Service Level Agreement ("SLA")

June 2025 v2

1.0 Introduction

This document is copyright of Tieva Limited and is for internal use and customer information.

Unless set out in this SLA, all capitalised terms in this SLA shall have the meaning given to them in the master services agreement to which this SLA relates ("MSA").

The purpose of this document is to define the service levels for the Services from the Supplier to the Client under the MSA.

This document should be read in conjunction with all applicable documents, which may include:

- Acceptable Use Policy;
- Service descriptions;
- MSA; and/or
- Order Form.

The Service may include modular solutions, which can be selected individually or in combination in accordance the Order Form.

2.0 Cloud Services

Cloud Services are provided on datacentre platform technologies, including private cloud, public cloud (hyperscale), hybrid cloud, and/or on-premise "Cloud Services".

3.0 Cloud Services Availability

The Service is designed to provide 99.9% Availability. "Availability" is defined as the Service being available for Client use,.

Service Availability (see Paragraph 5) is calculated to exclude any scheduled maintenance and Scheduled Downtime.

Scheduled maintenance and/or Scheduled Downtime on Cloud Services is initiated by the Supplier requesting approval from the Client's Representative. It is designed to implement requested changes such as configuration changes and/or Software upgrades but may also include installation of hot-fix service packs, hardware replacement, and/or hardware upgrades. Scheduled maintenance or Scheduled Downtime may also include shutdowns or re-starts that occur in the normal course of maintaining devices.

Scheduled maintenance on Cloud services are typically timed, but not guaranteed, to be outside Normal Business Hours and, given the infrastructure design, may not require any interruption to the Service. The timing of all such maintenance events will be communicated by email at least 72 hours in advance and, wherever possible,
pre-agreed with all Clients.

For Clients subscribed to Cloud Services, managed security, managed server, managed patch, and/or managed AV, the risk presented by software vulnerabilities is minimised and mitigated by the Supplier using commercially reasonable endeavours. The Supplier monitors security threats and updates, which are categorised as either 'critical' or 'non-critical' at the Supplier's sole

discretion. Critical patches are tested and released as a priority, whereas non-critical patches are scheduled into a program release as part of planned maintenance. All software releases are pre-notified to the Client upon reasonable notice.

On Cloud Services, the Supplier shall use its reasonable endeavours to ensure the maximum aggregate time for any maintenance is confined to less than 2% of the total number of minutes in any month. and if that time is exceeded, the excess time shall count for the purposes of Service Credit Calculations (see 5.0 below). In the event that Service Availability should fall below 99.9% for Cloud Solutions in any month, the sole remedy will be Service Credits.

The Client acknowledges that the Supplier does not have sole control of the datacentre or communication lines providing connectivity. Please refer to the MSA, which must be read in conjunction with this SLA.

The Client acknowledges that some Services depend entirely on wide-area-network provision and where not provisioned within the Service undertakes to provide suitable connectivity with appropriate resilience and SLA. The Supplier will not be responsible for, or award Service Credits to the Client, in any event resulting from third-party failures.

4.0 Service Management

4.1 Monitoring

If specified in the Order Form, the Supplier shall provide a help support desk, staffed with help desk technicians sufficiently qualified and experienced to identify and resolve most support issues relating to the Services ("Service Desk").

The Supplier uses monitoring tools to check and verify the health of the devices within the Service. Device Availability is tested in accordance with the applicable monitoring booklet made available to the Client by the Supplier. The Supplier's Service Desk is visually alerted if any monitored Business System fails to respond. The Supplier also monitors device logs and performance files to check optimal performance and provides reports at relevant Service review meetings, which allows the customer to verify Availability statistics.

Any Cloud Service perimeter firewalls are managed and monitored by the Supplier. By default, all firewalls are configured to deny all ports. Specific ports will be opened by mutual consultation prior to the Commencement Date or Services Commencement Date (as applicable), following which; the opening of additional ports must be specifically requested through a Change Request (as set out in the MSA).

4.2 Incident Management

The Supplier operates the following process:

- Provision a Service Desk for the reporting of support incidents, fault or vulnerabilities in the Managed Services ("Incident"), within contracted hours, as set out in the Order Form or otherwise agreed in writing between the parties, and via telephone, email, web portal, and mobile app;
- The Client may contact the Service Desk to report an Incident, and each report shall include a description of the Incident (and any start time, where relevant);
- Service Desk reasonably endeavours to answer telephone calls from the Client within 30 seconds;
- The Client shall provide the Supplier with:
    - prompt notice of any Incidents which it becomes aware of; and

- such output and other data, documents, information, assistance and (subject to compliance with all Client's security and encryption requirements notified to the Supplier in writing) remote access to the Clients Operating Environment, as are reasonably necessary to assist the Supplier to reproduce operating conditions similar to those present when the Client detected the relevant Incident and to respond to the relevant report;

- Service Desk records details of all Incidents logged by the Client and the Supplier will determine the priority of each Incident (see table under 'Escalation' section of this procedure;
- Service Desk allocates a unique Incident reference to each Incident verbally and issues an Incident acknowledgement summarising the Incident and references (by email to the person who logged the Incident unless agreed otherwise);
- Service Desk perform Incident diagnosis and instigate appropriate actions and response in accordance with this SLA;
- Service Desk escalates the Incident as required in accordance with this SLA;
- Service Desk arranges for on-site or third-party response and actions as required;
- Service Desk initiates and completes appropriate resolution to the extent that it is reasonably able to find a resolution;
- Service Desk analyses Incident history and makes recommendations to negate repeat or related Incidents, if necessary, the parties may request a change to the Services via a Change Request.).

Where a request falls outside the scope of the Service, the Supplier may provide engineering services at an additional charge. In such cases, the Supplier will work on a 'Reasonable Endeavours' basis on the Client's behalf. .

4.3 Incident Priority and Escalation

When an Incident is logged by the Client, it is classified by the Supplier based on priority (P1 to P4 – see below).

Based on the priority listed below, the Incident is escalated according to the following targets:

Priority	Estimated Response Time	Escalation Level 1	Escalation Level 2	Escalation Level 3	Communication Interval
P1	15 mins	Immediate	Immediate	Immediate	Hourly
P2	30 mins	2 hours	4 hours	2 days	Every 4 hours
P3	30 mins	8 hours	1 day	Never	Daily
P4	30 mins	2 days	Never	Never	Monthly

Unless agreed otherwise (for example, if the Client has purchased a 24/7 support package), the timeframes in the table above are based on Normal Business Hours. For the avoidance of doubt, this would mean that timeframes would pause outside of Normal Business Hours.

The time for the relevant escalation level above begins when the Supplier first acknowledges and responds to a logged Incident. The Estimate Response Time begins from the time the Incident is raised.

Key to Priority	Affecting Multiple Users	Affecting Single User
High (site, service, security breach or main LOB application unavailable)	P1	P2
Medium (system is unacceptably slow or degraded)	P2	P3
Low (system is slow and/or tasks more difficult than usual) plus Request Fulfilment (minor adds, moves, changes)	P3	P4

The escalation levels within the Supplier's business are defined as follows:

Escalation Level 1 – Service Desk Team Leader

Escalation Level 2 – Senior Engineer / Technical Services Manager

Escalation Level 3 – Group Service Desk Manager / Escalation within relevant Third Party vendor.

Escalation to relevant Third Party vendor is determined based on the nature of the Incident.

Where the Managed Services include Third Party Services the Supplier and Client shall follow the Incident Management process , however once escalated to the Third Party, that Third Party's service level arrangements shall apply and the above estimated response time and escalation times will be suspended…

If the Supplier is unable to resolve an Incident within the initial escalation, it may raise the escalation level.

Please note that the above estimated response and escalation times are times which the Supplier aims to meet but cannot guarantee due to factors which may be out of its control such as hardware failure or issues with multiple complex elements.

In the event of an Incident that involves Hardware, our estimated response time is 8 hours, and estimated resolution time 8 hours from response time, unless agreed otherwise in writing.

4.4 Service-Specific SLAs

4.4.1 The following applies across all backup services listed in this paragraph 4.4, unless agreed otherwise in writing:

IMPORTANT: The Client is solely responsible for storing any and all backup encryption keys in a secure location. Loss of any encryption keys by the Client may prevent recovery of the Services and the Client's backup data.

Data Backup and Restoration

The Client will be responsible for the availability of their network and those systems to be backed up by the applicable backup service. The Client will also be responsible for defining appropriate backup sets and schedules for those systems to be backed up.

The Supplier cannot guarantee to successfully back up all open files. The Supplier shall report on back up issues and shall use reasonable endeavours to work with the Client to resolve such issues. The Client will be responsible for reviewing such occurrences and modifying their backup sets as appropriate.

For confidentiality and security reasons, transmitted data shall not be opened or read by the Supplier. The Client shall ensure data integrity, including virus scanning, is maintained. The Client shall be responsible for performing all data restoration operations unless defined otherwise within the Order Form or elsewhere in this SLA.

Unless otherwise agreed in a given Order Form or in writing, the Client acknowledges that it is responsible for the selection and volume of data backed up and maintained within the Services. The Supplier reserves the right to charge for any and all data stored at the pro-rata rate in accordance with the MSA.

Reports

The Client will be responsible for reviewing and acting upon any reports provided by the Supplier.

RTO & RPO

- The estimated Recovery Point Objective (RPO) applies to all services. The RPO is less than or equal to 24 hours as standard, although this may be reduced if agreed in an Order Form or through a Change Request.
- Recovery Time Objective (RTO) is specific to each Client's Order Form requirements to be agreed between the Parties.

4.4.2 The following only apply to those specific Service(s) listed:

Private Cloud

If the Customer has subscribed to a Private Cloud Service, the Supplier shall maintain data backups of relevant servers and data shall be backed up once a day with an additional replica of this data copied to a geographically separate location.

The Supplier uses reasonable endeavours to make sure the backup process is effective and successful; however, the Client acknowledges that in the event of any loss or damage to data caused by the Supplier, the Supplier's sole liability and responsibility shall be to use commercially reasonable endeavours to restore the lost or damaged data from the latest backup of such data. For the avoidance of doubt, the Supplier is not liable for any direct, indirect or consequential loss which may occur. The Supplier shall not be liable for the backup of any open files, or extraneous data on the Client's site, or data resident on the local drive of a home/remote worker or any unrecognised device.

Managed Backup Service

If the Client has subscribed to managed backup Service, the Supplier shall provide one inclusive test data restoration per month, unless agreed otherwise in an Order Form or through a Change Request. This test data restoration shall be based on a single virtual machine or a single file, at the Suppliers discretion. For any additional test data restoration incidents above the pre-arranged amount, the Client shall incur charges at the Supplier's commercial rates prevailing at the time.

On-Premises Backup

If the Client has subscribed to an On-Premises Backup Service, in accordance with the applicable Order Form, the Supplier shall use reasonable endeavours to provide management and monitoring of backup operations for designated systems and data hosted on the Client's premises, using backup infrastructure provided and maintained by the Client.

Unless otherwise agreed in writing or in the relevant Order Form, the On-Premises Backup Service does not include replication to offsite or cloud locations. Such services may be arranged separately by mutual agreement and may be subject to additional charges.

Cloud Backup

If the Client has subscribed to a cloud backup service, the cloud backup provides an automated mechanism whereby the Client will be able to backup and recover data from designated devices.

The Client acknowledges the day-to-day operation of the Service provided by the Supplier will, in part, depend on certain key processes and related equipment, which are wholly under the Client's control as is the data designated for backup, which may change periodically.

The Client will be responsible for providing the necessary power, network connection, and environment to support the Service. The Client acknowledges that the Service depends entirely on wide-area-network and/or internet and must undertake to provide suitable connectivity with appropriate resilience and SLA. The Supplier will not be responsible for any incident/loss resulting from Third Party communications failures.

Disaster Recovery ("DR")

If the Client has subscribed to a DR Service in the Order Form and in the event of the Client invoking or experiencing a DR incident (actual or test), this SLA will be suspended for the duration of the DR incident. During this time, the following plan will apply:

Disaster Recovery	Typical DR incidents may include::
Classification: Client invokes a DR plan.	▪ Loss of or disruption to critical Business Systems ▪ Major data loss ▪ Loss of Client site ▪ Scheduled DR test (Pre-advised by Client to the Supplier at least 30 days prior to test)
Call Logging: within service times as set out in the Order Form	Call referred immediately to Supplier Service Desk manager who becomes the primary point of contact to coordinate the following actions:
Estimated Time to Fix: - Incident diagnosis will start immediately from the Client reporting the DR incident, and a recovery plan will be proposed to the Client depending on the exact nature, location, and scale of the DR incident. Incident resolution activity will be maintained on a 24-hour basis until the incident is resolved.	▪ Notify all relevant members of the Supplier senior management team ▪ Review previous incident history ▪ Gather diagnostics ▪ Propose repair/replacement/response ▪ Arrange technical personnel, if applicable ▪ Provide status updates to the Client ▪ Contact the Client to confirm successful resolution ▪ Provide the Client with DR incident report

PLEASE NOTE: It is highly recommended that the Client has a business continuity and/or DR plan or subscribed service, which is tested and operational.

All DR activities detailed above are chargeable at the prevailing daily rate at the time plus any/all expenses incurred in accordance with the MSA. Such charges are usually recoverable via Client insurance, but the Supplier can make no guarantees to this and reserves the right to levy charges for all DR actions and time spent by the Supplier on the DR incident.

5.0 Service Availability and Service Credits (applicable to Cloud Service only)

Service Availability is calculated on a monthly basis from the total number of minutes in the month and factored with the Availability Target of 99.9% against any minutes of the Service being unavailable excluding agreed and notified Scheduled Maintenance or Scheduled Downtime.

Service Availability is defined within this Service Level Agreement, and the total charges for the Service are defined within the Order Form. For Service below the Service Level Agreement definition of Availability, Service Credits are calculated as sole remedy and recompense to the Client.

The calculation for Service Credits is as follows:

$$\frac{\text{Non-Availability} - (\text{minutes in the Month} \times 0.1\%)}{\text{Minutes in month} \times 99.9\%} \times \text{Monthly Service Cost}$$

The maximum total Service Credit for any calendar month shall not exceed 100% of the Client's total monthly Fees for the relevant Service. Any such Service Credits exceeding the maximum total credit for a particular month cannot be carried over to another month. Service Credits are automatically calculated and applied to the Client's account and will be reported at the next applicable service review meeting.

THE RIGHT TO RECEIVE SERVICE CREDITS AS DESCRIBED IN THIS SLA IS THE CLIENT'S ONLY REMEDY FOR ANY FAILURE BY THE SUPPLIERTO MEET ANY PROMISES, GUARANTEES, AND WARRANTIES PROVIDED IN THIS SLA.

Exclusions to Service Credits

Connectivity and Third Party services, such as line of business applications from independent software vendors, are specifically excluded from Service Credits, as they are distinct and separate provisions with vendor control and/or other dependencies, over which the Supplier has little or no direct control.

Service Credits are also not calculated to include:

- Scheduled Maintenance or Scheduled Downtime
- Other maintenance performed by the Client or the Client's agents.
- Specific actions by the Client or the Client's agents on the Client's software applications.

Any of the following circumstances will invalidate any Service Credit:

- Late or overdue payment by the Client.
- Violation by the Client or the Client's agents of the Acceptable Use Policy.
- Unavailability or interruptions due to Client error or Client's agent error.
- Design, program or other defects in the Client's software applications.

- Failure to report an incident to the Supplier in accordance with this SLA or the Supplier's reasonable instructions.
- Acts beyond the Supplier's reasonable control, including but not limited to Force Majeure Events, Relief Events and any other actions beyond the Supplier's control.
- The Client's lack of availability to respond to incidents that require Client participation for resolution.
- The Client being in breach of its obligations under its Order Form, this SLA or the MSA.