agreement shall be invoked.

16 Service Reports

16.1. The Service Provider will provide service management information (the "**Service Reports**") as agreed with the Customer at a frequency not to exceed once per calendar month. The Service Reports will identify all issues and exceptions arising from the performance of the Services. Service Reports will be available to the Customer no later than ten (10) Business Days after the end of the reporting period (i.e. the calendar month to which they relate) and the content shall include:

a) System metrics such as processor, memory and storage utilisation;

b) Incident and problem management information;

c) Change requests and actions;

d) Service Availability reporting;

e) Reports relating to specific Services set out in the Service Definition such as vulnerability scanning and compliance; and

f) All services listed and measured as described in Article 2.

17 Service Hours

17.1. The general hours during which the Services are available are Monday to Sunday 00:00 to 24:00, including public holidays. The service hours for each individual Service (if different) are specified in the appropriate clauses of this Article 1.

17.2. The Service Provider may perform planned maintenance ("**Planned Maintenance**") activities on the second weekend of each calendar month commencing at 22:00 on Saturday and completing no later than 03:00 on Sunday. Planned Maintenance will not include any activities that will result in service outages, planned or unplanned, although the resilience of the Services (or part thereof) may be reduced during Planned Maintenance.

17.3. The Customer may plan unlimited maintenance windows per annum for any facilities, hardware, and/or software that are its responsibility and shall provide reasonable notice of such maintenance to the Service Provider in the event the maintenance will or may have an impact on the Services, such as the generation of Alerts.

17.4. Requests for a planned service outage ("**Planned Service Outage**") will be notified to the Customer at least one (1) month prior to the Planned Service Outage and shall be subject to the Change Control Procedure. The Service Provider may require two (2)

Planned Service Outage windows per annum each of which will not exceed ten (10) hours in duration. Subject to Article 2 Clause 7.2 Planned Service Outages shall not be deemed periods of unavailability for the purposes of service delivery metrics.

17.5. At the request of the Customer, availability of the Services may be maintained during a Planned Service Outage where the Customer has contracted additional resilience that permits continued operation and requests that it be utilised, including the ability to operate from alternate Premises to that used for normal Production operations.

17.6. The Service Provider shall ensure that Planned Maintenance and Planned Service Outages do not occur within the hours of 08:00 to 22:00. Planned Service Outages shall always be notified to the Customer as specified in Clause 17.4 and be planned by the Service Provider in such a way as to have minimum impact on the Customer's operations.

17.7. A minimum of forty eight (48) hours notification will be provided by the Service Provider for unscheduled maintenance, except where maintenance is considered by the Service Provider to be critical ("**Emergency Maintenance**"), when as much notice will be given as possible. The Service Provider will only carry out unscheduled maintenance where essential for the continuing performance of the Services. The Service Provider will notify the Customer in writing how long such unscheduled or Emergency Maintenance is expected to take.

18 Operational Change Management

18.1. All operational (non-material) Changes to the Services are subject to the terms described in this Clause 18 (the "**Change Control Procedure**") and therefore prior to the commencement of any work a Change Request Form must be completed and authorised by both Parties. All Services as defined in the Service Definition are subject to the Change Control Procedure. For the avoidance of doubt any material Changes to the Agreement or the scope of the Services will be handled via the Variation Procedure.

18.2. Emergency Change requests requiring submission and completion outside the Business Day can be raised by contacting the Service Provider's Service Desk via email with details of the request and confirming the reason for the emergency by telephone. For the purposes of this Clause 18, an "**Emergency Change**" request means an operational Change request which is identified or otherwise labelled by the Customer as an emergency

18.3. Each operational Change request must be submitted to the Service Provider's Service Desk with the required authorisation. Any unauthorised Change requests will be rejected and returned to the Customer without assessment. The Service Provider will review and respond to valid Change requests in the following time frames and include a proposed delivery date and time in the completed response, subject to confirmation in accordance with Clause 18.4:

Change Priority	Target Response Time
Emergency	Eight (8) Hours
Normal	Two (2) Business Days

18.4. For the avoidance of doubt the target response times listed in Clause 18.3 do not constitute objectives for completion of a Change. This can only be assessed on a Change by Change basis. The Service Provider does not commit to timescales for implementation of any Change request until said Change request has been approved by both Parties. The Service Provider shall expedite the delivery of Emergency Change requests.

19 Security

19.1. The Service Provider will only access Customer systems hosted or managed by the Service Provider to the extent authorised by the Customer and required to perform the Services. The Service Provider will carefully control use of login and passwords and, unless previously agreed with the Customer in writing, the Service Provider will never give any passwords to other individuals.

19.2. All emails and files sent to the Service Provider by the Customer or third parties to assist in problem diagnosis must be sent through the Service Provider mail server, thus ensuring necessary precautions relating to software viruses have been taken. In the event the Customer requires email and file transmissions to be encrypted the Service Provider will provide such encryption subject to the Customer accepting the reasonable costs of implementing any Customer specific encryption service elements. For the avoidance of doubt, file transmission via Secure File Transfer Protocol (SFTP) can be provided without additional cost.

ARTICLE 2 - SERVICE MEASUREMENT

1 Availability Based Service Elements

1.1. The Service Provider shall commit to service availability levels on the following key elements:

a) The electrical power to any bus bar in the Service Provider's Premises to which the Hardware is connected (the "**Electrical Power**"). For the avoidance of doubt, PDU output circuit breakers and the Hardware side power cabling are excluded from this warranty where the Hardware is supplied and/or owned by the Customer;

b) The temperature, humidity and dew point within the Service Provider's Premises (the "**Ambient Room Environment**") based on being maintained within the ASHRAE Class 1 guidelines;

c) The core infrastructure in the Service Provider's Premises to which the Customer is connected or needs to use in order to receive the Services including Service Provider provisioned and managed firewalls, patching units, switches and interconnecting cabling (collectively the "**Core Infrastructure**");

d) Connectivity services provisioned by the Service Provider at the Service Provider's Premises as described in the Service Definition including as applicable (i) Internet bandwidth availability to/from the Customer Environment, (ii) connectivity between the Customer's network and the Service Provider's Premises for Customer access, and/or (iii) connectivity between the Service Provider's Premises for data and other replication purposes, (collectively "**Connectivity Services**").

e) The availability of individual appliances, physical servers, storage platforms, logical partitions ("**LPAR**"), and virtual servers (collectively known as the "**Server Infrastructure**") to the Customer for use by the Customer's business, users and/or applications and where managed by the Service Provider.

2 Availability Based Service Element Reporting

2.1. Where the Customer Environment resides in the Service Provider's Premises the Service Reports will include details (including durations) of any interruptions to the Electrical Power that impacted the availability of the Services (a "**Power Incident**"). For the purpose of those reports the start time of a Power Incident (the "**Incident Start Time**") shall be defined and measured from the time the failure is detected by the Service Provider or is reported by the Customer to the Service Provider whichever is the earlier. The end time of a Power Incident (the "**Incident End Time**") shall be defined as the time at which the power supply can be demonstrated by the Service Provider to be available at the PDU bus bar.

2.2. Where the Customer Environment resides in the Service Provider's Premises the Service Reports will include details of any deviations from the Ambient Room Environment that impacted the availability of the Services (an "**Environment Incident**"). For the purpose of those reports the start time of an Environment Incident (the "**Incident Start Time**") shall be defined and measured, from the time the Ambient Room Environment deviation is detected by the Service Provider, or is reported by the Customer to the Service Provider (whichever is the earlier). The end time of an Environment Incident (the "**Incident End Time**") shall be defined as the time at which the Ambient Room Environment can be demonstrated by the Service Provider to have returned to within the Service Level parameters.

2.3. Where the Customer Environment resides in the Service Provider's Premises the Service Reports will include details (including durations) of any interruptions to the Core Infrastructure that impacted availability of the Services (a "**Core Incident**"). For the purpose of those reports the start time of a Core Incident (the "**Incident Start Time**") shall be defined and measured from the time the failure is detected by the Service Provider or is reported by the Customer to the Service Provider whichever is the earlier. The end time of a Core Incident (the "**Incident End Time**") shall be defined as the time at which the Core Infrastructure can be demonstrated by the Service Provider to be available to the Customer for the purposes of the Services.

2.4. Where Connectivity Services are provisioned by the Service Provider at the Service Provider's Premises the Service Reports will include details (including durations) of any interruptions to the connectivity that impacted availability of the Services (a "**Connectivity Incident**"). For the purpose of those reports the start time of a Connectivity Incident (the "**Incident Start Time**") shall be defined and measured from the time the failure is detected by the Service Provider or is reported by the Customer to the Service Provider whichever is the earlier. The end time of a Connectivity Services Incident (the "**Incident End Time**") shall be defined as the time at which the connectivity can be demonstrated by the Service Provider to be available to the Customer for the purposes of the Services.

2.5. The Service Reports will include details (including durations) of any interruptions to the Server Infrastructure that impact the delivery of the Services (a "**Server Incident**"). For the purpose of those reports the start time of a Server Incident (the "**Incident Start Time**") shall be defined and measured from the time the failure is detected by the Service Provider or is reported by the Customer to the Service Provider whichever is the earlier. The end time of a Server Incident (the "**Incident End Time**") shall be defined as the time at which the Server Infrastructure can be demonstrated by the Service Provider to be available to the Customer for the purposes of the Services

3 Service Levels for Availability

For purposes of measuring performance against Service Levels, availability ("**Availability**") will be calculated each calendar month as defined in Clause 6. Service Credits will be available pursuant to Clause 8 where one or more Service elements fails to achieve the Availability for a calendar month as specified herein and specifically the table below:

Service Element	Availability
Electrical Power	99.99%
Ambient Room Environment	99.99%
Core Infrastructure	99.99%
Connectivity Services (without resiliency)	99.80%
Connectivity Services (with resiliency)	99.99%
Server Infrastructure (without high availability)	99.90%
Server Infrastructure (with high availability)	99.95%

4 Service Levels for Operational Services

4.1. For purposes of measuring performance against Service Levels for the Service elements listed in the table below (the "**Operational Services**"), Availability will be calculated each calendar month as defined in Clause 6. Service Credits will be available pursuant to Clause 8 where an Operational Service fails to achieve an SLA Measure for that month as specified herein and specifically the table below:

SLA Description	SLA Details	SLA Measure
Service Desk Availability	Availability of the Service Desk for call logging	100% Availability
Infrastructure Monitoring	Service Provider Services monitoring availability	100% Availability
Event Response Times	Time taken to notify the Customer of Unknown Alert	95% within thirty (30) minutes
DDoS Mitigation Time	Time taken to start mitigation for an attack	100% within fifteen (15) minutes

4.2. For the avoidance of doubt, an unknown Alert ("**Unknown Alert**") for the purposes of this Clause 4 is an Alert that is not related to a standard Operating System message and is not documented in the Procedure Manual with appropriate actions to be performed by the Service Provider.

4.3. The DDOS Mitigation Time SLA Measure only applies where Distributed Denial of Service ("**DDoS**") protection is included in the Service Definition, and is measured from the point (as applicable) that a DDoS attack is either (i) automatically detected by the Service Provider or (ii) the Customer notifies the Service Provider that an attack presently exists by raising a Critical Incident with the Service Desk, whichever is the earlier.

5 Service Levels for Incidents

5.1. The severity level for an Incident or Service Request (the "**Assigned Severity**") is to be selected by the Customer at the time it is logged with the Service Provider based on the following classification. On being logged, each Incident and Service Request will be allocated a unique reference number by the Service Provider:

a) **Critical** – The Customer can no longer perform critical business functions; there is a material loss or corruption of data; a critical deadline is affected and there is no known workaround without reduction of functionality;

b) **Major** – There is loss of functionality but a workaround is in place with no reduction of functionality and there is no significant impact upon the Customer arising from the workaround;

c) **Medium** – There is loss of functionality with no requirement for a work around as there is no significant impact upon the Customer;

d) **Low** – Fault recognised, no business impact and no workaround required;

e) Service Requests – No fault, technical support or "how to" questions.

5.2. The Service Levels for Incident and Service Request Response Times and Update Frequencies (each as defined in Clause 5.3) are set out in the table below. Service Credits will be available pursuant to Clause 8 where the Service Provider fails to achieve the

SLA Measure (as out in the table below) in any particular month for Response Times against Incidents logged via telephone support and automated alerting:

Assigned Severity	Response Time	SLA Measure	Update Frequency
1 – Critical	15 minutes (24x7x365)	95% within Response Time	2 Hours (24x7x365)
2 – Major	30 minutes during Business Day	90% within Response Time	4 Hours during Business Day
3 – Medium	4 hours during Business Day	85% within Response Time	1 Business Day
4 – Low	8 hours during Business Day	Not Applicable	5 Business Days
5 – Service Requests	Next Business Day	Not Applicable	10 Business Days

5.3. For the purposes of this Schedule and the table in Clause 5.2, response time (the "**Response Time**") is defined as the time after an Incident or Service Request is logged with the Service Desk before diagnostic actions commence by suitably qualified Service Provider Personnel and the Incident update interval (the "**Update Frequency**") is the maximum period of time (unless agreed otherwise for a particular Incident or Service Request) between informative updates from the Service Provider to the Customer on progress to resolution or completion (as applicable).

5.4. The Service Provider will update the Procedure Manual for any Customer specific Incident profile in accordance with the Assigned Severities detailed in Clause 5.1. This will necessitate definition of the anticipated types of calls that may be received by the Service Provider and how they will be responded to depending upon the Service Levels for each component of the Customer Environment.

5.5. The Service Provider's performance in achieving the Response Time will be measured and reported through the Service Reports and calculated as detailed below for each individual level of Assigned Severity as described to this Clause 5:

Response Time (%) = Number of Response Times exceeding Service Levels in Month / Total number of incidents in Month x 100%

5.6. For the avoidance of doubt the Service Provider's performance will only be measured against Incidents that relate to the Services and not for Alerts or any Incidents that were incorrectly logged with the Service Desk and/or are not the responsibility of the Service Provider to resolve. If on investigating a logged Incident the Service Provider confirms that there is no fault with the Services or the fault was not the responsibility of the Service Provider to resolve, the Service Provider shall be entitled at its discretion to levy charges for out of scope activities as described in Schedule 3: Pricing.

5.7. No later than twenty four (24) hours after the reporting of a Critical Incident (unless agreed otherwise between the Parties), the Service Provider shall provide the Customer with an Initial Findings Document (IFD) providing as much information as is available at the time in relation to the root cause of the Critical Incident and the actions taken and/or planned to resolve it.

5.8. As soon as is reasonably practicable after the resolution of each Critical Incident and in any event within five (5) Business Days, the Service Provider shall deliver to the Customer a Root Cause Analysis (RCA) report in such form as the Customer may from time to time require on the cause and action taken to resolve the Incident including:

a) the root cause of the Incident where identified;
b) the actions taken by the Service Provider to resolve or workaround the Incident;
c) the outcome of those actions; and
d) any further remedial action that is required or desirable to prevent any recurrence.

5.9. The update and escalation procedures are documented in the Procedure Manual. The logging and maintenance of Incidents and other information in any Customer service desk and/or service management software is a Customer responsibility. Any assistance by the Service Provider in this respect will be subject to additional charge.

6 Service Availability Calculation

6.1. A Service is unavailable when there is an interruption to the Service being delivered to the Customer or the Ambient Room Environment falls outside the thresholds stated in Clause 1.1. The Availability of Services is measured over a calendar month and is defined as:

Availability (%) = (Total Hours in Month - Total Period of Unavailability)/ Total Hours in Month x 100%

6.2. For the purposes of calculating Availability of the Services a calendar month will commence on the first day of each month and end on the last day of each month except: (i) where the Service Commencement Date falls part way through a calendar month the first calendar month shall be deemed to commence on the Service Commencement Date; and (ii) the last calendar month shall be deemed to end on the last day of the month in which the Services are provided, whether part of the Exit Transfer or otherwise

7 Service Availability Limitations

7.1. The Service Provider shall not be liable for any failure to comply with the Service Levels defined where such failure has been caused by the Customer's material breach of any obligations set out in the Agreement and such breach impacts on the Service Provider's ability to achieve the Service Levels. In calculating Service Availability or the right of the Customer to claim Service Credits the following circumstances are excluded from the calculation as stated in Clause 6.1:

a) Service unavailability as a result of Service suspension pursuant to the Master Services Agreement;
b) Failure or malfunction of Customer equipment, applications or systems not owned or controlled by the Service Provider;
c) Failure where Good Industry Practice patching has not been permitted by the Customer on the failed component;
d) Defects in applications and/or other software not owned or controlled by the Service Provider;
e) Service unavailability to the extent due to faults on the Customer's side of the service;
f) Service unavailability to the extent due to circumstances created by the Customer;
g) Faults that do not affect Availability of the Services;
h) Service unavailability due to Planned Service Outages;
i) Service unavailability due to a Force Majeure Event.

7.2. For the avoidance of doubt, any period by which (i) actual time spent on Planned Service Outages exceeds the period notified to the Customer in accordance with Article 1 Clause 17.4 or (ii) Planned Maintenance results in a service outage, shall contribute towards the Total Period of Unavailability factor in the Availability calculation at Clause 6.1.

8 Service Credits

8.1. Without limiting the rights and remedies of the Customer for the matters other than the Service Provider's performance against the Service Levels and subject to Clause 9 the Service Credits set out in this Service Level Agreement are the only remedy available to the Customer for any failure of the Service Provider to comply with the Service Levels, with the exception of Critical Service Failures pursuant to Clause 9.

8.2. For the purposes of this Clause 8 the value of individual and the total Service Credits is based on the amount (excluding VAT) of the annualised Service Charges (payable as at the month for which any Service Credits are being calculated) divided by twelve (12) (the "**Monthly Service Charge**"). Irrespective of the total number of Service Credits claimed, the maximum amount payable by the Service Provider by way of Service Credits to the Customer in any one (1) month shall not exceed fifty (50) percent of the Monthly Service Charge.

8.3. For each calendar month that the Service Provider fails to achieve Availability for a measured Service Element, the Customer may claim a Service Credit for each separate failure of the Service Element that impacted the Customer's ability to access and/or use the Services. Where a service failure impacts multiple Service Elements it is the Customer's sole discretion as to which Service Credit is claimed. Only one (1) Service Credit may be claimed per failure. Service Credits are calculated as per the table below, and vary according to the Service Element as described:

Service Element	Critical Service Element	Service Credit
Electrical Power	Yes	10% of the Monthly Service Charge
Ambient Room Environment	Yes	10% of the Monthly Service Charge
Connectivity Services	Yes	10% of the Monthly Service Charge
Core Infrastructure	Yes	10% of the Monthly Service Charge
Server Infrastructure	Yes	10% of the Monthly Service Charge
Operational Services	No	5% of the Monthly Service Charge
Service Desk Response Times	No	5% of the Monthly Service Charge

8.4. In the event of any downtime during a calendar month the Service Reports will confirm the Availability of the Services for that period, and a list of all Incidents related to the delivery of Services to the Customer. It is the Customer's responsibility to submit a written or email request for Service Credits to the Service Delivery Manager within twenty (20) Business Days of receiving the Service Reports from the Service Provider. Requests for Service Credits outside this timeframe will not be honoured.

8.5. With the exception of Power Incidents and/or Environment Incidents where the Service Provider is delivering hosting services the Customer does not have the right to claim Service Credits and/or a Critical Service Failure pursuant to Clause 9 for the first month following the Services Commencement Date (the "**Assessment Period**"). During the Assessment Period the performance of the Service Provider and the Services shall be measured, reported on and reviewed as detailed in Article 1 Clause 15.3.

9 Critical Service Failures

9.1. The Service Provider accepts that severe perturbation of the provision of the Services should be treated differently from a single Incident. For the purposes of this Schedule and the Agreement the following will be deemed a catastrophic service outage ("**Catastrophic Service Outage**"):

a) a Power Incident in the Service Provider's Premises where Customer owned Hardware is hosted in the Service Provider's Premises; or

b) if the Service Provider is unable to restore the Critical Service Elements defined in Clause 8.3 to operate to full operation within eight (8) hours.

9.2. For the avoidance of doubt, the Server Infrastructure Availability will only be tested against 9.1 in the event of unavailability of any physical hardware and/or the failure of any iSeries and pSeries server(s) whether physical or LPAR. The failure of individual x86 virtual servers is excluded from the scope of this Clause 9.

9.3. Where there have been either (i) three (3) or more Catastrophic Service Outages in any rolling twelve (12) calendar month period; or (ii) there is a breach of the Service Levels for the same Critical Service Element in three (3) consecutive months at any time within a rolling six (6) month period, then the Customer shall (in addition to any Service Credits pursuant to Clause 8) be entitled to claim a critical failure of the Services (a "**Critical Service Failure**") and termination rights in accordance with the Master Services Agreement.

9.4. Where Customer owned Hardware is hosted in the Service Provider's Premises the Customer must ensure that all such Hardware has the ability to (and has been configured to actively) use all pertinent resilience attributes of the Services. The Customer must ensure that each item of the Hardware has two (2) connection points to the Electrical Power as provided by the Service Provider, with each connection point being to a separate half of the protected dual diverse service.

9.5. For the avoidance of doubt if the Customer does not ensure Customer owned Hardware complies with the requirements of Clause 9.4 in all material respects, then the Service Provider is exempted from any and all obligations, tests and/or other implications under this Service Level Agreement and the Agreement with regards to Critical Service Failures.

ARTICLE 3 – SERVICE PROVIDER'S PREMISES ACCESS POLICY

1 Premises Access Procedure

1.1. Subject to this Clause 1 and pursuant to the Master Services Agreement, the Service Provider will authorise and grant access to enter a Premises at all times, twenty four (24) hours a day seven (7) days a week, for the purpose of carrying out any necessary maintenance and/or installation activities. The procedure to be followed is dependent upon the reason for the access;

a) for non-emergency requests the Customer should submit (with at least twenty four (24) hours notice) a Service Request via the email address provided in Article 1 Clause 14, accompanied by the reason for access being requested, the names and contact details of Personnel and/or third parties to attend, and details of any special information (i.e., pre-arrival equipment deliveries, use of quarantine areas, etc.);

b) for emergency requests the Customer should contact the Service Provider (with as much notice as possible) on the telephone number provided in Article 1 Clause 14 specifying the reason for access being requested, the names and contact details of Personnel and/or third parties to attend, and details of any special information (i.e., pre-arrival equipment deliveries, use of quarantine areas, etc.);

1.2. The Service Provider shall be entitled to charge the Customer at the applicable rate as described in Article 2 of Schedule 3: Pricing where access to the Premises is required for non-emergency work outside Normal Working Hours including for the accompanying of Customer Personnel needing access to high risk, secure and/or shared locations such as Communication Rooms.

1.3. The Service Provider is authorised to reject or delay granting access to a Premises in the event that authority of the Customer Personnel submitting an access request in accordance with Clause 1.1 cannot be verified and/or on arrival at the Premises an authorised person with approved access does not have sufficient proof of identity.

1.4. The Customer shall supply the Service Provider with an escalation contact to be used in the event that access to a Premises is requested by Personnel or a third party not on a Service Request or other access request and/or access to the Premises is to be refused by the Service Provider for whatever reason. Access to the Premises is always granted at the Service Provider's sole discretion.

2 Premises Site Conduct for Visitors

In order to maintain the security, tidiness and safe working environment within the Service Provider's Premises the following conduct rules must be complied with by every person attending such Premises, at all times:

a) visitors arriving without prior authorisation will be denied access and requested to contact the relevant Service Provider Representative or the Customer as required to obtain access;

b) all visitors shall register with site security and be able to provide proof of identity issued by a Governmental Authority and have knowledge of the related access request reference numbers provided by the Service Provider;

c) visitors must be able to confirm details of work they intend carrying out and/or reason for visit to the site security and one site representative, as per the site access request logged with the Service Provider;

d) Service Provider Personnel or an authorised representative of the Service Provider must escort visitors at all times unless agreed otherwise at the sole discretion of the Service Provider;

e) visitors must not allow access to other individuals by bypassing the access procedures, and must at all times comply with all reasonable requests from the Service Provider with regards to security and health and safety;

f) external doors and secured internal doors to the Premises are not to be left open and unattended at any time and when working in delivery containers, doors must be kept closed at all times other than for purposes of loading / unloading;

g) the Service Provider must be notified of all equipment installation within the Service Provider's Premises prior to installation to permit asset tagging and appropriate Service Provider documentation updates;

h) the Service Provider reserves the right to refuse permission for mobile phones or other handheld telecommunication equipment into certain parts of the Premises whether such devices are switched off or not;

i) all refuse i.e. empty boxes, crates, wrapping etc. is to be removed and disposed of off-site and no food or drink is to be brought in or consumed within the Service Provider's Premises other than in the designated areas;

j) any articles left within the Premises except in the receptacles provided without the prior agreement of the Service Provider may be removed and disposed of in a manner to be determined at the Service Provider's discretion;

k) smoking is prohibited within all parts of the Premises and no equipment or tool capable of producing a naked flame is to be taken into the Service Provider's Premises written permission of the Service Provider; and

l) upon leaving the Premises, all visitors must inform the onsite security, Service Provider Personnel and/or other allocated authorised representative of their departure and return any security passes or other access control material.