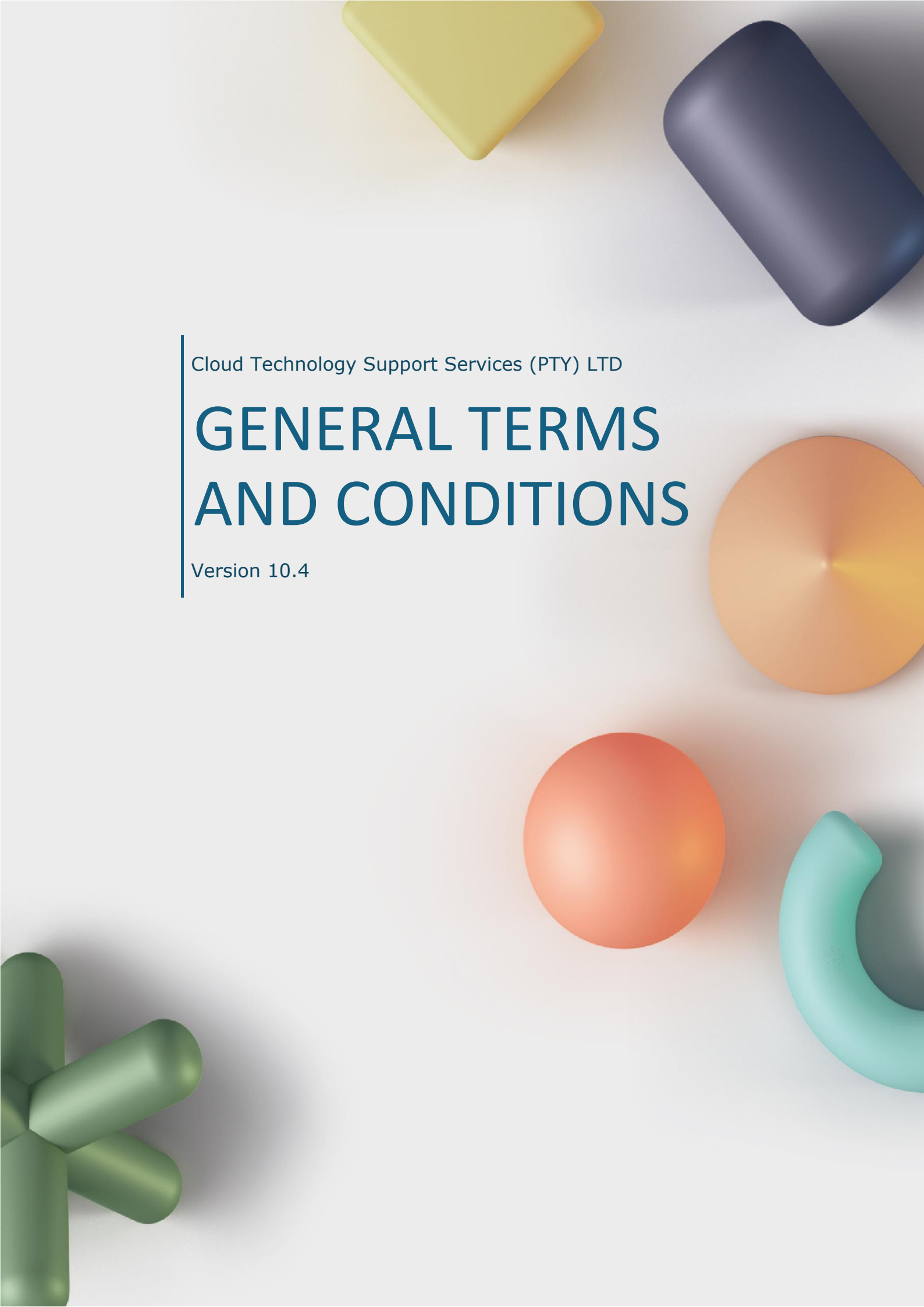
Cloud Technology Support Services (PTY) LTD

GENERAL TERMS AND CONDITIONS

Version 10.4



Contents

MASTER TERMS

1. Introduction and Structure

1.1 These General Terms and Conditions ("Terms") govern the provision of services and supply of goods by Cloud Technology Support Services (Pty) Ltd ("CTSS") to the Client.

1.2 These Terms apply together with any signed Services Agreement Schedule and the applicable Schedules incorporated by reference, as well as any Quote or Product-Specific Terms expressly incorporated into a Services Agreement Schedule (collectively, the "Agreement").

1.3 The Agreement consists of:

- These Master Terms;
- Schedule A – Managed Services (MSP);
- Schedule B – Managed Security Services (MSSP);
- Schedule C – Cloud Subscription Services;
- Schedule D – Responsibility Matrix;
- Schedule E – RMM Baseline Services; and
- Schedule F - Commercial Model and Pre-Purchased Hours.

1.4 If a client-specific Schedule or Responsibility Matrix is attached to a signed Services Agreement Schedule, that Client-specific document prevails for that Services Agreement Schedule only.

1.5 These Terms supersede all prior versions of CTSS General Terms and Conditions from the Effective Date.

2. Definitions

For purposes of this Agreement:

2.1 "Agreement" means these Terms together with all applicable Services Agreement Schedules and incorporated documents.

2.2 "Business Day" means any day other than a Saturday, Sunday or official public holiday in the Republic of South Africa.

2.3 "Business Hours" means 08:30 to 17:00 on Business Days.

2.4 "Client" means the legal entity accepting a Services Agreement Schedule or otherwise engaging CTSS to provide Services.

2.5 "Commitment Period" means a fixed service or licence term defined in a Services Agreement Schedule or imposed by a third-party provider, including under subscription licensing frameworks such as, but not limited to Microsoft's New Commerce Experience.

2.6 "Cloud Services" means third-party subscription or platform services supplied, resold, administered or supported by CTSS, including but not limited to Microsoft 365 and Microsoft Azure.

2.7 "Fees" means all amounts payable by the Client under this Agreement, including recurring charges, licence fees, project fees, time-and-materials charges and applicable taxes.

2.8 “Goods” means hardware, software or equipment supplied by CTSS.

2.9 “MSSP Services” means managed security monitoring, alert triage, containment and related services expressly defined in a signed MSSP Services Agreement Schedule.

2.10 “MSP Services” means managed IT support, monitoring, administration and related services expressly defined in a signed MSP Services Agreement Schedule.

2.11 “RMM Baseline Services” means the discretionary remote monitoring, automated patch management, endpoint telemetry monitoring and related baseline configuration services described in Schedule E.

2.12 “Services” means MSP Services, MSSP Services, Cloud Services, RMM Baseline Services and any other services provided under a signed Services Agreement Schedule.

2.13 “SLA” means a service level commitment expressly defined in a signed and current Services Agreement Schedule or in a Schedule incorporated therein.

2.14 “Services Agreement Schedule” means a written or digitally accepted document setting out the scope, Fees and applicable service terms agreed between CTSS and the Client.

3. Agreement Formation

3.1 Services and Goods are supplied pursuant to a signed or digitally accepted Services Agreement Schedule.

3.2 A digital signature or electronic acceptance via Halo PSA or any other approved electronic system constitutes valid and binding acceptance.

3.3 Each accepted Services Agreement Schedule incorporates these Terms and the applicable Schedules referenced therein.

3.4 The Agreement becomes legally binding upon the earliest of:

a) Written acceptance of a Services Agreement Schedule;
b) Digital or electronic acceptance, including acceptance via Halo PSA or any other approved electronic system;
c) Payment of any invoice issued by CTSS;
d) The Client requesting or instructing CTSS to commence Services in writing; or
e) Acceptance by conduct, including continued use of Services following written notice of these Terms or any update thereto.

3.5 Acceptance in any of the above forms constitutes full and binding agreement to these Terms and any incorporated Services Agreement Schedule.

3.6 Services apply only where expressly selected or described in a signed Services Agreement Schedule. No Schedule to these Terms creates an obligation on CTSS to provide Services unless incorporated through a signed Services Agreement Schedule.

4. Entire Agreement and Order of Precedence

4.1 The documents forming part of the Agreement constitute the entire agreement between the parties and supersede all prior discussions, proposals, representations or agreements relating to the subject matter.

4.2 In the event of any inconsistency between documents forming part of the Agreement, the following order of precedence applies:

The signed Services Agreement Schedule;

- Any signed Scope of Work or Secure Service document expressly incorporated into the Services Agreement Schedule;
- Any applicable Product-Specific Terms;
- The applicable Schedule referenced in the Services Agreement Schedule (including Schedules A–F);
- These Master Terms;
- Any Quote or proposal;
- Marketing materials or website content.

4.3 To the extent of any inconsistency, the higher-ranking document prevails.

4.4 No representation, statement or assurance not expressly recorded in the Agreement is binding.

4.5 No representation, statement, assurance or description of Services made in proposals, presentations, marketing materials, email correspondence, meetings or other communications shall expand the scope of Services or create any obligation beyond those expressly recorded in a signed Services Agreement Schedule. No employee, contractor or representative of CTSS has authority to vary or extend the scope of Services except through a written amendment signed by authorised representatives of both parties.

4.6 Scope of Work and Secure Service Documents

4.6.1 Standalone Scope of Work documents, including but not limited to Baseline Secure, Endpoint Secure, Hardened Secure, Server Secure, Compliance Secure and Complete Secure documents, apply only where expressly incorporated into a signed Services Agreement Schedule.

4.6.2 Such documents define technical implementation scope only and do not create independent SLA commitments, monitoring obligations, compliance guarantees or ongoing service entitlements unless expressly stated in the signed Services Agreement Schedule.

4.6.3 In the event of any inconsistency between a Scope of Services document and a Service Schedule (including Schedule A or Schedule B), the signed Services Agreement Schedule prevails.

4.6.4 No Scope of Services document shall expand the scope of Services beyond what is expressly contracted in the applicable Services Agreement Schedule.

4.7 Ongoing Secure Frameworks

4.7.1 Where a Secure Service document is incorporated into a signed Services Agreement Schedule as an ongoing control framework, such document defines a structured set of technical and administrative controls designed to reduce risk and align with recognised security practices.

4.7.2 Secure Service documents do not constitute certification, regulatory assurance, legal compliance confirmation, audit attestation or guarantee of conformity with any specific statutory, regulatory or industry framework unless expressly stated in a separate written agreement.

4.7.3 Implementation of controls under a Secure Service document reduces risk but does not eliminate risk and does not guarantee prevention of compromise, breach, loss, regulatory exposure or business interruption.

4.7.4 Periodic reviews, updates or enhancements to Secure Service documents may be made by CTSS to reflect evolving threat landscapes, platform capabilities, regulatory developments or industry best practice. Such updates shall not materially reduce the control objectives without notice.

4.7.5 Decisions regarding regulatory compliance, risk acceptance or certification remain the responsibility of the Client unless expressly transferred under a separate written agreement.

---

5. Fees and Invoicing

5.1 Fees are payable in accordance with the applicable Services Agreement Schedule or invoice.

5.2 Invoices are due on the date stated on the invoice ("Due Date").

5.3 Unless otherwise agreed in writing, all Fees are exclusive of VAT and any other applicable taxes.

5.4 The Client may not withhold, deduct or set off any amounts due to CTSS except where required by law.

5.5 CTSS may suspend Services in accordance with Section 6 if payment is not received by the Due Date.

---

6. Non-Payment and Service Continuity

6.1 If any invoice remains unpaid after the Due Date, CTSS will issue a payment reminder to the Client's nominated billing contact.

6.2 If payment remains outstanding, CTSS may implement the following staged service adjustments:

- From Day 1 after the Due Date, SLA response commitments may be suspended, and Services may be delivered on a best-effort basis until the account is brought current.

- From Day 7 after the Due Date, operational MSP, MSSP and RMM Baseline Services activities, including monitoring, patching, automation, change implementation and response services, may be suspended.
- From Day 14 after the Due Date, Cloud licences or subscriptions may be suspended or removed in accordance with Schedule C and the applicable provider's policies.
- From Day 30 after the Due Date, CTSS may terminate the affected Services or this Agreement, in whole or in part, upon written notice.

6.3 These measures are intended to ensure commercial fairness and service sustainability and do not constitute a penalty.

---

7. Reinstatement Following Suspension

7.1 Reinstatement of suspended Services is subject to:

- Settlement of all outstanding amounts; and
- Payment of a reasonable administrative re-enablement fee equal to ten percent (10%) of the overdue amount, subject to a minimum of R1,000.

7.2 The re-enablement fee represents an administrative charge associated with suspension and restoration of Services and is not a penalty.

7.3 CTSS may delay reinstatement until funds have cleared.

---

8. Commitment Period and Acceleration

8.1 Where Services or licences are subject to a Commitment Period, the Client remains responsible for Fees for the full duration of that Commitment Period.

8.2 If Services subject to a Commitment Period are terminated due to:

- Non payment;
- Material breach; or
- Early termination by the Client,

the Client remains liable for all Fees payable for the remainder of the applicable Commitment Period, and such Fees may be invoiced by CTSS upon termination.

8.3 Commitment obligations survive termination of the Agreement.

---

9. Cloud Licence Dependency

9.1 Cloud Services are subscription-dependent and are provided subject to active and fully paid licences.

9.2 Continued access to Cloud Services, data and related functionality depends on maintaining active subscriptions in good standing.

9.3 Suspension, expiry, cancellation or removal of licences may result in:

- Loss of access to services;
- Deactivation of accounts; and
- Permanent deletion of data in accordance with the applicable provider's retention policies.

9.4 CTSS does not control the infrastructure, retention timelines or deletion processes of third-party Cloud providers.

9.5 CTSS is not obliged to maintain licences or subscriptions at its own cost pending payment.

10. Suspension and Data Retention

10.1 Where licences are suspended or removed due to non-payment or termination, the Client acknowledges that access to services and data may be restricted.

10.2 Data retention and deletion following licence suspension or termination are governed by the applicable provider's policies.

10.3 CTSS does not have the ability to prevent data deletion once a provider's retention or deletion process has commenced.

10.4 Suspension or removal of licences in accordance with this Agreement does not transfer ownership of the Client's data, which remains the property of the Client.

10.5 The Client remains responsible for implementing appropriate backup and data preservation measures unless a separate Backup-as-a-Service Services Agreement Schedule has been entered into.

11. Commencement and Term

11.1 Services commence on the date specified in the applicable Services Agreement Schedule.

11.2 Unless subject to a Commitment Period, Services continue on a month-to-month basis and may be terminated on not less than one (1) full calendar month's written notice, such notice to expire at the end of a calendar month.

11.3 Services subject to a Commitment Period continue for the full duration specified in the Services Agreement Schedule or imposed by the provider.

12. Termination for Breach

12.1 Except for non-payment governed by Section 6, either party may terminate this Agreement for material breach not remedied within thirty (30) days after written notice.

12.2 Termination does not affect any rights or obligations accrued prior to termination.

13. Termination Following Extended Suspension

13.1 Where suspension for non-payment continues for more than thirty (30) consecutive days, CTSS may terminate the affected Services or this Agreement upon written notice.

13.2 Termination under this clause does not limit CTSS's right to recover:

- All outstanding Fees; and
- Any remaining Fees due under an applicable Commitment Period.

14. Transition Assistance

14.1 Upon termination, CTSS may provide reasonable transition assistance at the Client's written request.

14.2 Transition assistance:

- Is billable at prevailing rates unless otherwise agreed;
- Is subject to all outstanding amounts being settled; and
- Is limited to thirty (30) days from termination unless otherwise agreed in writing.

14.3 Transition assistance does not include project-managed migrations, forensic investigation or remediation services unless expressly agreed.

14.4 Nothing in this Agreement entitles CTSS to unlawfully withhold the Client's property or lawful tenant ownership rights.

---

15. Post-Termination Position

15.1 Following completion of transition assistance, CTSS has no ongoing obligation to retain Client data, administrative access, backups or documentation unless legally required.

15.2 CTSS may securely delete residual data in accordance with its internal retention policies.

15.3 Following termination and handover, CTSS has no responsibility for the ongoing availability, integrity, security or compliance of the Client's systems or services.

---

16. Service Delivery Principles

16.1 Services are delivered during Business Hours unless otherwise defined in a Services Agreement Schedule.

16.2 After-hours services are provided only where included in a Services Agreement Schedule or requested by the Client and accepted by CTSS.

16.3 The Client shall provide reasonable access, authority and cooperation necessary for CTSS to deliver the Services.

16.4 Service delivery may be affected by third-party provider performance, platform constraints, Client responsiveness or widespread incident conditions.

16.5 Where CTSS requires delegated administrative access or Passwordless Multi-Factor Authentication access to deliver Services, the Client shall not revoke, restrict, or materially limit such access during the term of an active Services Agreement Schedule without prior written notice.

16.6 Revocation or restriction of required administrative access may result in suspension of SLA commitments and shall not constitute breach by CTSS where such access limitation prevents delivery of contracted Services.

16.7 Where access is removed or restricted by the Client, CTSS shall not be liable for service degradation, security gaps, delayed response or compliance impact arising from

such restriction.

17. SLA Applicability

17.1 No response times, service levels, monitoring obligations or remediation commitments apply unless expressly defined in a signed and current Services Agreement Schedule.

17.2 Draft proposals, expired agreements or informal communications do not create ongoing SLA entitlements.

17.3 Where no active SLA is in force, Services are delivered on a best-effort basis.

17.4 Clients with an active SLA are prioritised in accordance with the applicable Service Schedule.

17.5 Where MSSP Services are suspended in accordance with Clause 25.5 due to failure to meet minimum security baseline requirements, any applicable SLA commitments relating to such MSSP Services shall be suspended for the duration of the suspension period. No SLA credits, response-time guarantees or service-level remedies shall accrue during such period.

17.6 Nature of SLA Commitments

17.6.1 SLA response targets relate solely to the time within which CTSS will acknowledge and commence triage of an incident.

17.6.2 SLA response targets do not constitute guarantees of resolution within any specific timeframe.

17.6.3 Resolution time depends on complexity, third-party provider performance, Client responsiveness, access availability, severity of impact and external conditions.

17.7 SLA Timer Suspension

17.7.1 SLA response or remediation timers are suspended during any period in which:

- Required Client access, approval or information is not available;
- Third-party provider outages or platform limitations prevent action;
- The Client has restricted or revoked necessary administrative access;
- A Force Majeure event applies; or
- A security suspension under Clause 22A is in effect.

17.7.2 SLA timers resume once the blocking condition has been resolved.

17.8 SLA Remedies

17.8.1 Except where expressly defined in a signed Services Agreement Schedule, no financial credits, penalties or automatic fee reductions apply for alleged SLA breaches.

17.8.2 SLA commitments are service-level objectives only and are subject to the aggregate limitation of liability in Section 26.

18. Incident Classification and Prioritisation

18.1 All service requests, alerts and events are subject to triage and severity classification by CTSS.

18.2 Classification is determined acting reasonably based on operational impact, including business disruption, number of users affected, security impact and service availability.

18.3 Where multiple high-priority incidents exist, CTSS will allocate resources based on overall operational impact across its client base.

18.4 The receipt of an alert or notification from a third-party platform does not in itself constitute a security incident.

18.5 Investigation, containment or remediation obligations arise only where expressly included in a contracted MSSP Services Agreement Schedule.

---

19. After-Hours Services and Billing

19.1 After-hours periods include any time outside Business Hours and all South African public holidays.

19.2 After-hours services are billed at:

- 1.5 times the prevailing hourly rate for work performed Monday to Friday outside Business Hours;
- 2 times the prevailing hourly rate for work performed on Saturdays, Sundays or public holidays.

19.3 A minimum billing period of one (1) hour applies to after-hours engagements, with billing in thirty (30) minute increments thereafter.

19.4 Where a Client has Pre-Purchased Hours allocated under Schedule F, after-hours time will be deducted from the applicable Service category allocation at the uplifted rate.

19.5 CTSS may require prepayment for after-hours work where an account is not in good standing.

---

20. Provider Outage and SLA Suspension

20.1 SLA response and resolution timers are suspended during any period in which a third-party provider experiences an outage or service degradation that prevents CTSS from performing its obligations.

20.2 SLA timers resume once sufficient platform functionality is restored to enable CTSS to act.

20.3 CTSS does not provide independent uptime guarantees for third-party Cloud platforms unless expressly agreed in writing.

---

21. Change Management

21.1 Routine operational changes may be requested and approved through written electronic communication, including email or the ticketing system, where such changes do not materially affect architecture, licensing obligations, security posture, availability or cost.

21.2 Changes that materially affect security posture, architecture, licensing commitments, billing structure or service scope require a formal Change Request (“CR”).

21.3 A CR will set out the scope, estimated effort, impact, prerequisites and scheduling requirements. No work will commence until the CR is approved in writing by the Client.

21.4 Time spent on approved changes is billable in accordance with the applicable Services Agreement Schedule or prevailing rates unless expressly included within a contracted service.

---

22. Emergency Protective Measures

22.1 Where CTSS reasonably believes, acting in good faith, that immediate action is required to prevent, contain or limit a security incident, operational outage, regulatory exposure or material risk to the Client, CTSS infrastructure, shared security tooling, or other clients, CTSS may implement temporary protective measures without prior approval.

22.2 Protective measures may include temporary account restrictions, enforcement of security controls, access limitation, session revocation, configuration changes, or isolation of affected systems, strictly to the extent reasonably necessary to contain or reduce the identified risk.

22.3 Any emergency action taken under this clause shall be proportionate, limited in scope and duration, and directed solely at mitigating the immediate threat condition.

22.4 CTSS will notify the Client as soon as reasonably practicable after implementation of emergency measures and will provide a summary of the reason for the action taken.

22.5 Emergency containment measures do not constitute full remediation unless expressly included in a signed Services Agreement Schedule. Subsequent investigation, remediation, recovery, restoration, rebuild, regulatory assistance, or extended incident response services are billable unless expressly included within a contracted MSSP service.

22.6 Nothing in this clause obliges CTSS to provide forensic investigation, regulatory reporting assistance, system rebuild, data restoration, or extended remediation services unless expressly included in a signed Services Agreement Schedule.

22A. Security Risk Suspension

22A.1 Where CTSS reasonably determines, acting in good faith, that the Client's configuration, refusal to implement critical security controls, unmanaged vulnerability, or sustained non-compliance with agreed minimum security requirements creates a material risk that:

- materially threatens CTSS infrastructure, shared security tooling, or other clients; or
- would likely result in unlawful processing, regulatory breach, or statutory non-compliance if Services continued,

CTSS may issue a written notice describing the identified risk and the remediation steps required.

22A.2 If the material risk is not addressed within the specified reasonable remediation period stated in the notice, CTSS may suspend only those affected Services strictly to the extent necessary to protect its infrastructure, tooling, compliance position, or other clients.

22A.3 Any suspension under this clause shall be proportionate, limited in scope, and applied only for so long as the material risk persists.

22A.4 Suspension under this clause does not relieve the Client of its obligation to pay Fees during the suspension period, provided that such Fees relate to Services that remain contractually committed or reserved.

22A.5 Services will be restored promptly once the material risk has been adequately remediated and CTSS has reasonably verified such remediation.

22A.6 This clause does not apply where the material risk arises solely from a breach of this Agreement by CTSS.

---

23. General Client Responsibilities

23.1 The Client retains ownership of its data and remains responsible for governance, regulatory compliance and business continuity obligations.

23.2 The Client is responsible for user access decisions, credential management and internal approval processes unless expressly delegated under a signed Services Agreement Schedule.

23.3 Where CTSS identifies operational or security risks, such risks may be documented and communicated to the Client.

23.4 Decisions relating to risk acceptance, implementation of recommendations or deferral of corrective action remain the responsibility of the Client.

23.5 The Client acknowledges that cyber security and managed security services reduce risk but do not eliminate risk and do not constitute insurance. CTSS does not provide insurance coverage or financial indemnification against loss arising from cyber incidents, data breaches or operational disruption. The Client is responsible for determining whether to obtain and maintain appropriate cyber insurance or other risk transfer mechanisms. The absence of such insurance does not expand the liability of CTSS under this Agreement.

---

24. Backup and Data Responsibility

24.1 Platform redundancy, high availability or built-in retention features do not constitute backup.

24.2 Backup services are provided only where expressly defined in a signed Services Agreement Schedule.

24.3 Even where backup services are contracted, the Client remains responsible for determining the adequacy of backup scope, retention periods and restore testing frequency in line with legal and business requirements.

24.4 Where no Backup-as-a-Service Services Agreement Schedule exists, CTSS has no responsibility for data loss, corruption, deletion or retention expiry.

24.5 Unless expressly contracted under a separate Services Agreement Schedule, CTSS does not act as custodian, escrow agent, trustee or preservation agent of the Client’s

data. The Client remains responsible for determining and implementing appropriate data preservation, legal hold and retention measures.

25. Minimum Security Baseline

25.1 To enable CTSS to deliver Managed or Security Services responsibly and effectively, the following minimum-security controls represent the target baseline state for environments under an active MSSP or security engagement:

- Multi-Factor Authentication enforced for all users;
- Passwordless Multi-Factor Authentication enforced for privileged or administrative roles;
- At least two secure emergency access accounts;
- Conditional Access baseline policies appropriate to the platform;
- Unique administrative identities with role-based access; and
- Security logging enabled in accordance with platform capabilities.

25.2 Where the Client environment does not meet the minimum baseline at commencement of Services, CTSS will identify material gaps and may document such gaps in a Risk Register or remediation plan. MSSP Services may commence in parallel with a structured uplift process.

25.3 During any agreed remediation period, the Client acknowledges that security exposure may be elevated until baseline controls are implemented. CTSS shall not be responsible for incidents directly attributable to the absence of identified baseline controls that remain unremediated.

25.4 Remediation, uplift or implementation work required to achieve the minimum baseline is not included within MSSP Services unless expressly defined in a signed Services Agreement Schedule and may be quoted separately or billed at prevailing rates.

25.5 Where, after written notice and a reasonable remediation period, the Client declines or fails to implement critical baseline controls that materially increase risk exposure, CTSS may suspend the affected MSSP Services and any associated SLA commitments strictly to the extent necessary until the required controls are implemented. Suspension under this clause does not relieve the Client of its obligation to pay applicable Fees during the suspension period. MSSP Services will resume once compliance with the minimum baseline is confirmed.

25.6 Security Services reduce risk but cannot eliminate risk. No control set guarantees the prevention of compromise.

26. Aggregate Limitation of Liability

26.1 CTSS's total aggregate liability arising out of or in connection with this Agreement, whether in contract, delict, including negligence, statute, misrepresentation or otherwise, shall not exceed the total Fees paid by the Client to CTSS in the twelve (12) months immediately preceding the date on which the claiming party became aware, or ought reasonably to have become aware, of the facts giving rise to the claim.

26.2 All claims arising from the same event, series of related events, or connected acts or omissions shall be treated as a single claim for purposes of applying the aggregate limitation set out in Clause 26.1.

26.3 Any claim arising out of or in connection with this Agreement, whether in:

a) Contract;
b) Delict;
c) Statute or otherwise;

must be instituted by service of summons or equivalent originating process in a court of competent jurisdiction within twelve (12) months from the date on which the claiming party became aware, or ought reasonably to have become aware, of the facts giving rise to the claim.

Failing such institution within the period stated above, the claim shall be permanently barred and unenforceable, notwithstanding any longer period of prescription that may otherwise apply under the Prescription Act 68 of 1969.

This clause constitutes a contractual limitation period agreed between the parties and operates independently of statutory prescription. The limitation period applies irrespective of termination, expiry or suspension of this Agreement.

This limitation period does not apply to claims arising from fraud or wilful misconduct.

26A. Application of Limitation to Security and Data Events

For the avoidance of doubt, the aggregate limitation of liability set out in Clause 26.1 applies to all claims arising out of or in connection with any security incident, cyber event, ransomware event, business email compromise, phishing-related incident, data breach, unauthorised access, system intrusion, malware infection, compromise of credentials, or interruption of access to systems or cloud services.

This includes any alleged failure to detect, monitor, prevent, investigate, escalate, respond to or contain a security threat or suspicious activity, and any claim relating to the provision or non-provision of MSSP Services, monitoring services, alert triage, containment measures, security configuration or related security services.

All such claims, whether framed in contract, delict including negligence or statute, misrepresentation or otherwise, remain subject to the aggregate limitation of liability set out in Clause 26.1.

---

27. Excluded Losses

27.1 To the maximum extent permitted by law, CTSS shall not be liable for any indirect, incidental, special or consequential loss, including loss of profit, revenue, business opportunity, goodwill, anticipated savings, productivity, operational capacity, business interruption, cost of substitute services, or data.

27.2 Any liability relating to data loss, security incident, service interruption or third-party platform failure remains subject to the aggregate limitation in Section 26.

27.3 To the maximum extent permitted by law, CTSS shall not be liable for any administrative fine, regulatory penalty, statutory sanction, enforcement action or similar

financial imposition imposed on the Client by any regulator, supervisory authority or governmental body, including under the Protection of Personal Information Act, 2013 or any successor legislation, irrespective of whether such fine, penalty or sanction arises from or relates to a security incident, data breach, service interruption or any alleged act or omission of CTSS. Nothing in this clause excludes liability for fraud or wilful misconduct to the extent such liability cannot lawfully be excluded.

28. Third-Party Dependencies

28.1 Many Services rely on third-party providers, platforms, telecommunications carriers and software vendors.

28.2 CTSS does not guarantee uninterrupted availability or performance of third-party services.

28.3 Failures, outages, degradation, platform retirements or policy changes by third-party providers do not constitute a breach by CTSS.

28.4 Where service credits are issued by a third-party provider, CTSS will reasonably assist in submitting claims and will pass through any credits received. Such credits constitute the Client's sole financial remedy for the applicable provider outage.

29. Contributory Responsibility

29.1 CTSS shall not be liable to the extent that any loss or damage arises from:

- The Client's failure to implement recommended controls or corrective actions;
- The Client's failure to maintain appropriate backup, retention or disaster recovery arrangements;
- Misuse, compromise or unauthorised disclosure of credentials under the Client's control;
- Delay in providing required access, approvals or information;
- Acts or omissions of third-party providers outside CTSS's reasonable control.

30. Indemnity

30.1 The Client indemnifies CTSS against third-party claims arising from:

- Unlawful use of software or services by the Client;
- Breach of third-party licence terms;
- Regulatory non-compliance attributable to the Client;
- Failure to maintain appropriate backups where not contracted through CTSS.

30.2 This indemnity excludes loss caused by CTSS's gross negligence and remains subject to the aggregate limitation in Section 26.

31. Non-Excludable Liability

31.1 Nothing in this Agreement excludes liability which cannot lawfully be excluded under South African law.

---

32. Confidentiality

32.1 Each party shall keep confidential any non-public information disclosed in connection with this Agreement and shall not disclose such information to third parties except:

- As required for the performance of the Services;
- With prior written consent; or
- Where required by law.

32.2 Confidentiality obligations survive termination of the Agreement.

32A. Data Protection and POPIA Alignment

32A.1 For purposes of the Protection of Personal Information Act, 2013 ("POPIA") and any other applicable data protection legislation, the Client acts as the Responsible Party and CTSS acts as an Operator to the extent that CTSS processes personal information on behalf of the Client in delivering the Services.

32A.2 CTSS shall process personal information only for the purpose of performing its obligations under this Agreement and in accordance with the Client's documented instructions as reflected in the Agreement and applicable Services Agreement Schedules.

32A.3 The Client remains responsible for ensuring that it has a lawful basis for processing personal information and for providing all required notifications to data subjects.

32A.4 CTSS shall implement reasonable technical and organisational safeguards appropriate to the nature of the Services to protect personal information against unauthorised access, loss or damage.

32A.5 Where CTSS becomes aware of a security compromise affecting personal information processed on behalf of the Client, CTSS shall notify the Client without undue delay and cooperate reasonably in providing information necessary for the Client to fulfil its statutory notification obligations.

32A.6 The Client acknowledges that certain Services involve the use of third-party cloud providers who may act as independent Responsible Parties or Operators under their own terms. CTSS is not responsible for the independent compliance obligations of such third parties.

32A.7 CTSS does not independently determine the purposes and means of processing personal information unless expressly agreed in writing.

32A.8 Nothing in this clause creates joint responsibility or joint controllership unless expressly agreed in writing.

32B. Public Statements and Attribution

The Client may make factual disclosures identifying CTSS as a service provider where required for regulatory notification, legal compliance or ordinary business

communication. The Client shall not attribute fault, negligence, breach or causation to CTSS in any public statement, media communication, regulatory submission or third-party communication without the prior written consent of CTSS, such consent not to be unreasonably withheld where attribution is factually and legally established. Nothing in this clause restricts disclosures required by law.

---

33. Intellectual Property

33.1 All intellectual property owned by CTSS prior to commencement of the Agreement remains the property of CTSS.

33.2 Any tools, scripts, automation frameworks, monitoring configurations, documentation templates, methodologies, reporting formats or operational processes developed or used by CTSS in providing the Services remain the property of CTSS unless expressly agreed otherwise in writing.

33.3 The Client retains ownership of its data, tenant environments and environment-specific configurations.

33.4 Nothing in this Agreement transfers ownership of CTSS's proprietary materials to the Client.

33.5 Upon termination, the Client is entitled to access its data and tenant environment, but not CTSS's proprietary tools or internal methodologies unless expressly agreed.

---

34. Non-Solicitation

34.1 During the term of the Agreement and for twelve (12) months following termination, the Client shall not directly solicit or employ any employee of CTSS who was materially involved in providing Services to the Client.

34.2 This restriction does not prevent employment resulting from a general public advertisement not specifically directed at CTSS personnel.

34.3 In the event of a breach of this clause, the Client shall pay liquidated damages equal to six (6) months' gross remuneration of the relevant employee, which the parties agree represents a reasonable pre-estimate of likely loss.

---

35. Variation

35.1 CTSS may update these Terms from time to time to reflect legal, regulatory, operational, security, commercial, or industry changes.

35.2 CTSS will provide not less than thirty (30) days' written notice of any material update to these Terms.

35.3 Updates apply prospectively from the effective date specified in the notice and do not apply retroactively to events occurring prior to that date.

35.4 No update to these Terms shall:

- Reduce or materially alter the scope of Services expressly defined in a signed Services Agreement Schedule;

- Reduce or materially alter agreed SLA response targets during an active Commitment Period; or
- Alter pricing or Commitment Period obligations already agreed in a signed Services Agreement Schedule for the duration of the applicable Commitment Period, unless expressly agreed in writing by authorised representatives of both parties with the exception of Cloud Subsription Services as per Schedule C4.

35.5 Continued use of Services after the effective date of updated Terms constitutes acceptance of the updated Terms.

35.6 No variation to a signed Services Agreement Schedule is effective unless agreed in writing.

---

36. Governing Law

36.1 This Agreement is governed by the laws of the Republic of South Africa.

---

37. Dispute Resolution

37.1 The parties shall first attempt to resolve disputes through good faith negotiation between senior representatives.

37.2 If unresolved within fourteen (14) days of written notice, the dispute may be referred to mediation in South Africa.

37.3 Nothing prevents either party from seeking urgent interim relief from a court of competent jurisdiction.

---

38. Jurisdiction

38.1 The parties consent to the jurisdiction of the Southern Gauteng High Court of South Africa.

---

39. Force Majeure

39.1 Neither party shall be liable for failure to perform obligations due to events beyond reasonable control.

---

40. Assignment and Cession

40.1 The Client may not assign its rights or obligations, nor cede its rights without written consent from CTSS.

40.2 CTSS may assign this Agreement as part of a restructuring, merger or sale.

40A. Subcontracting

40A.1 CTSS may subcontract or delegate the performance of any part of the Services to affiliates, specialist contractors, cloud providers, security tooling vendors, or other third-party service providers.

40A.2 CTSS remains responsible for the performance of subcontracted Services in accordance with this Agreement.

40A.3 The Client acknowledges that certain Services inherently involve the use of third-party infrastructure, platforms, hosting environments, monitoring systems, automation tools and security technologies.

40A.4 Nothing in this clause creates a partnership, joint venture, or agency relationship between the Client and any subcontractor of CTSS.

40A.5 Where subcontracting involves processing of personal information, such processing remains subject to Section 32A (Data Protection and POPIA Alignment)

40B. Audit and Access Limitation

40B.1 Nothing in this Agreement grants the Client any right to audit, inspect, access or test CTSS internal systems, infrastructure, security controls, tools, or facilities except where expressly required by applicable law.

40B.2 Any statutory audit right shall be:

Limited to information reasonably necessary to demonstrate compliance with this Agreement;

- Subject to confidentiality obligations;
- Conducted during normal business hours; and
- At the Client's cost unless otherwise required by law.

40B.3 The Client shall not conduct or commission penetration testing, vulnerability scanning, security testing, or performance testing against CTSS systems or shared infrastructure without prior written consent.

40B.4 This clause does not restrict the Client's access to its own tenant environments or data.

40C. Compliance with Laws and Anti-Corruption

40C.1 Each party warrants that it shall comply with all applicable laws and regulations in connection with this Agreement.

40C.2 The Client shall not use the Services for any unlawful purpose, including activities that violate applicable anti-corruption, anti-bribery, sanctions, export control, or data protection laws.

40C.3 CTSS may suspend or terminate Services immediately upon written notice if it reasonably believes that continued provision of Services would result in a breach of applicable law.

40C.4 The Client shall indemnify CTSS against losses arising from unlawful use of the Services by the Client or its users.

---

41. Severability and Waiver

41.1 If any provision is held unenforceable, the remainder remains in force.

41.2 Failure to enforce a right does not constitute waiver.

---

42. Survival

42.1 Clauses relating to payment, Commitment Period, limitation of liability, indemnity, confidentiality, intellectual property and dispute resolution survive termination.

SCHEDULE A: Managed Services (MSP)

A1. Scope of Managed Services

A1.1 MSP Services are limited strictly to the scope expressly defined in the signed Services Agreement Schedule.

A1.2 Service levels, response times and monitoring obligations apply only where expressly defined in a Services Agreement Schedule and are subject to the Master Terms.

A1.3 Services not expressly included in a Services Agreement Schedule are outside scope and billable at prevailing rates.

A2. Service Nature

A2.1 MSP Services are operational IT management and support services.

A2.2 MSP Services do not include continuous security monitoring, threat hunting, forensic investigation, breach containment or managed detection and response unless expressly included in a separate MSSP Services Agreement Schedule.

A3. Security Advisory Position

A3.1 Where a potential security issue is identified during delivery of MSP Services, CTSS may provide advisory guidance.

A3.2 Advisory guidance does not constitute a security monitoring or incident response obligation.

A4. Backup Services

A4.1 Backup services are provided only where expressly defined in a signed Services Agreement Schedule.

A4.2 Microsoft 365 retention policies, Azure retention features, endpoint restore points or similar platform features do not constitute backup.

A4.3 Where Backup-as-a-Service is contracted, restore requests are handled in accordance with the Services Agreement Schedule. Restore testing may be billable unless expressly included.

A5. Incident Response

A5.1 Security Incident Response is not included in MSP Services unless expressly defined in a Services Agreement Schedule.

A5.2 Where MSP time is available under the Services Agreement Schedule, CTSS may allocate time to preliminary investigation at its discretion.

A5.3 Extended remediation, forensic analysis, recovery or third-party coordination is billable unless included in a contracted MSSP Service.

A6. Client Responsibilities under MSP

A6.1 The Client remains responsible for:

- Risk acceptance decisions;
- Regulatory compliance;
- Business continuity planning;
- User access governance.

A6.2 Recommendations provided by CTSS form advisory guidance unless expressly included in contracted Services.

SCHEDULE B: Managed Security Services (MSSP)

B1. Scope

B1.1 MSSP Services are provided only where expressly defined in a signed MSSP Services Agreement Schedule.

B1.2 MSSP Services may include monitoring, alert triage, defined containment actions and defined remediation tasks within the scope and service levels set out in the applicable Services Agreement Schedule.

B1.3 No monitoring or response obligations arise unless a current MSSP Services Agreement Schedule is in force.

B2. Functional Secure

B2.1 Functional Secure services refer to configuration hardening, security posture improvement and implementation of best practice controls.

B2.2 Functional Secure does not include continuous monitoring or incident response unless separately contracted.

B3. Alert Handling

B3.1 All alerts and security events are subject to classification in accordance with the Master Terms.

B3.2 Service levels apply only to events falling within the contracted MSSP scope.

B3.3 Security tooling and third-party platforms may generate false positives or false negatives.

B4. Containment Authority

B4.1 Where MSSP Services are contracted, CTSS may implement proportionate containment measures to limit active threats.

B4.2 Containment may include temporary account restrictions, enforcement of security controls or isolation of affected systems.

B4.3 Extended remediation, forensic investigation, recovery services or third-party coordination are provided only where expressly included in the Services Agreement Schedule and may be subject to additional Fees.

B5. Risk Reduction Acknowledgement

B5.1 MSSP Services are designed to reduce risk but cannot eliminate risk.

B5.2 No Security Service guarantees prevention of breach or compromise.

B5.3 The Client acknowledges that security monitoring, alert triage, containment measures and related security services are provided on a reasonable endeavours basis within the defined scope of the applicable Services Agreement Schedule and do not

constitute a warranty, guarantee or assurance that any specific threat, vulnerability, exploit, breach attempt or malicious activity will be identified, prevented or successfully mitigated.

B6. Risk Register

B6.1 Identified risks may be documented in a Risk Register and presented to the Client.

B6.2 The Client remains responsible for decisions regarding implementation of recommended actions unless expressly included in scope.

SCHEDULE C: Cloud Subscription Services

C1. Role and Service Boundary

C1.1 CTSS acts as a reseller, broker or administrative intermediary of third-party Cloud Services.

C1.2 The resale, provisioning, renewal, billing or administrative management of Cloud subscriptions does not constitute:

- Managed Services (MSP);
- Managed Security Services (MSSP);
- Continuous monitoring;
- Tenant administration;
- Security configuration;
- Compliance management;
- Data governance;
- Incident response; or
- Operational support,

unless expressly included in a signed Services Agreement Schedule.

C1.3 Access to Cloud Services is subscription-dependent and governed by the applicable third-party provider's customer agreement, policies and service terms.

C1.4 The Client acknowledges that third-party Cloud providers operate as independent service providers and that CTSS does not control their infrastructure, availability, retention policies, security architecture or internal operational processes.

C1.5 No entitlement to configuration, management, security posture enforcement or advisory services arises solely by virtue of CTSS reselling, administering or billing a Cloud subscription.

C2. Licence Dependency

C2.1 Active paid licences are required for access.

C2.2 Suspension or termination may result in access loss and permanent deletion under provider retention policies.

C2.3 CTSS has no control over provider deletion timelines.

C2.4 Suspension or removal of licences in accordance with this Agreement constitutes contractual enforcement of payment and subscription obligations and does not constitute unlawful interference with the Client's property, systems or data. Any data deletion resulting from a licence suspension or termination is performed by the third-party provider in accordance with its retention policies, not by CTSS.

C2.5 CTSS is under no obligation to fund, maintain or temporarily extend any Cloud subscription or licence at its own cost pending payment by the Client, and failure to do so shall not constitute breach of this Agreement.

C2.6 Where a Cloud subscription or licence is suspended for any reason, including non-payment, the Client request, contractual enforcement, provider action, or account status, the applicable Commitment Period and associated Fees remain payable in full.

C2.6.1 No service credits, refunds, offsets, extensions, reductions, or fee adjustments shall accrue during any period of suspension.

C2.6.2 The Client acknowledges that CTSS remains financially committed to upstream provider obligations, including under Microsoft's New Commerce Experience framework, irrespective of suspension status.

C2.6.3 Reactivation of a suspended subscription does not entitle the Client to any retrospective credit, pro-rata adjustment, extension of term, or reduction of Fees.

C2.6.4 This clause does not apply where suspension arises solely from a material breach of this Agreement by CTSS that directly caused the suspension and which has been formally acknowledged by CTSS or determined in accordance with Section 37 (Dispute Resolution).

C3. Commitment Periods

C3.1 Certain licences may be subject to fixed Commitment Periods, including under Microsoft NCE.

C3.2 Commitment fees remain payable in full for the duration regardless of usage or early termination.

C3.3 Commitment obligations survive termination.

C3.4 Subscriptions renew automatically unless cancelled on not less than 2 (two) full calendar month's written notice prior to renewal.

C3.5 Where a Commitment Period is imposed by a third-party provider, including under Microsoft's New Commerce Experience framework, such commitment constitutes a binding upstream obligation. The Client acknowledges that such commitments are non-cancellable and non-refundable except as expressly permitted by the provider, and that early termination or suspension of Services does not relieve the Client of payment obligations for the remainder of the Commitment Period.

C4. Pricing Adjustments

C4.1 Pricing may change due to provider increases, exchange rate movements or licensing model changes.

C4.2 CTSS may adjust pricing upon reasonable notice to reflect such changes.

C5. Service Credits

C5.1 Platform uptime commitments are provided solely by the third-party provider.

C5.2 CTSS does not provide independent uptime guarantees.

C5.3 Provider-issued service credits are passed through and constitute the sole financial remedy for provider outages.

C6. Commercial Model Interaction

C6.1 Where Cloud-related administration, configuration, advisory or remediation work is performed, such work shall be:

- Governed by the applicable Service Schedule; and
- Subject to Schedule F (Commercial Model and Pre-Purchased Hours), where provided under a Pre-Purchased Hours model.

SCHEDULE D: Responsibility Matrix

D1. Purpose

D1.1 This Matrix clarifies the allocation of responsibilities between CTSS, the Client and third-party providers.

D1.2 Where a client-specific Matrix is attached to a Services Agreement Schedule, that Matrix prevails for that Services Agreement Schedule.

D1.3 Marketing materials and informal discussions do not expand the scope beyond the Agreement.

D2. Baseline Allocation

Area	CTSS	CTSS MSP	CTSS MSSP	Client	Provider
Licence provisioning	✓	✓	✓		
End-user helpdesk	Ad Hoc	✓ (per SLA)	Ad Hoc		
Tenant admin	Ad Hoc	✓ (per SLA)	Limited		
Backup & restore	✕	✓ (per SLA)	✕	✓ (Ownership)	Retention only
Security monitoring	Ad Hoc	Ad Hoc	✓ (per SLA)	Notify CTSS	
Incident response	✕	Advisory	✓ (per SLA)		
Compliance decisions	✕	Advisory	Advisory	✓ (Ownership)	

"Ad Hoc" indicates that the activity may be performed on a Time and Materials basis only and does not constitute an ongoing obligation.

D3. Interpretation

D3.1 Where an activity is not expressly marked as CTSS responsibility under the applicable service model, responsibility remains with the Client unless expressly defined in a Services Agreement Schedule.

D3.2 Provider obligations are governed by the provider's terms.

D3.3 Nothing in this Schedule overrides the limitation of liability provisions in the Master Terms.

D3.4 Where an activity or responsibility is not expressly allocated to CTSS under the applicable service model in this Schedule or in a signed Services Agreement Schedule, responsibility remains with the Client.

SCHEDULE E: RMM Baseline Services

E1. Nature of RMM Baseline Services

E1.1 RMM Baseline Services consist of automated endpoint management and limited configuration monitoring services made available by CTSS to qualifying Clients who maintain active Microsoft 365 subscriptions through CTSS.

E1.2 RMM Baseline Services may include:

- Automated deployment of operating system updates and patches;
- Basic monitoring of device health metrics, including processor, memory and storage utilisation;
- Monitoring of Windows Defender and Windows Firewall status;
- Limited posture and status checks, including:
  - Microsoft 365 multi-factor authentication enablement status;
  - privileged role assignments;
  - risky permission configurations;
  - inactive account identification; and
  - Remote management agent deployment for purposes of:
    - Maintenance;
    - Monitoring; and
    - Hygiene automation.

E1.3 RMM Baseline Services are provided as a foundational hygiene layer and do not constitute Managed Services (MSP) or Managed Security Services (MSSP) unless separately contracted under a signed Services Agreement Schedule.

E2. Service Scope and Limitations

E2.1 RMM Baseline Services are provided on a best-effort basis only and are not subject to any service level agreement unless expressly defined in a separate signed Services Agreement Schedule.

E2.2 RMM Baseline Services do not include:

- Continuous monitoring or 24/7 supervision;
- Managed detection and response services;
- Incident response, forensic investigation or breach remediation;
- Helpdesk support, end-user support or troubleshooting services;
- Architecture design, advisory or compliance services; or
- Any form of guarantee that systems will remain secure, patched, available or free from compromise.

E2.3 RMM Baseline Services are intended to provide automated hygiene and limited visibility only. The Client acknowledges that such services do not eliminate operational or security risk.

E2.4 Nothing in this Schedule creates any obligation on CTSS to provide remediation, investigation, advisory or support services beyond the automated tasks expressly described in E1 unless separately contracted and agreed in writing.

E3. Client Responsibilities

E3.1 The Client remains solely responsible for the overall management, security, backup, availability and compliance of its systems, devices and cloud environments unless expressly included in a separate signed Services Agreement Schedule.

E3.2 The Client is responsible for:

- Maintaining appropriate backup and disaster recovery arrangements;
- Ensuring that operating systems and applications are properly licensed and supported;
- Approving and implementing security recommendations where applicable;
- Replacing or repairing failing hardware components; and
- Making all business and risk acceptance decisions relating to its environment.

E3.3 Where RMM Baseline Services identify a potential issue, alert or configuration concern, the Client remains responsible for determining whether further investigation, remediation or escalation is required unless such services are separately contracted.

E3.4 The Client acknowledges that failure to implement recommended controls, security configurations or remediation actions may materially increase operational and security risk.

E4. Authorisation and Access

E4.1 By selecting RMM Baseline Services in a signed Services Agreement Schedule, the Client expressly authorises CTSS to:

- Install and maintain a remote management agent on authorised devices;
- Access such devices remotely for maintenance and hygiene automation purposes;
- Execute automated scripts and deploy operating system patches and updates;
- Collect system telemetry, configuration data and security status information necessary for monitoring and automation; and
- Perform limited configuration checks within Microsoft 365 environments where applicable.

E4.2 The Client acknowledges that remote management functionality may include background administrative access necessary to perform automated maintenance tasks.

E4.3 CTSS will exercise such access only for purposes consistent with this Agreement and will implement reasonable safeguards appropriate to the nature of the Services.

E4.4 The Client may request removal of the RMM agent at any time in writing. Upon such request, RMM Baseline Services will cease, and the agent will be removed within a reasonable period.

E5. Conditional Inclusion and Withdrawal

E5.1 RMM Baseline Services are a discretionary bundled inclusion made available to qualifying Clients who maintain active Microsoft 365 subscriptions through CTSS.

E5.2 RMM Baseline Services are optional and will only apply where expressly selected in a signed Services Agreement Schedule.

E5.3 CTSS may modify, suspend or withdraw RMM Baseline Services upon not less than thirty (30) days' written notice to the Client.

E5.4 CTSS may suspend RMM Baseline Services immediately:

- Where the Client's account is not in good standing;
- Where continued provision would create legal, regulatory or security risk;
- Where required by third-party provider policy or technical constraint.

E5.5 Withdrawal or suspension of RMM Baseline Services does not affect the Client's underlying Microsoft 365 subscription or any separately contracted Services.

E5.6 Upon withdrawal or termination of RMM Baseline Services, CTSS will remove the remote management agent from affected devices within a reasonable period.

SCHEDULE F: COMMERCIAL MODEL & PRE-PURCHASED HOURS

F1. Commercial Structure

F1.1 Services under a signed Services Agreement Schedule may be provided on one or more of the following commercial models:

- Pre-Purchased Monthly Service Hours;
- Time and Materials at prevailing rates;
- Fixed Fee Project Pricing;
- Recurring Subscription Fees.

F1.2 The applicable model for each Service category shall be defined in the signed Services Agreement Schedule.

F1.3 Where Pre-Purchased Hours are selected, this Schedule F applies.

F2. Pre-Purchased Monthly Service Hours

F2.1 The Client selects a defined monthly allocation of service hours for each Service category.

F2.2 Pre-Purchased Hours apply only to the specific Service category for which they are contracted, including but not limited to:

- MSP Hours;
- MSSP Hours.

F2.3 Service categories operate independently and are commercially ringfenced.

F3. Ringfencing and Non-Transferability

F3.1 MSP Hours may only be applied to MSP Services.

F3.2 MSSP Hours may only be applied to MSSP Services.

F3.3 Pre-Purchased Hours may not be transferred, reallocated, substituted or offset between Service categories unless expressly agreed in writing by authorised representatives of both parties.

F3.4 The existence of unused hours in one Service category does not create entitlement to services in another category.

F4. Hour Consumption and Billing

F4.1 Time is recorded in accordance with CTSS standard billing increments.

F4.2 All work performed, including advisory, investigation, configuration, change implementation, triage, containment or consultation, consumes hours from the applicable Service category.

F4.3 After-hours work consumes hours at the uplifted rate defined in Section 19 of the Master Terms. Where uplifted rates apply, time will be deducted at the adjusted rate.

F5. Expiry of Hours

F5.1 Pre-Purchased Hours apply only to the applicable monthly billing period.

F5.2 Unused hours expire at the end of the billing period unless expressly agreed otherwise in writing.

F5.3 Expired hours are not refundable and do not roll over.

F6. Overage

F6.1 Where the Client exceeds the allocated Pre-Purchased Hours in any Service category, additional time shall be billed at the prevailing standard hourly rate for that Service category.

F6.2 Overage time is invoiced in arrears.

F6.3 Overage does not expand scope or create entitlement to additional service levels.

F7. Adjustment of Pre-Purchased Hours

F7.1 The Client may request an increase to its monthly Pre-Purchased Hours allocation by providing written notice to CTSS.

F7.2 Any increase shall take effect only from the first day of the next billing cycle.

F7.3 Mid-cycle increases do not apply retrospectively to hours already consumed.

F7.4 Where hours are exhausted during a billing cycle, all additional time shall be billed at the prevailing standard hourly rate until the next billing cycle commences.

F7.5 Decreases to Pre-Purchased Hours, where permitted under the applicable Services Agreement Schedule, shall also take effect only from the first day of a subsequent billing cycle and may not reduce any Commitment Period obligations.

F8. SLA Independence from Hour Allocation

F8.1 SLA response targets are defined in the applicable Service Schedule and apply regardless of the number of Pre-Purchased Hours selected.

F8.2 Selection of a higher or lower monthly hour allocation does not increase, decrease or modify SLA response targets unless expressly agreed in writing.

F8.3 Pre-Purchased Hours define service capacity only and do not constitute a guarantee of resolution within a specified timeframe.

F9. Licence Resale and Service Separation

F9.1 The resale, administration or billing of Cloud subscriptions does not create an entitlement to tenant administration, operational support, security monitoring, compliance management, incident response or configuration services.

F9.2 Such services are provided only where expressly included in a signed Services Agreement Schedule.