Service Level Agreement (SLA)

December 2022 v1

1.0 Introduction

This document is copyright TIEVA Ltd and is for internal use and customer information.

The purpose of this document is to define the Service Description provided within the Services (the "Service") from TIEVA Ltd (the "Company") to the Customer ("Customer") under the Service Contract, which is the contract document defining Customer requirement from the Service. The Service is designed to be available, secure, fast, resilient, and scalable accommodating current and future requirements of the Customer within contract parameters.

This document should be read in conjunction with all associated documents: Service Acceptable Use Policy, Service Description, Service Level Agreement (SLA), Service Contract, which specifies prices, and the Terms and Conditions of Service, all of which govern the Service.

The Service includes modular solutions, which can be selected individually or in combination according to Customer requirement and preference. The SLA covers the Service commitments by the Company underpinning all Services, including general IT support of the Customer's technology.

2.0 Cloud Services

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

3.0 Cloud Services Availability

The Service is designed to provide 99.9% Availability. "Availability" is defined as the Service being available for Customer use, free from interruption, at the benchmark speed established and recorded at the Service Commencement Date as recorded by the Company's monitoring systems.

Service Availability is calculated to exclude Scheduled Maintenance and Planned Maintenance.

Scheduled Maintenance on Cloud services is initiated by the Company following acceptance of a Customer Change Request. 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 may also include shutdowns or re-starts that occur in the normal course of maintaining devices.

Planned Maintenance on Cloud services is designed to complete pre-planned upgrades or changes necessary to optimal management of infrastructure or facility and generally includes installation of hot-fixes, service packs, hardware replacement, and/or hardware upgrades. Planned Maintenance may also include shutdowns or re-starts that occur in the normal course of maintaining devices.

Scheduled and Planned 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 Customers.

For Customers 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 Company. The Company monitors security threats and updates, which are categorised as either

'critical' or 'non-critical' at the Company's sole discretion. Critical patches are tested immediately 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 Customer as above.

On Cloud services, the Company will ensure that 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. In the event that Service Availability should fall below 99.9% for Cloud Solutions in any month, the sole remedy will be Service Credits.

Connectivity, communication links, and datacentre provisions are usually designed to be inherently resilient, dependent on Customer requirements; however, the Customer acknowledges that the Company does not have sole control of the datacentre or communication lines providing connectivity. Please refer to the Terms and Conditions of Service, which must be read in conjunction with this SLA.

The Customer acknowledges that some Services depend entirely on wide-area-network provision and where not provisioned within the Service Contract must undertake to provide suitable connectivity with appropriate resilience and SLA. The Company will not be responsible for, or award Service Credits to the Customer, in any event resulting from 3rd party communications failures.

4.0 Service Management

4.1 Monitoring

The Company uses proactive monitoring tools to check and verify the health of the devices within the Service. Device Availability is tested at five to fifteen-minute intervals. The Company's Service Desk is visually alerted if any monitored System fails to respond. The Company also monitors device logs and performance files to check optimal performance and provides reports at Service Review Meetings, which allows the customer to verify Availability statistics.

Cloud Service Perimeter Firewalls are managed and monitored by the Company. By default, all firewalls are configured to deny all ports. Specific ports will be opened by mutual consultation prior to the Commencement Date, following which; the opening of additional ports must be specifically requested through Change Management (Section4.4). Managed Licensing

4.2 Incident Management

The Company operates the following process:

4.2.1 Provision a Service Desk for the reporting of support incidents within contracted hours and via telephone, email, web portal, and mobile app.

4.2.2 Service Desk is targeted by KPI to answer the telephone within 30 seconds.

4.2.3 Service Desk record details of all incidents logged and mutually agree the priority of each incident (see table under 'Escalation' section of this procedure) in accordance with the Support Contract Specification

4.2.4 Service Desk allocates a unique incident reference to each incident verbally and issues an incident acknowledgement summarising the incident and references (by email).

4.2.5 Service Desk perform incident diagnosis and instigate appropriate actions and response in accordance with the Service Contract.

4.2.6 Service Desk escalates the incident as required.

4.2.7 Service Desk arranges for on-site or 3rd party response and actions as required.

4.2.8 Service Desk initiates and completes appropriate resolution.

4.2.9 Service Desk obtains mutual agreement of resolution and incident closure.

4.2.10 Service Desk analyses incident history and makes recommendations to negate repeat or related incidents (Problem Management).

Where a request falls outside the scope of the Service, the Company may provide engineering services at an additional charge. In such cases, the Company will work on a 'Best Endeavours' basis on the Customers behalf and accepts no liability related thereto.

4.3 Incident Priority and Escalation

When an incident is logged, it is classified based on priority (P1 to P5 – see below), which is mutually agreed with the Customer.

Based on this priority, the incident is escalated according to the following targets from the time the incident is raised:

Priority	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
P5	N/A	N/A	N/A	N/A	N/A

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
Unused currently	P5	

The escalation levels 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 Vendor

Escalation to Vendor is determined based on the nature of the incident.

3rd party management where applicable follows the above path, however once escalated to the 3rd party we are bound by their SLA's.

Each Customer has defined SLAs, which dictate response times. If a SLA is approaching breach this is escalated to P1. Escalation is performed by email and telephone for Priority Level 3.

Hardware Break-Fix is typically either 4+4 or 8+8 (Response + Targeted Fix).

4.4 Change Management

Change Management is a service permitting the Customer access to the Company resource(s) to effect changes (scheduled or emergency) to the Service. The use of this is limited to a pre-determined volume of Change Management Requests/Incidents within a Service Contract period and can be used for requests such as the configurations and set-up of new or additional system accounts, changes to permissions, settings or configurations and/or increases/decreases to parameters such as storage volumes.

The Company and the Customer jointly agree on the assignment of a Change Category, which determines the response level to each requested Change Request/ Incident as follows:

Emergency Change Request		
The Company will notify the Customer of the acceptance or rejection of the request	If the request is accepted, the Company will aim to inform the Customer of the timeline for completion of the request	Objective to schedule the completion of the request
2 Working Hours	2 Working Hours	8 Working Hours

Scheduled Change Request		
The Company will notify the Customer of the acceptance or rejection of the request	If the request is accepted, the Company will aim to inform the Customer of the timeline for completion of the request	Objective to schedule the completion of the request
16 Working Hours	24 Working hours	72 Working hours

Each Change Management Request/Incident is analysed by the Company within 2 Working Hours of receipt and an estimated time to complete notified to the Customer. For the purposes of Company Service Contract pricing, each Customer is allocated a maximum number of Change Management Requests/Incidents, which equate to a maximum time per annum equivalent to 15 minutes per Change Management Request/Incident. The Company will maintain a record of Change Management Requests/Incidents.

It is essential that Change Management Incidents emanate from pre-approved Customer personnel. The following responsibilities for Change Management are defined:

The Company will:

4.4.1 Provide and maintain a Change Management Log.

4.4.2 Verify the Change Request is from an Authorised representative of the Customer.

4.4.3 Control and document all changes to minimise any interruption to the Service.

4.4.4 With each proposed change:

(a) Agree/Reject the change.

(b) Coordinate Company resources for each agreed change.

(c) Prioritise changes per agreed change category.

(d) Contribute to impact or risk analysis where necessary.

4.4.5 Notify an Authorised Representative of the completion of a Change Request.

4.4.6 Obtain the agreement of a Customer Authorised Representative that a Change Request Incident can be closed.

4.4.7 Reserve the right to recover costs associated with Change Request Incident failure caused by the Customer.

4.4.8 Ensure only authorised representatives submit Change Requests to the Company.

4.4.9 Submit a documented Change Request (to a pre-approved documentary format) describing at a reasonable level the detail of the change, the rationale for the change and the impact the change may have on the Service.

4.4.10 Contribute to impact or risk analysis where necessary.

4.4.11 Be responsible for any Customer third-party service provider requirements.

4.4.12 Not make changes without first obtaining the Company approval. Any scheduled or planned changes must be detailed in writing to Service Desk prior to commencement.

4.4.13 Reimburse the Company for any costs incurred arising from a change failure caused by the Customer.

4.5 Data Management

The Company commits to manage Customer data within a secure and legal manner observing all applicable UK legislation and in accordance with instruction from appropriate UK Authorities and expects the Customer to similarly comply.

The Company recognises that Customer data may contain private and commercially sensitive information and that the Customer owns rights to their data. In the normal operation of the Service, the Company will not read, copy or access Customer data other than by electronic methods for the purposes of security scanning or Customer request.

The Company bears no responsibility to meet its obligations caused by the deficiencies in the quality, integrity, accuracy, or existence of Customer data.

The Company undertakes that any storage device or component thereof containing customer data will not be released in readable or operable form to third parties without the written permission of the Customer. This excludes damaged or defective equipment and/or storage devices replaced by manufacturer warranty in the case of equipment failure.

For the purposes of the Data Protection legislation the Customer is the 'Data Controller'. The Company is the 'Data Processor' in so far as storage of data but does not read, amend or delete data unless so instructed by the Customer. The Company confirms that all Customer data held within Cloud Services resides entirely within UK-only datacentres.

Multi-Factor-Authentication (MFA) is not provided as standard; however, this can be provided by hard token and/or mobile phone if required. Any MFA requirement must be detailed within the Company Service Contract.

Data Encryption is not provided as standard; however, on some Services but not all backup data is encrypted to AES256 FIPS140-2 in transit and at-rest.

The Company operates Service within the ISO9001 Quality framework and controls data under the ISO27001 Information Security Standard.

In the event of termination of a Services Contract, all Customer data stored by the Company will be made available to the Customer by a mutually agreed time and method to transfer the data to

Customer-provisioned storage devices. The Company reserves the right to charge for a more complex mutually agreed arrangement.

4.6 Personnel

The Company operates the Service within defined operational and quality parameters, including staffing and personnel. Qualified Technical Engineers and Technical Managers are assigned specific operational responsibilities and report to the Board of Directors. The aim is always to provide a world-class service, observing IT best practice and all applicable legislation to meet or exceed customer expectation.

A single point of contact is available to all Service Contract Customers; the Account Manager will conduct regular Service Review Meetings with the Customer to assess and monitor Service performance.

The Customer must notify and obtain written agreement and consent from the Company before changing, removing or deploying any technology solutions that may affect the Service. This applies to Customer staff and third parties operating on behalf of the Customer and is especially relevant when considering System access and security.

4.7 Service-Specific SLAs

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

Private Cloud

The Company maintains data backups of servers according to Customer requirement. As standard, data is backed up once a day with an additional replica of this data copied to a geographically separate location. The Recovery Point Objective (RPO) is <=24 hours as standard although this can be reduced based on customer requirements. Recovery Time Objective (RTO) is specific to each Customer's Service Contract requirements with varying options commercially available.

The Company uses all reasonable endeavours to make sure the backup process is effective and successful; however, the Customer must recognise that the Company is not liable for any direct, indirect or consequential loss which may occur. The Company cannot be responsible for the backup of any open files, or extraneous data on Customer site, or data resident on the local drive of a home/remote worker or an unrecognised device.

The Service Contract can provide one inclusive test data restoration incident per month if the Managed Backup Service is subscribed to. Additional test incidents will be deducted from Change Management or incur charges at the Company's commercial rates prevailing at the time.

The Customer acknowledges that they are responsible for the selection and volume of data backed up and maintained within the Service. The Company reserves the right to charge for any and all data stored at the pro-rata rate in accordance with the Service Contract.

Cloud backup

Cloud backup provides an automated mechanism whereby the Customer will be able to backup and recover data from designated devices as defined in the Service Description.

This is a managed service, and although the Company will be responsible for the availability of the Service components, the day-to-day operation of the Service will, in part, depend on certain key processes and related equipment, which are wholly under the Customer's control as is the data designated for backup, which may change periodically.

The Customer will be responsible for providing the necessary power, network connection, and environment to support the Service as defined in the Service Description and/or relevant Project document. The Customer must acknowledge 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 Company will not be responsible for any incident/loss resulting from 3rd party communications failures.

The Customer will be responsible for providing authorised and free access to a Company Engineer to deliver the product and services to the Customer site on a pre-arranged installation date(s).

The Customer will make available a designated and appropriately qualified representative to work with the Company Engineer during the installation of the product and services, and this person will confirm the data to be backed-up as part of the Commencement.

The Company Engineer will deliver the specified products and services to the Customer site on a pre-arranged installation date(s) as specified in the Service Contract referenced 'Commencement Charges'.

All defined products and services will be installed, commissioned, and tested to ensure that the equipment is fully operational. The Company Engineer will demonstrate the Service to the designated Customer representative on the Service, proving it is capable of backing up and recovering data.

At this time, the Company Engineer will hand over the Service to the Customer as live and operational. The Company Engineer will present the designated authorised Customer representative with a Sign-Off document to approve the installation. The designated Customer representative will confirm that the backup functionality of the service has been demonstrated to his/her satisfaction and sign-off the Commencement.

IMPORTANT: The Customer is solely responsible for storing their backup encryption keys in a secure location. Loss of the encryption keys by the Customer will prevent recovery of the Service and the Customer's backup data.

Data Backup and Restoration

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

The Company cannot guarantee to successfully back up all open files. The Company reports the open files that fail to backup to the Customer, however, the Customer will be responsible for reviewing such occurrences and modifying their backup sets as appropriate.

For confidentiality and security reasons, transmitted data is never opened or read by the Company. It, therefore, remains the Customer's responsibility to ensure that data integrity, including virus scanning is maintained. The Customer will be responsible for performing all data restoration operations unless defined otherwise within the Service Contract.

The Customer acknowledges that they are responsible for the selection and volume of data backed up and maintained within the Service. The Company reserves the right to charge for any and all data stored at the pro-rata rate in accordance with the Service Contract.

Reports

The Customer will be responsible for reviewing and acting upon the reports provided by the Company.

Service and Maintenance

The Customer will accept installation of all products and Service releases and engineering changes (hardware, software, or firmware) deemed necessary by the Company to maintain and/or upgrade the Service.

The Customer must notify and obtain written agreement and consent from the Company before changing, removing, or deploying any technology solutions that may affect the Service. This applies

to Customer staff and third parties acting on behalf of the Customer is especially relevant when considering System access and security.

Disaster Recovery (DR)

Unless the Customer has subscribed to a Service in the event of the Customer invoking or experiencing a Disaster Recovery incident (actual or test), this SLA will be suspended for the duration of the Disaster Recovery incident. During this time, the following plan will apply:

Disaster Recovery	Typical Event:
Classification: Customer invokes a Disaster Recovery Plan.	▪ Loss of or disruption to critical Systems ▪ Major data loss ▪ Loss of Customer site ▪ Scheduled Disaster Recovery Test (Pre-advised by Customer to the Company at least 30 days prior to test)
Call Logging: within Service Times	Call referred immediately to Company Service Desk Manager who becomes the primary point of contact to coordinate the following actions:
Time to Fix: - Incident diagnosis will start immediately, and a recovery plan will be proposed to the Customer depending on the exact nature, location, and scale of the incident. Incident resolution activity will be maintained on a 24-hour basis until the incident is resolved.	▪ Notify all relevant members of the Company Senior Management Team ▪ Review previous incident history ▪ Gather diagnostics ▪ Propose repair/replacement/response ▪ Arrange technical personnel, if applicable ▪ Provide status updates to the Customer ▪ Contact the Customer to confirm successful resolution ▪ Provide the Customer with DR Incident Report

PLEASE NOTE: It is highly recommended that the Customer has a Business Continuity and/or Disaster Recovery 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. Such charges are usually recoverable via Customer insurance, but the Company can make no guarantees to this and reserves the right to levy charges for all Disaster Recovery actions.

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 or Planned Maintenance.

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

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 Customer's total Monthly Recurring Charge as defined in the Service Contract. 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 Customer's account and will be reported at Service Review Meetings.

THE RIGHT TO RECEIVE SERVICE CREDITS AS DESCRIBED IN THIS SERVICE LEVEL AGREEMENT IS THE CUSTOMER'S ONLY REMEDY FOR ANY FAILURE BY THE COMPANY TO MEET THE PROMISES, GUARANTEES, AND WARRANTIES PROVIDED IN THE AGREEMENT.

Exclusions to Service Credits

Connectivity and 3rd Party managed 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 Company has little or no direct control.

Service Credits are also not calculated to include:

- Scheduled or Planned Maintenance
- Other Maintenance performed by the Customer or the Customer's agents.
- Specific actions by the Customer or the Customer's agents on the Customer's Software applications.

Any of the following circumstances will invalidate any Service Credit:

- Late or overdue payment of the Company Account by Customer.
- Violation of the Acceptable Use Policy.
- Unavailability or interruptions due to Customer error or Customer's agent error.
- Design, program or other defects in the Customer's software applications.
- Failure to report an incident to the Company by agreed means.
- Acts beyond the Company's reasonable control, including but not limited to natural disasters, changes resulting from government, political or other regulatory actions, strikes or labour disputes, acts of civil disobedience, acts of war, acts against parties (including carriers and other vendors to the Company), and any other actions beyond the Company control.
- The Customer's lack of availability to respond to incidents that require Customer participation for resolution.