MANAGED SERVICES

SERVICE LEVEL AGREEMENT SCHEDULE

Version: 2
Date: July 2026

Managed Services Agreement

1. INTERPRETATION AND DEFINITIONS

1.1 In this Agreement, the following expressions shall have the following meanings unless the context otherwise requires:

"**The Company**" means Amicus ITS Limited t/a Aura Technology (Company Registered Number 03879859), as defined in the Order Form.

"**The Customer**" means the Customer as defined in the Order Form.

"**Customer Equipment**" means the Customer's IT hardware and software utilised in the provision of the Hosting Services by the Company.

"**Employment Liabilities**" means all actions, proceedings, costs (including reasonable legal costs), losses, damages, fines, penalties, compensation, awards, demands, orders, expenses and liabilities connected with or arising from the employment of the Employee or their termination of employment including, without limitation, any claims of unfair or wrongful dismissal, breach of contract, sex, race, sexual orientation, religion or belief, or disability or age discrimination, a breach of the TUPE Regulations or any other claim arising from any other Employment Law;

"**Key Personnel**" means any Personnel involved in the day-to-day delivery of Service to the Customer.

"**Personnel**" means any individual employed by the Company.

"**Replacement Provider**" means any company, organisation or person who replaces The Company following termination or expiry of all or part of this Contract.

"**The Company's Representative**", the Representative of the Company at the Commencement Date, is responsible for overseeing the Contract and is named in the Order Form.

"**TUPE**" means the Transfer of Undertakings (Protection of Employment) Regulations 2006.

"**Authorised Contact(s)**" means members of staff at the Customer who are authorised to make requests for changes to this schedule regarding managing Authorised Users and Authorised Devices and are named in the Order Form.

"**Authorised User**" means an Authorised member of staff who will have access to the services outlined in this schedule. Users agree at Onboarding or in writing from time to time for the purposes of interacting with the Company under the terms of this Agreement.

"**Authorised Device**" means a company-owned device that has access to the services outlined in this schedule.

"**Managed Services**" means services sold as per the order form and any corresponding terms and conditions and applicable service schedules.

"Workstation or Laptop Device" is any user-based computer running supported Windows or Apple operating systems.

"Mobile Device" is any compatible mobile device that is owned by the Customer or an Authorised User that is approved for use on the Customer IT System by the Authorised Contact.

"Server Device" refers to any device running a supported Microsoft Windows or VMware operating system, including hardware support where appropriate and support for devices in supported Cloud environments. Note that support for any environments is not included unless managed by the Company.

"Network Device" is any network device agreed to be supported at the point of order. For clarity, any infrastructure device that does not run a server operating system and requires support will be considered a Network device, unless otherwise specified by the Company.

"Order Form" is a formal agreement that outlines the specific IT services and products to be delivered by the Company to a named Customer. It serves as a binding contract once signed by both parties and is governed by the Company's General Terms and Conditions and any attached schedules, such as service level agreements (SLAs) or Managed Service terms.

"Initial Term" means the period beginning on the agreed Commencement Date of the contract on the Order Form and continuing for a defined duration, typically 36 months.

2. GENERAL

2.1 In the event of a conflict between provisions of a product or service, the order of resolution is as follows: First, the conditions specified in the order form; second, the relevant service schedule; and third, the general terms and conditions.

2.2 With effect from each anniversary of the Commencement Date, the Managed Services Charges are subject to an annualised inflationary increase, which is limited to the lesser of the prevailing rate of CPI or RPI. Where this is a negative number, no inflationary increase will be applied.

2.3 The Agreement shall remain in force for the Initial Term and may not be terminated for convenience during this period. Upon expiry of the Initial Term, the Agreement shall automatically continue for successive periods of three (3) months (each a "renewal term"), unless and until either party gives not less than ninety (90) days' prior written notice to terminate. Any such notice may only take effect on or after the expiry of the Initial Term.

2.4 With effect from the day after the end of the Initial Term, charges shall be reset to the greater of: (a) the then-current charges (after any indexation applied during the Initial Term); or (b) 115% of the initial charges. Thereafter, annual indexation applies as above.

2.5 The Customer agrees that it will only use the Services in accordance with the provisions of the Agreement and the Company's reasonable instructions from time to time.

2.6 The Company may, at its sole discretion, suspend the Managed Services (in whole or in part) if the Company is entitled to terminate the Agreement for any reason.

2.7 Exercise by the Company of its right of suspension in connection with non-payment by the Customer of the Company's valid charges under the General Terms & Conditions shall not function as a waiver of any right or termination which the Company may have under this agreement.

2.8 Managed Services are subject to the Company's Acceptable Use Policy (AUP).

3. SERVICEDESK

3.1 Service Desk is the single point of contact for incidents and requests relating to the Managed Service, for Authorised Users.

3.2 Service Desk staff will respond to telephone calls and emails, logging all Incidents and Requests into the company's service management system, which will generate a unique reference.

3.3 The Company will maintain a Service Desk that will manage the logging, prioritisation and resolution of all Incidents and Requests reported by the Customer and/or the Company in accordance with the Service Desk description and service levels set out below.

3.4 Following the reporting of an Incident or Service Request to the Service Desk, Authorised Users will receive a confirmation email. This email will contain the reference number for the logged ticket.

3.5 The Service Desk will determine the business impact and urgency of the Incident with the Authorised User. These factors will be used to set the priority and the target time for responding to the Incident. It is the responsibility of the Service Desk to ensure responses to Incidents are within these target times.

3.6 The Service Desk maintains ownership of all Incidents and tracks their progress against resolution targets. Incidents that miss their target resolution will be escalated by the Service Desk to senior management within the Company. Critical Incidents will be escalated immediately if they miss their target resolution, and remedial actions will be outlined in writing by the Company to the Customer, including full details of the Incident and the necessary steps for rectification.

3.7 The Incident ticket is considered resolved and closed once the service has been restored or a workaround has been provided. Root cause analysis or a permanent solution to a workaround will be investigated and implemented on a problem ticket, which will be raised by the Service Desk. It is the responsibility of the Service Desk team to ensure all Incidents are marked as completed. Incidents will not be left open to monitor if they recur.

3.8 Once an incident has been completed, it cannot be reopened. In such cases, a new incident will be created.

4. LOGGING AN INCIDENT OR REQUEST

4.1.1 **Critical Incidents (Priorities 1 or 2)**

4.1.1.1 These should be reported to the Service Desk by telephone using the number provided during onboarding. It is the responsibility of the Company employee who receives a call reporting a Critical Incident to ensure it is logged in the Service Desk software.

4.1.2 **Normal Incidents (Priorities 3 or 4)**

4.1.2.1 These should be reported by telephone to the Service Desk. Alternatively, an Incident can be emailed to the support email address provided during onboarding, or via the web-based client portal.

4.1.2.2 Incidents will also be automatically logged by the Company's Remote Monitoring and Management software. Such incidents will be triaged and assigned the appropriate priority. These incidents will receive the same SLA as any other incident.

4.1.3 **Requests**

4.1.3.1 Requests should be logged by email/telephone/web with the Service Desk and from an Authorised User only.

4.1.3.2 If a request is logged by an Authorised User, the Service Desk will send a request for further information or authorisation. This should be completed and returned as soon as possible to avoid delaying the fulfilment of the Request. The Service Request will be accepted once all information required to action the Request has been received

4.1.3.3 The Customer must supply (and not unreasonably withhold) important or accurate information at the outset or when requested subsequently by the Company.

4.1.3.4 The Customer and any related third party must respond to or act upon reasonable instructions and/or requests for assistance in a timely manner.

5. HOURS OF OPERATION

5.1 The Company Service Desk will be available remotely to the Customer during the following hours:

5.1.1 24x7 365 days per year (incidents and requests), unless otherwise agreed between the Customer and the Company on the Order Form.

5.1.2 Any incident or request requiring an on-site engineer for remediation will be handled during Business hours, Monday to Friday, 9 am – 5.30 pm. Support provided outside this timeframe may incur additional fees, which are available on request.

5.1.3 The Network Operations team uses monitoring systems that continuously oversee managed systems 24 hours a day. If any managed system becomes unavailable, an incident will be logged with the Service Desk, and an investigation into the issue will begin according to the SLAs, which specify prioritisation levels and target response and resolution times where applicable.

5.1.4 Telephone support is available via a designated telephone number. Support requests made to the Company's dedicated support number by Authorised Users will be answered by the first available engineer. The Company Standard Service Level Agreement applies, as set out below.

5.1.5 Email support through a designated email address. Support requests sent by email will be attended to by the first available engineer. The Company Standard Service Level Agreement applies, as outlined below.

5.1.6 Support is available through the Company client portal. Support requests submitted via the portal will be attended to by the first available engineer. The Company standard Service Level Agreement applies, as outlined below.

6. AUTHORISED DEVICES, AUTHORISED USERS AND AUTHORISED CONTACTS

6.1 The Managed Service is only provided directly to Services sold, Authorised Users, and the Authorised Devices they use. Authorised Devices and Services will be identified, and any Company management or monitoring agents will be installed during the onboarding process if required. Authorised

Contacts and Authorised Users at the Customer will be agreed upon during onboarding, and any additional Users, Devices, or Services identified for inclusion by the Authorised Contact will be billed accordingly. Numbers may vary during the billing period depending on the Customer's requirements, but cannot be reduced to below the initially quoted users on this order per month for the Contract Term. Any support requests from the Customer for unauthorised Users, Devices, or Services will be escalated to the Authorised Contact at the Customer.

7. SERVICE DESK LEVEL 1

7.1 The Company Level 1 Service Desk team is responsible for providing first-time fix support and handling basic service requests. Their primary objective is to resolve issues during the initial contact, including "how to" queries and basic troubleshooting tasks.

7.2 Incident logging and tracking are managed via the Company's ticketing system, which records all Incidents and Requests.

7.3 24/7 availability for Authorised User support, ensuring continuous assistance.

7.4 Escalation protocols to Level 2 and Level 3 teams for complex or unresolved issues.

7.4.1 **Service Desk Level 1 typical tasks.**

7.4.1.1 User Access and Authentication

(a) Password resets and account unlocks.

(b) Troubleshooting login failures across Windows, Azure AD, and Microsoft 365 platforms.

(c) Resolving client-side multi-factor authentication (MFA) issues.

7.4.1.2 Desktop and Device Support

(a) Diagnosing and resolving printer connectivity issues.

(b) Troubleshooting peripheral device problems (e.g. mouse, keyboard, webcam).

(c) Resolving display and resolution issues on the Authorised Users' desktop.

7.4.1.3 Software and Application Support

(a) Reinstalling or updating commercial off-the-shelf (COTS) software packages.

(b) Assisting with "how to" queries for COTS applications like Microsoft Outlook, Teams, and Excel.

(c) Fixing basic application crashes or errors.

7.4.1.4 Network and Connectivity

(a) Resolving client-side Wi-Fi and LAN connectivity issues.

(b) Assisting Authorised Users with client-side VPN access problems.

(c) Troubleshooting slow internet or network dropouts.

8. SERVICE DESK LEVEL 2

8.1 The Company Level 2 Service Desk provides technical support for escalated incidents and service requests. Their role bridges the gap between first-line resolution and deeper infrastructure, or application-level troubleshooting provided by the Service Desk Level 3.

8.2 Incident and Request Management: Handle tickets escalated from Level 1 or received directly, using structured processes aligned with SLA targets.

8.3 Incident logging and tracking are handled through the Company's ticketing system, which logs all Incidents and Requests.

8.4 24/7 availability for Authorised User support, ensuring continuous assistance.

8.5 Escalation path to the Level 3 team for complex or unresolved issues.

8.5.1 **Service Desk Level 2 typical tasks.**

8.5.1.1 User Access and Authentication

(a) Resolving persistent multi-factor authentication failures across Microsoft 365 and Azure AD environments.

(b) Managing user accounts and permissions within Active Directory and Azure AD, including group policy adjustments and role-based access control.

(c) Diagnosing and resolving licensing conflicts and provisioning issues.

8.5.1.2 Desktop and Device Support

(a) Diagnosing and resolving OS-level faults across Windows and macOS environments.

(b) Supporting Infrastructure environments, including performance tuning and user experience optimisation.

(c) Identifying hardware bottlenecks (e.g. RAM shortages) and coordinating upgrades to improve performance.

(d) Investigating and resolving freezing or lag in business-critical applications.

(e) Resolving persistent issues with printers, webcams, and other peripherals that Level 1 could not fix.

8.5.1.3 Software and Application Support

(a) Diagnosing and fixing freezing, lagging, or crashing in applications such as Microsoft Outlook, Teams, and Excel.

(b) Re-installing and configuring bespoke and commercial off-the-shelf (COTS) software across various operating systems.

8.5.1.4 Network and Connectivity

(a) Diagnosing and resolving connectivity issues across local and wide area networks.

(b) Manage firewall configurations and resolve VPN access problems to ensure secure remote connectivity.

9. SERVICE DESK LEVEL 3

9.1 The Company Level 3 Service Desk team is responsible for managing major incidents, problem management, and complex escalations that require advanced technical expertise.

9.2 Incident and Request Management: Handle tickets escalated from Level 2 or received directly, using structured processes aligned with SLA targets.

9.3 Incident logging and tracking are handled through the Company's ticketing system, which logs all Incidents and Requests.

9.4 24/7 availability for Authorised User support, ensuring continuous assistance.

9.5 Lead technical investigations and collaborate with 3rd party vendors to resolve complex issues.

9.5.1 **Service Desk Level 3 typical tasks.**

9.5.1.1 User Access and Authentication

(a) Advanced Identity Management: Troubleshooting and configuring Entra ID (Azure AD) for hybrid and cloud-only environments.

(b) Troubleshooting SSO integrations across Microsoft 365, third-party SaaS platforms.

(c) Auditing, resolving conditional access policies, MFA enforcement, and identity protection rules.

9.5.1.2 Desktop and Device Support

(a) Tuning Azure Virtual Desktop performance, including session host scaling and FSLogix profile management.

(b) Supporting Infrastructure environments, including performance tuning and user experience optimisation.

(c) Diagnosing persistent hardware faults, driver conflicts, and OS-level corruption across Windows and macOS.

9.5.1.3 Software and Application Support

(a) Application Stack Troubleshooting: Resolving performance issues in Microsoft 365, Exchange Online, SharePoint, Teams, and third-party business apps

(b) Custom Integration Support: Supporting API-based integrations between business systems and cloud platforms

(c) Troubleshooting bespoke and commercial off-the-shelf (COTS) software across various operating systems.

9.5.1.4 Network and Connectivity

(a) Managing complex firewall rules, VLANs, and routing protocols across multi-site environments

(b) supporting SD-WAN, Starlink, and Microsoft Teams Voice solutions

(c) Leading resolution efforts for major network outages and security incidents

10. INCIDENT MANAGEMENT

10.1 An Incident is defined as an unplanned interruption to an IT service or a reduction in its quality. It can also refer to an event that hasn't yet affected the service but has the potential to do so, such as declined access to the User's applications, deterioration in the service, or unacceptably poor response. It is distinct from requests made to the Service Desk, such as mapping a printer or installing new equipment.

10.2 The primary objective of Incident management is to restore service to an Authorised User or Users as soon as possible. This is often achieved using an acceptable workaround to the issue while the root cause is investigated separately as a problem.

10.2.1 **Incident Management Process**

10.2.1.1 An Incident is logged with the Service Desk, who will generate (or confirm) an Incident ticket reference number. The Company will endeavour to resolve the Incident according to the priority defined.

10.2.2 **Priority Level**

10.2.2.1 Priority is determined by understanding the business impact and urgency of an Incident. 'Impact' is a measure of the number of people affected by the Incident.

10.2.2.2 'Urgency' pertains to the speed required to resolve an Incident and reflects how quickly the impact will be experienced by the business, such as missing important deadlines.

10.2.2.3 The Service Desk will agree on the business impact and urgency of the incident with the affected user or users. If agreement cannot be reached, or if there is uncertainty regarding the correct prioritisation, the assessment will be escalated to more senior staff at the company and the customer.

10.2.3 For the purposes of the Managed Service, the Company adopts the following priority categories:

10.2.3.1 **Low Priority:** one device/user is affected. The issue relates to only a minor annoyance. There is no productivity loss.

10.2.3.2 **Medium Priority:** one device/user is affected moderately, resulting in some productivity loss, or multiple machines/users are affected with only minor loss of productivity.

10.2.3.3 **High Priority:** An incident affects multiple machines/users at one site, resulting in the loss of business-critical functions in one area.

10.2.3.4 **Critical Priority (Major Incident):** The incident affects multiple machines/users, severely impacting business productivity, reputation, and function.

11. SERVICE REQUEST FULFILMENT

11.1 The term 'Service Request' is a general description for various types of requirements that customers need fulfilled by the Company**.** Many of these are small adjustments – low risk, frequent, low cost, and so on (e.g., a request for access to a database, installing additional software on a specific device, relocating desktop equipment), or simply questions seeking information. The Service Request service speeds up these processes, ensuring a quick response.

11.1.1 Examples of Service Requests include requests for access, moves, new account creation, removal of access from leavers, and assistance with applications.

11.1.2 Large-scale projects, including moves of several people and equipment or onboarding new Infrastructure, are handled as projects and are charged separately and managed by the Company Account Management and/or Project Management teams.

12. INCIDENT/REQUEST TARGETS

12.1.1 Incident Response - The response target is the elapsed time between logging the call with the Service Desk and the Incident's acceptance by the appropriate support team when a support technician is assigned.

12.1.2 Acceptance of incidents will only take place when all information required to progress and resolve them has been provided to the service desk. This acceptance will trigger an acknowledgement email to the User who reported the Incident. This email will contain the ticket reference number.

12.1.3 The following table shows the target response times for each priority level, along with the target resolution time for Move, Add, and Change requests (Service Requests).

Priority Level	Critical	High	Medium	Low
First Response	30 minutes	1 hour	3 hours	8 hours
SLA Target	90%	90%	90%	90%
Move, Add, Change Requests resolution time (Request and Configuration Management)	24 Hours			

12.1.3.1 The target response level for the above service levels is 90%, in relation to the agreed support hours provided by the Company.

12.1.3.2 The Company shall not be deemed to be in breach of the SLA where circumstances prevent it from providing the Services, including (but not limited to) lack of internet connectivity at the Customer location(s) or in any other circumstances outside of the Company reasonable control such as (but not limited to) reliance on a third party vendor or service provider for a service, relevant information, timely action or response, or in any other circumstances that would amount to a Force Majeure Event.

12.1.4 **Incident Resolution**

12.1.4.1 The resolution target is the elapsed time between logging the call with Service Desk and the restoration of service. There may be additional work required to make the fix permanent or to investigate the underlying cause and thus prevent recurrence.

12.1.4.2 The restoration of service will be shown by the Incident status being set to complete.

12.1.4.3 If, after three business days of the Authorised User being contacted to indicate resolution of the Incident, the Authorised User has not contacted the Service Desk to report that the resolution to the Incident was not successful or acceptable, it is assumed that the Authorised User is satisfied with the resolution, and the Incident or Request will be completed.

13. PROBLEM MANAGEMENT

13.1 Problem Management is designed to resolve the root cause of incidents, minimising their adverse impact on the Customer's organisation and preventing recurrence.

13.2 A problem is an unknown underlying cause of one or more incidents, while a known error is a problem that has been successfully diagnosed and has a workaround.

13.3 Problems are often identified from multiple incidents with common symptoms or from a single significant incident indicative of a single error with an unknown cause but significant impact.

13.4 The problem management service manages and resolves the root causes of recurring or significant IT incidents, reducing the impact of problems on business operations and preventing future disruptions.

13.5 The Customer shall support the implementation of permanent fixes or changes resulting from problem investigations. This includes scheduling downtime, approving change requests, and agreeing to any additional project costs that may be required.

13.6 Where the root cause of a problem lies with a third-party vendor or system under the Customer's control, the Customer shall be responsible for engaging the relevant third party and coordinating resolution efforts. The Company will provide technical support and documentation as needed

13.7 In Scope;

13.7.1 Problem Detection & Logging: Identifying problems through trend analysis, major incident reviews, or repeated incidents.

13.7.2 Root Cause Analysis (RCA): Investigating underlying causes using structured methodologies.

13.7.3 Known Error Management: Documenting known errors and workarounds in the Knowledge Base.

13.7.4 Problem Resolution: Coordinating with relevant teams to implement permanent fixes.

13.7.5 Problem Review & Reporting: Providing regular reports on problem trends, root causes, and resolution status.

13.8 Out of Scope;

13.8.1 Major infrastructure redesigns resulting from problem findings.

13.8.2 Any changes considered by the Company that require significant planning, testing, or downtime (e.g., infrastructure upgrades, migrations, security changes).

13.8.3 Third-party vendor escalations requiring extended coordination or legal involvement.

13.8.4 Custom reporting or deep-dive analytics beyond standard monthly reports.

13.8.5 On-site investigations unless included in the Managed Service.

13.8.6 Training or workshops on problem management tools or processes.

14. REQUEST & CONFIGURATION MANAGEMENT

14.1 Moves, adds, and changes are included as part of the service; however, any item listed in **Section 33** or the Order Form will not be considered in scope.

14.2 The Company Service Desk will create all new user accounts for the Customer following the process specified during the onboarding procedure. Additionally, the Company Service Desk will assist any new user in setting up a suitable profile on any authorised device to complete their work. However, end-user training will not be provided and remains the responsibility of the Customer or can be arranged at an additional cost.

14.3 Tasks related to new user creation will take up to 24 business hours to complete and require a minimum of five working days' notice. Because of the maintenance involved in these requests, they are excluded from our standard Service Level Agreement.

15. CHANGE MANAGEMENT

15.1 The Company will manage changes to the IT environment to ensure minimal disruption and controlled implementation. This includes assessing, planning, approving, implementing, and reviewing changes.

15.2 All changes must be submitted via a formal Change Request (CR). The Company will assess the impact, risk, and resources required. All Changes will be classified as Standard, Emergency, or Major.

15.3 The Company may implement emergency changes without prior approval to restore service or prevent major incidents. A post-change summary will be provided within 48 business hours.

15.4 Customer Responsibilities

- 15.4.1 Notify the Company of any changes to the configuration or updates to the supported devices under the managed service.
- 15.4.2 Provide timely approvals and relevant information.
- 15.4.3 Ensure internal stakeholders are informed and available.
- 15.4.4 Attend Change Advisory Board (CAB) meetings if required.

15.5 In Scope.

- 15.5.1 Processing and implementing Standard Changes (e.g., routine patching, configuration updates).
- 15.5.2 Participation in regular CAB meetings.
- 15.5.3 Maintaining the Change Log and reporting.
- 15.5.4 Emergency changes are required to restore service.

15.6 Out of Scope.

- 15.6.1 Any changes that require significant planning, testing, or downtime (e.g., infrastructure upgrades, migrations, security changes) are considered.
- 15.6.2 Changes initiated by the Customer that require work to be carried out outside of 8 am to 6 pm, Monday to Friday (excluding public and bank holidays).
- 15.6.3 Changes involving third-party coordination or bespoke development.
- 15.6.4 Extensive impact assessments or documentation beyond the standard scope.
- 15.6.5 Training or communication materials tailored for the Customer teams.
- 15.6.6 Any costs resulting from a Customer or 3rd Party change.

16. NETWORK OPERATIONS CENTRE

16.1 As part of the Managed Service, the Company will monitor and manage the Customer's authorised Workstations, Laptops, Servers and Network Devices and raise tickets to resolve issues as appropriate.

16.2 The Company will maintain a Network Operations Centre that will manage the logging, prioritisation and resolution of all Incidents reported by the Customer and/or the Company's remote monitoring and management solution in accordance with the Network Operations Centre services and Service Levels set out in 15.12.

16.3 Network Operations Centre Team will respond to alerts, telephone calls and emails, logging all Incidents into the Company's service management system, which will generate a unique reference.

16.4 The Network Operations Centre is the single point of contact for incidents relating to the Managed Service for Authorised Users.

16.5 Following the reporting of an Incident to the Network Operations Centre, the Authorised User will receive a confirmation email. This email will contain the reference number for the logged ticket.

16.6 The Network Operations Centre will agree on the business impact and urgency of the Incident with the Authorised User. These will be used to calculate the priority, and thus the target time to respond to the Incident. It is the responsibility of the Network Operations Centre to ensure that responses to Incidents are within these target times.

16.7 The Network Operations Centre retains ownership of all Incidents and monitors their progress against response targets. Incidents which miss their target response will be escalated by the Network Operations Centre to senior management within The Company.

16.8 The Incident ticket is resolved and completed when the service has been restored, or a workaround has been provided.

16.9 Root cause analysis or a permanent fix to a workaround will be investigated and carried out under problem management if the Customer has this service.

16.10 Incidents will not be left open to see if they recur. Once an Incident has been completed, it cannot be reopened. In such cases, a new Incident will be created.

16.11 As and where required, the Company Network Operations Centre will carry out permission-based remote remediation in order to resolve the reported issue(s). Remediation work will only be carried out for authorised Workstations, Laptops, Servers and Network devices, and where the facility to connect remotely exists.

16.12 **SLA**

Priority Level	Critical	High	Medium	Low
First Response	30 minutes	1 hour	3 hours	8 hours
SLA Target	90%	90%	90%	90%
Move, Add, Change Requests resolution time (Request and Configuration Management)	24 Hours			

17. SERVER MONITORING, PATCHING AND REMEDIATION

17.1 The Managed Service is designed as a fully managed service for Server devices. Monitored alerts or tickets raised by the Company or the Customer will be analysed, prioritised and corrective action taken.

17.2 Typical Server Monitoring

Agent status	Hypervisor health	Reboot required	SQL DB
CPU	Memory	Server temperature	SQL memory
Disk space	Patch status	SNMP	SQL buffer
Disk I/O	Raid	Uptime	SQL transactions
FAN	Windows services	Windows Firewall	SQL services

17.3 The Company will perform patching for supported Microsoft operating systems. Security, Definition, Updates, Rollups, and Critical Updates will be automatically deployed and applied according to the Company's predefined schedule.

Services	Description
Critical Updates	A fix for a specific problem addressing a critical, but non-security-related bug.
Definition Updates	Software update containing additions to a product's definition database.
Drivers	Software controlling the input and output of a device.
Feature Packs	New functionality is distributed outside the context of a product release, which is usually included in the next full release.
Security Updates	A fix for a product-specific, security-related vulnerability.
Service Packs	A cumulative set of hotfixes, security updates, critical updates, updates, and additional fixes. Service packs may also contain customer-requested design changes or features.
Tools	A utility or feature for completing a task or set of tasks.
Updates	A fix for a specific noncritical, non-security-related problem.
Update Rollups	A cumulative set of hotfixes, security updates, critical updates, and updates packaged together for easy deployment, generally targeting a specific area.

17.4 The Company does not support patching for operating systems that are deemed End of Life or out of support.

17.5 The Company will perform automated post-installation checks, if necessary, take steps to remediate any discovered issues upon rebooting, including verifying the monitored Windows services for failures and addressing any identified problems.

17.6 Patching Schedule

17.6.1 Patches are approved for deployment seven days after release. All approved patches are scheduled to be deployed on a designated weekday at 12:30 a.m. on a weekly, biweekly, or monthly basis unless otherwise agreed in the Order From.

17.6.2 The Company shall perform routine and critical maintenance activities during the standard maintenance window, which is 12:30 am to 03:30 am GMT, on business days. Any maintenance requiring system downtime shall happen during the maintenance window.

17.6.3 Downtime outside the maintenance window shall be communicated to the Customer at least 48 hours in advance and shall not proceed without written consent.

17.6.4 Emergency maintenance may be conducted outside these windows with immediate notification.

17.7 If required, supported third-party application patches will be scheduled and installed automatically. A full list of supported 3rd party applications can be found at https://auratechnology.com/terms/3rdpartyapps

17.8 The Company will monitor and remediate Anti-virus/Anti-malware updates for supported anti-virus and antimalware products supplied by the Company.

17.9 The Company will perform proactive routine maintenance activities on a scheduled basis as follows:

17.9.1 Disk clean-up & temporary file deletion.

18. NETWORK MONITORING, PATCHING AND REMEDIATION

18.1 The Managed Service is designed as a fully managed service for network devices. Monitored alerts or tickets raised by **The Company** or **The Customer** will be analysed, prioritised and corrective action taken.

18.2 Typical Network Monitoring

Uptime	Availability	Reboot required	UPS status
Power supply failure	VPN Failure	Licence Issue	Environmental status

18.3 The Company cannot guarantee that devices not supplied by the Company can be monitored. The Company's ability to monitor these devices is contingent upon the third-party provider providing the correct configuration.

18.4 Internet connections or WAN services routed through authorised devices will be monitored for availability.

18.5 Liaison with third-party connectivity providers that are not provided through the Company is only available where the Customer has given the Company authorisation to act on their behalf and will be provided on a best-efforts basis.

18.6 Routine maintenance is provided on an as-needed basis for Network devices.

18.6.1 Company-supplied network Devices are checked monthly, and available security updates are applied in the agreed maintenance window.

18.6.2 Zero-day vulnerabilities advised by the Vendor are applied under the emergency change procedure.

18.6.3 Moves, adds, and changes for network devices will be limited to modifications that do not impact the overall structure and design of the network. If a request is deemed out of scope, it will be referred to the Company Account Manager to provide a quote to the Customer for project work.

18.6.4 The Company does not support patching for operating systems that are deemed End of Life or out of support.

19. DESKTOP MONITORING, PATCHING AND REMEDIATION

19.1 The Managed Service is designed as a fully managed service for Desktop devices. Monitored alerts or tickets raised by the Company or the Customer will be analysed, prioritised and corrective action taken.

19.2 Typical Desktop Monitoring

Firewall status	Patch status	Reboot required	SQL DB
CPU	Memory	Disk space	Windows Services
AV status	Warranty Information		

19.3 The Company will perform automated patching for supported Microsoft operating systems. Security, Critical, and Definition Updates, as well as Update Rollups and Feature Packs, will be automatically deployed and applied according to the Company's pre-defined schedule.

Services	Description
Critical Updates	A fix for a specific problem addressing a critical, but non-security-related bug.
Definition Updates	Software update containing additions to a product's definition database.
Drivers	Software controlling the input and output of a device.
Feature Packs	New functionality distributed outside the context of a product release, which is usually included in the next full release.
Security Updates	A fix for a product-specific, security-related vulnerability.
Service Packs	A cumulative set of hotfixes, security updates, critical updates, updates, and additional fixes. Service packs may also contain customer-requested design changes or features.
Tools	A utility or feature for completing a task or set of tasks.
Updates	A fix for a specific noncritical, non-security-related problem.
Update Rollups	A cumulative set of hotfixes, security updates, critical updates, and updates packaged together for easy deployment, generally targeting a specific area.
Upgrades	Windows full version upgrades

19.4 The Company does not support patching for operating systems that are deemed End of Life or out of support (For Example, Windows XP and Windows 7)

19.5 Patches are approved for deployment seven days after release. All approved patches are scheduled to be deployed daily until a device has received all relevant patches. If a device needs to be rebooted to complete the installation of any patches, the user will be notified and will have four hours to restart the device; otherwise, it will automatically reboot to finish the installation.

19.6 Upgrades, due to their size, are approved and deployed over a one-month schedule to Customer Devices.

19.7 The Customer must ensure that supported devices are regularly online for at least four consecutive working hours to ensure the successful deployment of patches. Failure to make devices available may result in project costs to bring the infrastructure to a supportable state.

19.8 If required, supported third-party application patches will be scheduled and installed automatically. A Full list of supported 3rd party applications can be found at https://auratechnology.com/terms/3rdpartyapps

19.9 The Company will perform managed patching for supported Apple operating systems, provided the Customer has taken the Company's Apple Device Management Solution. Apple Software Updates will be automatically deployed and made available to the Authorised User for installation as they are released by Apple.

19.10 The Company will monitor and remediate Anti-virus/Anti-malware updates for supported anti-virus and antimalware products supplied by the Company.

19.11 The Company will perform proactive routine maintenance activities on a scheduled basis as follows:

19.11.1 Disk clean-up & temporary file deletion.

20. MANAGED BACKUP MONITORING AND REMEDIATION

20.1 The Company will monitor scheduled backup jobs daily, provided the Company has either implemented or approved the Customer's backup solution for use, and take remedial action based on alerts for failed, overrunning, or incomplete backups.

20.2 Analyse and resolve issues affecting backup systems, including hardware and software components.

20.3 Perform proactive maintenance tasks to ensure backup jobs complete successfully.

20.4 Restore data from backups upon request, subject to the agreed-upon Recovery Point Objective (RPO) established at onboarding or the Company's minimum standard backup Schedule, as follows.

20.4.1 M365 4x daily backups, 12-month retention

20.4.2 Google Workspace 4x daily backups, 12-month retention

20.4.3 Virtual and Physical Servers 1x daily backups, 12-month retention

20.5 The following are excluded unless explicitly agreed in the Order Form:

20.5.1 End-user training related to backup systems.

20.5.2 Remediation for unsupported hardware/software or where remote access is not possible.

20.5.3 Restoration of services based on the Company's determination of a Business Continuity or Disaster Recovery Event.

20.5.4 Business Continuity and Disaster Recovery (BCDR) Plan testing or simulated test restorations.

20.5.5 Project-based activities include planning new backup strategies and implementing additional cloud-based solutions.

20.5.6 Test restores and validity checks other than the Company's backup solutions, automated quality and integrity checks.

20.6 Customer Responsibilities

20.6.1 Ensure all devices requiring backup are authorised and backup requirements are provided to the Company.

20.6.2 Notify the Company of any suspected data corruption or loss immediately.

20.6.3 Accept that remediation tasks may require up to 72 hours for completion and are excluded from standard SLA targets.

21. PROACTIVE ENGINEERING

21.1 Aura's Proactive Engineering Service is a strategic IT function embedded within its Managed IT offering, designed to deliver operational excellence, automation, and business value through regular customer engagement. The service focuses on improving system stability, reducing repeat issues, and enhancing user productivity by leveraging existing IT platforms and customer line-of-business applications.

21.2 In Scope.

21.2.1 Monthly Customer Reviews: Analysis of reports, ticket trends, and repeat issues, with follow-up actions and recommendations.

21.2.2 Authorised User Enablement: Providing training materials, Manual updates to customer and internal documentation and championing the adoption of deployed service and/or solutions.

21.2.3 Automation Identification: Spotting opportunities for small automation (e.g., starters/leavers, Power Automate flows) to improve business processes and the Authorised User IT experience.

21.2.4 Customer Advocacy: Collaborating with Account Managers to align IT with organisational goals.

21.3 Out of Scope.

21.3.1 Technical Design Work: Architecture, engineering, and solution design.

21.3.2 Project Delivery: Implementation of IT projects, migrations, or deployments.

21.3.3 Reactive Support: Day-to-day troubleshooting is handled by the Service Desk, Customer Success, or Network Operations teams

21.3.4 Line-of-Business Application Development: Custom software development.

21.3.5 Production of the Customer's Technology Roadmap.

22. AGREED SERVICE WINDOWS

22.1 All services provided by the Company require changes to be made periodically, which could, but not necessarily, be due to:

22.1.1 Routine maintenance

22.1.2 Installation of critical security fixes

22.1.3 Installation or updates to hardware or application software

22.2 Some changes will require downtime to the affected system outside of the maintenance window, and these changes will be notified accordingly and will not be undertaken without the prior agreement of the Customer.

23. ASSET MANAGEMENT

23.1 The Company shall deliver Asset Management services, including device tagging if requested, and reporting for devices that can be monitored by the Company's Remote Monitoring and Management Solution.

23.2 The Company shall deploy RMM software to all authorised devices. This software will be used to provide an Asset List in a monthly scheduled report to the Customer.

23.3 Only devices explicitly authorised during onboarding or added to the Managed Services Contract at the Customer's request during the contract term shall be covered. Any requests for unauthorised devices will be escalated to the designated Authorised Contact.

24. CUSTOMER DOCUMENTATION AND SERVICE REPORTING

24.1 The Company will produce a predefined standard set of reports describing the service provided to the Customer on a monthly basis.

24.2 Service review meetings are held monthly (or as otherwise agreed between the Company and the Customer) between the Company and the Authorised Contact. They provide a forum to discuss service achievements and issues. The review is chaired by the Company Account Manager and/or Service Delivery Manager and will require representation from the customer at an appropriately senior level.

24.3 The Company will use reasonable endeavours to provide the reports to all Authorised Contacts no later than 2 days before the service review meeting date.

25. SERVICE DELIVERY MANAGEMENT

25.1 The Service Delivery Manager (SDM) will maintain the operational relationship between the customer and the Company for contracted services, acting as the primary point of contact for service-related matters.

25.2 The Company will provide a named SDM responsible for managing the operational relationship with the customer and ensuring contracted services are delivered to agreed standards.

25.3 The SDM shall monitor and report on the performance of contracted services, ensuring delivery aligns with agreed-upon Service Level Agreements (SLAs) and proactively addresses any deviations.

25.4 The SDM shall coordinate the resolution of service issues, invoking hierarchical escalation procedures when necessary, and act as the Major Incident Manager when required.

25.5 Out of Scope

25.5.1 Service support not explicitly listed in the Order Form, including ad hoc consultancy or project-based activities.

25.5.2 Requests for custom reporting outside of the Company's standard reports for the Managed Service may incur additional charges.

25.5.3 Resolution delays caused by third-party vendors or service providers.

26. VIRTUAL IT DIRECTOR SERVICE

26.1 The Company's Virtual IT Director Service provides strategic IT leadership to organisations without the cost or commitment of a full-time IT Director. It is designed to provide a strategic overview of security, governance, and business alignment into IT operations.

26.2 The vITD acts as a senior advisor, engaging directly with board-level stakeholders to shape IT strategy, manage risk, and ensure compliance. It does not replace the Company's Technology Roadmap service, which is a paid consultancy piece of work.

26.3 In Scope.

26.3.1 Strategic IT Leadership: Board-level engagement to align IT with business goals and regulatory requirements.

26.3.2 Customer Advocacy: Acting on behalf of the customer to recommend solutions that meet business objectives.

26.3.3 Board-Level Reporting: Regular updates to senior leadership on IT performance, risks, and opportunities.

26.3.4 Technology Roadmap Ownership: Ongoing management of a Customer's strategic Technology Roadmap.

26.4 Out of Scope.

26.4.1 Technical Design Work: Architecture, engineering, and solution design

26.4.2 Project Delivery: Implementation of IT projects, migrations, or deployments

26.4.3 Reactive Support: Day-to-day troubleshooting and ServiceDesk services

26.4.4 Production of the Customer's Technology Roadmap

27. ONSITE SUPPORT

27.1 If an Incident or Request cannot be resolved remotely, at the sole discretion of the Company, it will be escalated to the Company's field engineering team for onsite resolution or to the Customer's third-party vendor or onsite team where appropriate.

27.2 Any incident or request requiring an on-site engineer for remediation will be handled during Business hours, Monday to Friday, 9 am – 5.30 pm. Support provided outside this timeframe may incur additional fees, which are available on request.

28. DEDICATED RESOURCE

28.1 A dedicated resource refers to personnel assigned exclusively to the Customer account or site to deliver managed services. These individuals operate as the Customer's internal IT team and are responsible for day-to-day service desk operations, ticket handling, and escalation management based on the engineering roles defined in the Order Form.

28.2 The Customer shall be solely responsible for ensuring that all dedicated resources assigned to perform services under this Agreement are fully inducted into all relevant Customer procedures, policies, and operational protocols prior to the commencement of any work. This includes, but is not limited to:

28.2.1 Health and Safety policies and procedures.

28.2.2 Site-specific safety requirements and emergency protocols.

28.2.3 Environmental compliance and sustainability practices.

28.2.4 Data protection and confidentiality obligations.

28.2.5 Code of conduct and behavioural expectations.

28.2.6 Any other procedures reasonably required by the Customer to ensure safe, lawful, and effective service delivery.

28.3 The Company shall provide dedicated personnel to be based at the Customer's designated location, operating Monday to Friday, based on the agreed hours in the Order Form.

28.3.1 **Holiday and sickness cover**

28.3.1.1 The Company shall provide holiday cover for the Dedicated Resource to ensure continuity of service. Cover shall be limited to the scope of responsibilities of the Dedicated Resource and shall not extend to additional duties unless agreed in advance.

28.3.1.2 Where a dedicated resource is off sick, the following shall apply.

(a) Single Dedicated Resource – Remote cover from the Company Shared Service Desk, dedicated cover provided by the next business day.

(b) Multi-Dedicated Resource – Remote cover from the Company Shared Service Desk, Dedicated cover provided within two business days.

28.4 The Dedicated Resources shall not be required to perform tasks outside the scope of the Managed Service as defined in the Order Form. This includes, but is not limited to.

28.4.1 Project work, infrastructure upgrades, or strategic IT planning

28.4.2 Support for unauthorised users, devices, or services not listed in the Order Form or approved by the Authorised Contact and the Company.

28.4.3 Vendor management and procurement shall be subject to the Company's explicit agreement in writing.

28.5 Any request to expand the responsibilities of the Dedicated Resource must be submitted through the Company's formal Change Management process and approved by the Company. The Company reserves the right to assess the impact, cost, and feasibility of such changes before implementation.

28.6 The Company and the Customer shall jointly monitor ticket volumes and SLA performance. If ticket volumes consistently exceed thresholds outlined in the order form, and/or recommendations have not been implemented to improve any part of the managed technology, leading to increased workload,

the Company may suggest adding further dedicated resources. Any such additions shall be subject to mutual agreement and a formal contract amendment. The Company reserves the right to suspend SLA targets if the volume of work surpasses the capacity of the dedicated resources.

28.7 The Customer agrees not to assign tasks to Dedicated Resources that fall outside the defined scope. The Company reserves the right to escalate any such requests to the Authorised Contact and to decline execution until a formal change request is approved.

28.8 **Change in Dedicated Resource**

28.8.1 The Company reserves the right to substitute, reassign, or replace any dedicated resource assigned to the Customer's location, provided that such substitution does not materially affect the quality or continuity of the services being delivered. The Company shall use reasonable efforts to ensure that any replacement resource possesses equivalent qualifications, experience, and capability to perform the required services. The Company will notify the Customer in advance of any such change and, where practicable, will consult with the Customer to ensure a smooth transition.

28.9 The Customer shall have the right to request a change in the dedicated resource personnel assigned by the Company to deliver services at the Customer's location. Such a request must be made in writing and include a reasonable justification, which may include but is not limited to concerns regarding performance, conduct, or compatibility with The Customer's team.

28.9.1 Upon receipt of a valid request, the Company shall review the matter in good faith and, where the request is deemed reasonable, will initiate the process of identifying and assigning a suitable replacement resource. The Company will use commercially reasonable efforts to complete the substitution within ten (10) business days, subject to resource availability and operational constraints.

28.9.2 The Company shall ensure that any replacement personnel possess qualifications and experience equivalent to or exceeding those of the outgoing resource and shall take steps to maintain continuity of service and minimise disruption during the transition. The Customer acknowledges that repeated or unreasonable requests for personnel changes may impact service delivery.

28.9.3 If any dedicated resource personnel is found to have engaged in gross misconduct, including, but not limited to, theft, fraud, harassment, violence, or a serious breach of confidentiality, the Company shall immediately remove the individual from the Customer's location and initiate disciplinary procedures in accordance with its internal policies. A replacement resource shall be assigned as soon as reasonably practicable. The Company reserves the right to provide equivalent cover from the shared service desk as an interim measure, and shall notify the Customer of the incident and the steps taken.

29. SOFTWARE

29.1 As part of the Managed Service, the Company may include licensed software services for all Authorised Devices or Users; any software supplied by the Company will be listed on the Order Form.

29.2 The Company reserves the right, at its sole discretion, to modify, substitute, or replace any software provided under this agreement with software of equivalent functionality and performance, without prior notice, provided that such replacement does not materially diminish the intended use or capabilities of the original software.

30. THIRD-PARTY DEPENDENCY

30.1 Where the Company is dependent on third parties outside of its direct control, the Customer recognises that the Response or Resolution Time may extend beyond the target. At all times in the provision of the service requirements, the Company shall keep the Customer informed when it becomes aware of potential delay beyond the Service Levels due to third-party dependency and seek assistance through management escalation as appropriate.

30.2 The Customer must maintain external support contracts with core specialist applications and software vendors, such as accounting software and other specialist line of business applications. The Company may not always provide user support, but will act as an intermediary when needed and will aim to manage the solution through the third-party contractor where possible.

31. CUSTOMER ONBOARDING

31.1.1 Customer onboarding will be required to commence the Managed Service. The onboarding schedule and onboarding costs will be discussed and agreed upon in the Order Form and with the Customer at commencement.

32. CUSTOMER OFFBOARDING

32.1.1 Customer offboarding will be required to remove the Managed Service. The offboarding schedule and offboarding costs will be discussed and agreed upon in the Order Form and with the Customer at commencement.

33. EXIT PLAN

33.1 The Company shall assist in migrating away from the Service following the expiry or termination of this Agreement for any reason. As a minimum, provided the account is fully paid up to and including the termination date, the Company shall supply a copy of all Customer Data, passwords specific to the Customer, and virtual machine images of dedicated servers.

33.2 The charges for this migration assistance and any additional services required by the Customer upon termination will be applied at a rate to be agreed upon by both parties at the time of termination, in accordance with the Change Control Procedure, using the Company's applicable rate at that time.

33.3 The parties agree in good faith to establish the Exit Plan and agree on their respective responsibilities and deliverables within 14 days of either party giving notice to terminate this Agreement. The responsibility for agreeing the Exit Plan lies with the Company Account Manager and the Authorised Contact.

33.3.1 Replacement Provider - The Customer shall ensure that the Replacement Provider makes available and provides suitably skilled resources for the timely and efficient handover of the services.

34. EXCLUSIONS

34.1.1 The Company reserve the right to exclude the following items:

34.1.1.1 Parts, equipment or software not covered by vendor/manufacturer warranty or support.

34.1.1.2 The cost of any parts, equipment, or shipping charges of any kind.

34.1.1.3 The cost includes any software, licensing, renewal, or upgrade fees of any kind.

34.1.1.4 The cost of any third-party vendor or manufacturer support, or incident fees of any kind.

34.1.1.5 The cost to bring the Customer environment up to the minimum standards required to provide the Services.

34.1.1.6 Service and repair made necessary by the alteration or modification of equipment other than that authorised by the Company, including alterations, software installations or modifications of equipment made by the Customer's employees or anyone other than the Company or its subcontractors.

34.1.1.7 Maintenance of applications/software packages, whether acquired from the Company or any other source, unless otherwise specified.

34.1.1.8 Software builds, operating system upgrades or data transfer for new desktops, laptops or servers introduced into the environment. These new systems can be covered under this agreement under the Change Control Procedure for an additional charge once they meet the minimum specification for this agreement.

34.1.1.9 Setting up any new hardware or virtual machines (including workstations and laptops) will be regarded as a project task and billed separately from this agreement.

34.1.1.10 Reconfiguring hardware, software or operating systems due to a change in the Customer requirements will be regarded as a project task and billed separately from this agreement.

34.1.1.11 Programming (modification of software code) and program (software) maintenance, unless specified.

34.1.1.12 Major network upgrades or projects.

34.1.1.13 ISP or carrier-related issues, if provided by a third-party service provider not contracted with by the Company.

34.1.1.14 Training services of any kind.

34.1.1.15 If the Customer's business continuity plan is activated, the Service Levels will be suspended until recovery actions are completed as agreed by the parties.

34.1.1.16 Any services not listed in the Order Form**.**

35. CUSTOMER RESPONSIBILITIES

35.1 Authorised User responsibility with the Service Desk

35.1.1 Users should provide as much detail as possible to the Service Desk when reporting the Incident or making the Request, including, where possible, the device Asset Tag Number, error messages, etc.

35.1.2 The User should assist the Service Desk and the Company staff in making themselves available to provide further information, respond to the Service Desk promptly whenever possible, and aid in incident resolution and testing of resolutions.

35.1.3 To assign the correct priority, the user must provide a realistic assessment of the Business Impact and Urgency. Overestimating these can lead to too many Incidents being assigned a high priority, which may result in genuine high-priority Incidents missing their targets.

35.1.4 The Company will attempt to contact the Authorised User three times by phone or email to progress an Incident or Request. Should the Authorised User not respond the Company will complete the ticket with the assumption that no further work is required.

35.2 Service Request Fulfilment

35.2.1 Requests should be logged by email/telephone/web with the Service Desk.

35.2.2 When appropriate, the Service Desk will send a request for further information or authorisation. This should be completed and returned as soon as possible, so as not to delay the fulfilment of the Request. The Service Request will be accepted once all information required to action the Request has been received.

35.3 Hardware and Software

35.3.1 It is the responsibility of the Customer to maintain appropriate Hardware or Software licenses or warranties on all Authorised Devices. Devices which are not covered by such warranties may be excluded.

35.3.2 The Customer shall be solely responsible for ensuring that all software installed, used, or accessed on any IT assets under this agreement is properly licensed and compliant with applicable software licence terms. This includes, but is not limited to:

35.3.2.1 Maintaining valid and current licences for all third-party and proprietary software.

35.3.2.2 Ensuring that software usage does not exceed the scope or limits of the licence agreements.

35.3.2.3 Providing the Company with accurate and timely information regarding software installations and licence entitlements.

35.3.2.4 Cooperating with any audits or compliance checks initiated by software vendors or the Company to verify license adherence.

35.3.3 The Company shall not be liable for any fines, penalties, or legal actions resulting from the Customer's failure to comply with software licensing requirements. In the event of non-compliance, the Customer agrees to indemnify and hold harmless the Company from any resulting claims or damages.

35.4 General

35.4.1 All users have a duty to exercise reasonable care and responsibility for the systems in accordance with the policies and procedures of the Customer.

35.4.2 It is not the responsibility of the Company under this agreement to manage vendor warranties for any equipment on the Customer's site that has not been supplied by the Company.

35.4.3 In the event of a hardware-related incident being logged against an item that is out of warranty, any part should be sourced by the Customer using the Company as required. At this point, the SLA may be paused. The Company may provide either a repair or replacement quotation for the faulty item (whichever is deemed most cost-effective), and related documentation or tickets will be raised as necessary.

36. HOLD HARMLESS CLAUSE

36.1 The Customer acknowledges that the Managed Services provided by the Company may include technical advice, security recommendations, and project proposals intended to enhance the Customer's IT infrastructure, data protection, and operational efficiency**.** The Customer agrees that.

36.1.1.1 **Advice Not Followed**: The Company shall not be liable for any loss, damage, or disruption resulting from the Customer's decision to ignore, delay, or partially implement any technical or security advice given.

36.1.1.2 **Unimplemented Recommendations and Projects**: The Customer accepts full responsibility for any consequences arising from the non-implementation, postponement, or alteration of recommended projects, upgrades, or security measures, regardless of the reason.

36.1.1.3 **Third-Party Dependencies**: **The Company** shall not be liable for any failures, delays, or damages caused by third-party vendors, software providers, or hardware manufacturers, including, but not limited to, incompatibility, service outages, or security vulnerabilities.

36.1.1.4 **Customer-Controlled Systems and Data**: The Customer is entirely responsible for managing, controlling access to, and securing its systems and data.

36.1.1.5 **Customer Policy and Actions:** The Company shall not be liable for any breaches, data loss, or unauthorised access that arise from the Customer's internal policies, personnel actions, or failure to implement adequate safeguards.

36.1.1.6 **Chargeable Work Summary:** If any issue, incident, or remedial action results from the customer's failure to follow advice, implement recommendations, or proceed with proposed projects, all related investigation, resolution, and support work undertaken by the Company shall be considered chargeable at the prevailing rates.

37. EMPLOYEE PROVISIONS

37.1 The parties intend and acknowledge that the commencement of the provision of the Managed Service by the Company shall not constitute a relevant TUPE transfer, and the regulations do not apply.

37.2 The Customer shall indemnify and keep indemnified the Company against any Employment Liabilities arising out of or in any way connected with the employment or termination of employment of any person who alleges that their employment should have or did transfer to the Company pursuant to the TUPE Regulations under this Agreement.

37.3 The Customer agrees that it shall not (except with the prior written consent of the Company) directly or indirectly solicit or entice away (or attempt to solicit or entice away) from the employment of the Company any person employed or engaged by the Company (whether or not in the provision of the Services) at any time during the Initial Term or for a further period of 12 months after the termination of this Agreement.

38. CONTRACT CHANGE CONTROL PROCEDURE

38.1 The Company and the Customer shall discuss any change to the Service by the other, and such discussion shall result in either a written request for a change by the Customer or a written recommendation for a change by the Company under the contract change control procedure.

39. CONTRACT CHANGE MANAGEMENT

39.1 Changes to services that are outside of normal service delivery are managed through the Change Control procedure and the Company Account Manager. To ensure sufficient time for implementing changes, the correct lead time for requesting a change must be provided. A change request procedure will be established, including lead times, following the implementation of the service levels in this document.

40. VARIATION

40.1 The Company may make minor amendments to these conditions at any time, and the Customer will be bound by any such changes from the date they are made. While the Company will endeavour to provide the Customer with updated versions, it is the Customer's responsibility to check the Company's website periodically for any modifications. The latest version of these conditions will be available at https://www.auratechnology.com/managed-it-terms (or at any other location notified by the Company). Posting these changes shall be considered sufficient notice of such minor changes to the Customer.

40.2 Material Changes to the terms will be provided in writing to the Customer Authorised Contact seven working days before the terms come into effect.