Telair Managed IT Services

SERVICE SCHEDULE

Contents

1. Purpose

This Service Schedule defines how Telair delivers Managed IT Services, including the scope of coverage, service levels, inclusions, exclusions, responsibilities, billing rules, and operational requirements. It forms part of the Telair Managed IT Services Master Services Agreement (MSA). Where the MSA sets legal terms, this document describes how the service operates in practice.

Where this Service Schedule and the Customer's accepted Quote conflict, the Quote prevails with respect to scope, pricing, quantities, and term. Where this Service Schedule and the MSA conflict, the MSA prevails.

---

2. Service Delivery Model

Telair delivers Managed IT Services using a **per user support model**, supported by optional device, infrastructure, and 24×7 emergency coverage add-ons. All individuals accessing Customer systems must be assigned to a supported user type. Devices and infrastructure components may require additional add-on coverage for patching, security, monitoring, and support.

All users within the Customer organisation must be covered under a Telair Managed IT support plan. Partial coverage is not permitted.

Services are delivered remotely wherever possible, with onsite attendance provided when remote remediation is not feasible.

Commercial pricing for each user type, device plan, and infrastructure tier is defined solely in the Customer's accepted Quote. Internal Telair pricing schedules may be used to prepare quotes but do not form part of this Agreement unless explicitly provided to the Customer.

---

3. User Support Plans

This section defines the support provided to each user category. Each plan is available with Business Hours support, with optional 24×7 Emergency Support where purchased.

Each plan includes inclusions, exclusions, purpose, and coverage behaviour.

The inclusions and exclusions below define the scope of each User Support Plan. Work outside that scope, including projects, new deployments, and major changes, is excluded unless separately scoped and approved.

3.1 Standard User Support

Inclusions:

- Support for one user and their assigned primary workstation
- Remote troubleshooting and incident response
- Operating system and application patching
- Antivirus/EDR monitoring and management
- Microsoft 365 or Google Workspace administration (identity, MFA, licensing, mailbox configuration, password resets)
- Endpoint security configuration and monitoring
- Routine support of endpoints already enrolled in a supported endpoint management platform, including device sync/status checks, policy/application issue triage, and basic remediation within the Customer's existing configuration or Telair standard baseline.
- Device health, patch, and security posture monitoring where supported by Telair tools or a supported endpoint management platform.

Exclusions:

- Support for additional devices unless covered by an add-on
- Initial deployment, migration, architecture design, application packaging, device enrolment frameworks, Autopilot / DEP / ABM configuration, compliance framework design, and major reconfiguration of Intune, JAMF, or other UEM platforms are excluded unless separately scoped and approved.
- Advanced security or compliance configuration (scoped separately)
- Application-specific support outside standard productivity suites and ordinary endpoint access troubleshooting, including line-of-business applications, specialist software, integrations, data issues, workflow design, and vendor-specific administration, unless separately scoped

Purpose: Designed for users with a dedicated workstation requiring full support of identity, productivity suites, and endpoint security.

Coverage Behaviour: Business Hours users receive full support during standard hours. 24×7 Emergency Support users receive after-hours assistance for Severity 1–2 incidents such as outages, authentication failures, or severe degradation; routine issues are addressed during Business Hours. Each Standard User plan includes support for **one named user and one primary workstation**. Any additional workstations or endpoints used by that user must be covered under an **Additional Workstation Support** plan or other applicable device add-on.

3.2 Frontline User Support

Inclusions:

- Identity and access support, including MFA
- Login assistance and password resets
- Account administration
- Basic application support for approved frontline workflows, limited to access issues, login failures, basic configuration checks, and first-line triage for mobile, shared, kiosk, warehouse, or POS use cases

Exclusions:

- Dedicated workstation support
- Complex software troubleshooting unrelated to frontline workflows
- Support for shared devices unless a Shared Workstation Support plan is in place
- Line-of-business application administration, data correction, workflow design, reporting, integrations, or vendor-specific application support unless separately scoped

Purpose: Designed for users who access business systems without a dedicated workstation, such as mobile, frontline, warehouse, or POS staff.

Coverage Behaviour: Business Hours coverage provides support during standard hours. 24×7 Emergency Support enables urgent after-hours assistance for Severity 1–2 access-blocking incidents affecting frontline users, such as critical authentication failures or inability to access approved frontline applications required for live operations. Non-urgent matters queue for Business Hours. Frontline Users are not assigned a dedicated workstation under this plan. Where a shared device is used regularly by multiple frontline staff and requires patching, security, or support, it must be covered under a Shared Workstation Support plan.

3.3 Email-Only User Support

Inclusions:

- Mailbox access support, including webmail access and basic supported mail client setup
- MFA assistance and identity verification
- Mailbox configuration, alias/forwarding adjustments, and licensing administration

Exclusions:

- Device support of any kind, including workstation, mobile device, printer, network, or operating system issues

- Local mail client troubleshooting beyond basic account setup, including Outlook profile rebuilds, OST/PST issues, add-ins, unsupported third-party mail clients, or endpoint-based sync problems
- Support for non-email applications or line-of-business systems

Purpose: Suitable for users who only require email and identity support without supported device coverage, such as contractors, casual users, or low-utilisation roles.

Coverage Behaviour: Business Hours coverage handles standard support needs. 24×7 Emergency Support applies only to urgent mailbox access issues such as MFA lockouts, authentication failures, or mail flow issues materially affecting business continuity. This plan does not include support for any workstation, mobile device, shared device, or broader endpoint troubleshooting. Where a device requires support, it must be covered under the appropriate user and device combination defined elsewhere in this Service Schedule.

4. Device Coverage Plans

Device Coverage Plans provide patching, monitoring, security management, and support for Customer devices. Support under this section is billed **per covered device** in accordance with the Customer's accepted Quote. Devices must be listed in Telair's Site Summary or asset register for coverage and billing to apply. Each plan is available with Business Hours support, with optional 24×7 Emergency Support where purchased.

The inclusions and exclusions below define the scope of each Device Coverage Plan. Work outside that scope, including projects, new deployments, and major changes, is excluded unless separately scoped and approved.

4.1 Additional Workstation Support

Inclusions:

- Support for an additional workstation assigned to a Standard User
- Operating system and application patching
- Antivirus/EDR administration, including deployment where required, health monitoring, update/status management, policy application within Telair's standard baseline, and response to ordinary detections or quarantine events
- Remote troubleshooting and configuration adjustments
- Performance and health monitoring

Exclusions:

- Onsite new device builds
- Complex application support outside standard productivity suites

- Shared device support (requires Shared Workstation plan)
- Managed detection and response (MDR), threat hunting, forensic investigation, incident response retainers, or advanced security remediation unless separately scoped or purchased

Purpose: For users with more than one workstation that requires full patching, protection, and troubleshooting coverage.

Coverage Behaviour: Business Hours users receive full support during standard hours. 24×7 Emergency Support users receive after-hours assistance for critical workstation failures that prevent essential work.

4.2 Shared Workstation Support

Shared Workstation Support applies only to devices not assigned to a single dedicated user. Devices used primarily by one individual must be covered under Additional Workstation Support.

Inclusions:

- Patch management and firmware updates
- Antivirus/EDR administration, including deployment where required, health monitoring, update/status management, policy application within Telair's standard baseline, and response to ordinary detections or quarantine events
- Remote troubleshooting for shared-use devices
- Monitoring of resource utilisation and performance

Exclusions:

- Dedicated user workspace configuration
- Support for personalisation features or multi-profile OS designs

Purpose: Designed for devices used by multiple individuals, such as shift workers, warehouse teams, or frontline staff using common terminals.

Coverage Behaviour: Business Hours support applies during standard hours. 24×7 Emergency Support covers critical device failures affecting essential frontline workflows.

4.3 Peripheral Support

Applicability: Peripheral support applies to all Customer sites. The level of support depends on whether the site is covered under the base best effort service or a paid Peripheral Support Add-on (Small Site or Large/Complex Site). All supported peripherals must be listed in the Customer's asset register or Site Summary for coverage to apply.

Telair does not guarantee that all peripheral devices can be fully supported due to vendor variability, driver limitations, legacy devices, or unsupported hardware.

4.3.1 Included Best Effort Peripheral Support (Base Level)

Included for all Managed IT Customers at no additional charge.

Inclusions:

- Best effort troubleshooting for standard peripherals (printers, scanners, displays, EFTPOS, signage)
- Basic connectivity and driver assistance (where supported)
- Limited vendor engagement (reasonable effort to assist with lodging warranty or support cases)
- Basic configuration help for simple devices

Exclusions:

- SLA backed response or resolution times
- Onsite attendance for peripheral issues
- Physical repair, replacement, or hardware servicing
- Support for large peripheral fleets (>10 devices) unless covered by an add-on
- Support for critical, regulated, or specialised peripherals without an add-on
- Guaranteed support for legacy, unsupported, or consumer grade peripherals

Purpose: Provides general assistance for common peripherals without creating SLA liability or operational overhead.

4.3.2 Peripheral Support Add-on – Small Site

For sites with **up to 5 supported peripherals**, requiring higher reliability or more frequent support.

Inclusions:

- Prioritised Business Hours troubleshooting
- Remote triage and deeper diagnostic assistance
- Support for print queues, drivers, and basic integration (e.g., print server)
- Reasonable Business Hours vendor engagement for diagnosed faults, including assistance with support cases, warranty coordination, log collection, and configuration checks where appropriate

Exclusions:

- 24×7 emergency support
- Hardware repair or installation
- Critical/regulated devices (requires Large/Complex Add-on)

Purpose: Enhances support for smaller sites with moderate usage of printers, scanners, EFTPOS, or signage.

4.3.3 Peripheral Support Add-on – Large/Complex Site

For environments with 6 or more peripherals, high business dependence, or complex device types (POS networks, retail floor devices, industrial scanners, etc.).

Inclusions:

- Enhanced Business Hours prioritisation
- Support for fleet scale or business critical peripherals
- Assistance with device rollout, configuration standards, and ongoing maintenance
- Multi-vendor coordination for complex environments

Exclusions:

- Regulated or industry certified medical equipment (requires separate scope)
- Guaranteed performance levels without an agreed SLA
- After-hours support unless billed at SBR

Purpose: Provides robust support for high volume or high complexity peripheral environments.

4.3.4 Peripheral Listing Requirements

For any paid peripheral support tier, **devices must be listed** in Telair's Site Summary or Asset Register. Coverage applies only to listed peripherals.

Unlisted peripherals receive base best-effort support only.

4.3.5 Coverage Behaviour

- All peripheral support (base or add-on) is provided during Business Hours only.
- 24×7 Emergency Support does **not** apply to peripherals.
- Onsite attendance for peripheral-only issues is always billable at SBR unless explicitly included in a scoped engagement or Quote.

---

5. Server & Infrastructure Support

This section provides formal support definitions for servers and hypervisors. Each support category is available with Business Hours support, with optional 24×7 Emergency Support where purchased. Support under this section is billed per server and per hypervisor host, as reflected in the Customer's accepted Quote. Only listed

servers and hosts are covered; unlisted or legacy systems may be supported on a best-effort or SBR basis at Telair's discretion.

The inclusions and exclusions below define the scope of each Server and Infrastructure Support category. Work outside that scope, including projects, new deployments, major changes, and platform expansion or redesign activities, is excluded unless separately scoped and approved.

5.1 Server Support

Inclusions:

- Monitoring of CPU, memory, disk utilisation, RAID status, and operating system event logs
- Operating system patching, security updates, and routine maintenance
- Remediation of system-level issues affecting performance or stability
- Routine administration and support of Active Directory roles, file/print services, authentication services, and core OS components within the existing supported design
- Coordination with hypervisor hosts (VMware/Hyper-V/Proxmox) for resource-related issues
- Server operating system administration, including local policy management, agent health, antivirus/EDR administration, service health checks, and routine configuration maintenance within the existing supported design

Exclusions:

- Application server tuning (SQL Server, line-of-business apps, custom workloads)
- Unsupported or end-of-life server operating systems
- Server rebuilds, migrations, or major version upgrades (scoped separately)
- Backup platform design, restore testing, retention architecture, disaster recovery orchestration, and business continuity planning unless expressly included in the Customer's accepted Quote

Purpose: To maintain stable, secure, and performant server environments that support user authentication, file access, critical business services, and workloads.

Coverage Behaviour: BH includes routine troubleshooting and scheduled maintenance. 24×7 extends support to urgent faults including outages, authentication failures, critical services failing, or storage faults impacting business continuity.

5.2 Hypervisor Support

Hypervisor hosts are billed where they are in service and supported by Telair, regardless of whether workloads are actively running at a given time.

Inclusions:

- Monitoring of host resource utilisation, including CPU, memory, storage, and datastore capacity where supported
- Hypervisor patching and routine host maintenance where supported
- Troubleshooting host-level performance, availability, and connectivity issues
- Routine guest lifecycle administration limited to standard start, stop, restart, and basic resource adjustment tasks within the existing supported design
- Vendor escalation for hypervisor faults

Exclusions:

- Creation of new virtual machines, template builds, or thin provisioning design
- Complex hypervisor clustering, including HA, DRS, stretched clusters, or cluster architecture changes
- Storage architecture, storage policies, multipathing, advanced datastore management, storage I/O tuning, or SAN consulting
- Hypervisor migrations, cross-platform conversions, or major version upgrades
- Capacity planning, redesign, or platform expansion projects

Purpose: To provide foundational support for supported virtualisation platforms, including VMware, Hyper-V, and Proxmox, where they host Customer workloads.

Coverage Behaviour: Business Hours support covers routine host maintenance, performance investigation, and standard guest administration. 24×7 Emergency Support applies to critical host failures or severe degradation impacting supported server availability.

---

6. Network & Infrastructure Device Support

Infrastructure support is offered per device, with Business Hours or optional 24×7 Emergency Support. Firewall supply, licensing, and configuration bundles may also be provided where expressly included in the Customer's accepted Quote. Each firewall, router, switch, and wireless access point supported under this section is billed per device and per tier or service category in accordance with the Customer's accepted Quote. Devices must be recorded in Telair's Site Summary or asset register; otherwise, support may be declined or billed at SBR.

6.1 Firewall Supply, Licensing & Configuration Bundles

6.1.1 Sophos Firewall ALP Bundle

The Sophos Firewall ALP Bundle is a quoted firewall supply, licensing, and configuration bundle. It is not an ongoing managed firewall support plan. Where purchased under a Managed IT Services arrangement, it is provided only where expressly included in the Customer's accepted Quote. The applicable firewall model, licence type, licence term, configuration scope, and professional services allowance are defined in the Customer's accepted Quote. Sophos licensing and any other third-party components included in the ALP Bundle are subject to supplier terms and supplier-imposed price changes, which may be passed through in accordance with the MSA.

Inclusions:

- Supply of the Sophos firewall hardware specified in the Customer's accepted Quote
- Sophos firewall licensing as specified in the Customer's accepted Quote, including Standard Protection or Xstream Protection where applicable
- Professional services for initial firewall configuration based on the agreed scope
- Basic handover of configured firewall settings relevant to ongoing support

Exclusions:

- Onsite installation, cabling, rack mounting, physical deployment, or site attendance unless separately quoted
- Structured cabling, electrical work, wall mounting, or physical works requiring a licensed trade
- Network redesign, complex migration, rulebase restructuring, segmentation redesign, or security hardening beyond the agreed configuration scope
- Configuration of services, devices, or third-party systems not included in the Customer's accepted Quote
- Ongoing firewall monitoring, maintenance, firmware updates, policy administration, or support unless the firewall is covered under an applicable Firewall Support plan in the Customer's accepted Quote

Purpose: To provide a bundled option for supplying, licensing, and initially configuring a Sophos firewall under a defined Quote.

Coverage Behaviour: ALP Bundle activities are delivered as quoted hardware, licensing, and professional services. Where the Customer also purchases Managed Firewall Support, ongoing monitoring, maintenance, firmware updates, policy administration, and support are provided under the applicable Firewall Support tier in Section 6.2.

6.2 Firewall Support (Basic, Standard, Advanced)

Firewall support is delivered under three tiers reflecting device complexity and Customer security requirements.

6.2.1 Basic Firewall Support

Inclusions:

- Monitoring of firewall uptime and connectivity status
- Internal visibility to Telair of basic device health and availability alerts where supported by the firewall platform and monitoring tools
- Light configuration adjustments (e.g., IP, static routes, basic NAT)
- Notification and escalation of detected outages or faults

Exclusions:

- Firmware updates or patching
- Configuration backup or restoration
- Policy/rule management beyond basic NAT or routing
- IDS/IPS or advanced threat tuning
- Vendor liaison or deep troubleshooting

Purpose: For low complexity sites or Customer managed environments. Telair provides awareness and light config only; the Customer manages security posture.

Coverage Behaviour: Business Hours support covers monitoring and assistance. 24×7 Customers receive after-hours support for critical faults disrupting site connectivity.

6.2.2 Standard Firewall Support

Inclusions:

- Firmware/security updates
- Security policy and rule administration
- Routine firewall configuration changes and optimisation within the existing design, including ordinary adds, moves, and changes such as rule updates, NAT changes, address object updates, VPN peer adjustments, and standard policy maintenance
- Regular configuration backups and restoration
- Threat/event monitoring (including IDS/IPS where supported)
- Vendor liaison for incident remediation
- Proactive health/performance monitoring

Exclusions:

- HA, multi-WAN, or SDWAN support
- Firewall redesign, including rulebase restructuring, segmentation changes, addressing changes, WAN topology changes, migration projects, or hardening projects beyond ordinary operational administration (scoped separately)

Purpose: Suitable for business environments requiring ongoing management of security policy, firmware, and performance.

Coverage Behaviour: BH covers routine changes, alerts, and maintenance. 24×7 expands coverage to urgent disruptions or threat events outside Business Hours.

6.2.3 Advanced Firewall Support

Inclusions:

- All inclusions from Standard Firewall Support
- HA pairs, multi-WAN, or SDWAN environments
- Complex policy administration and optimisation within the existing supported architecture
- Security compliance alignment and audit assistance
- Integration with identity/cloud/security systems
- Detailed change control and documentation
- Multivendor/third-party coordination

Exclusions:

- Major firewall redesigns, re-architecture, vendor migration projects, or large-scale security transformation work beyond ongoing operational administration (quoted separately)

Purpose: For multisite or mission critical networks where the firewall forms the core of the infrastructure.

Coverage Behaviour: BH support covers ongoing management; 24×7 support includes urgent assistance for high impact security or availability incidents.

6.2.4 Firmware Updates (BH vs 24×7)

- Business Hours: Firmware updates occur during BH unless safe for unattended after-hours execution. Updates requiring monitoring or downtime coordination occur in BH unless quoted separately.
- **24×7:** Firmware updates may be scheduled after hours at no additional cost.

6.3 Router Support

Router support covers edge routing devices used for WAN, VPN, or SDWAN adjacent functionality.

Inclusions:

- WAN routing configuration
- VPN setup and troubleshooting
- Firmware updates and basic routing optimisation within the existing supported design
- Basic device health, interface status, and connectivity monitoring where supported
- WAN failover testing (where supported)

Exclusions:

- SD-WAN orchestration, unless covered under Advanced Firewall Support or a separately scoped SD-WAN service
- Carrier managed router configuration beyond Customer interfaces
- Complex BGP/MPLS design changes

Purpose: Provides configuration, maintenance, and troubleshooting support for Customer routing equipment used for WAN, internet, and VPN connectivity.

Coverage Behaviour: BH covers routing adjustments and routine troubleshooting. 24×7 covers urgent WAN or VPN failures affecting business operations.

6.4 Unmanaged Switch Support

Unmanaged switches have limited visibility and no meaningful configuration interface, so support is provided on a best-effort basis only.

Inclusions:

- Basic connectivity troubleshooting
- Link and port status checks where physically or operationally observable
- Remote power cycling where supported by an upstream controllable power source or PDU

Exclusions:

- VLAN, trunking, QoS, STP/RSTP, or any managed switching features
- Firmware administration, configuration backup, or restore
- Performance diagnostics beyond basic connectivity confirmation
- Network redesign or remediation of environments dependent on unmanaged switching

Purpose: Supports basic diagnostics for unmanaged switches used in low-complexity or non-critical roles.

Coverage Behaviour: Business Hours support provides best-effort diagnostics only. 24×7 Emergency Support applies only to critical connectivity outages where the unmanaged switch is a covered device and remote diagnosis is possible.

6.5 Managed Switch Support

Managed switches provide enhanced monitoring and configuration capabilities.

Inclusions:

- VLAN/tagging/trunking configuration
- STP/RSTP configuration and troubleshooting
- Firmware updates
- Configuration backup and restoration
- Port monitoring and performance diagnostics

Exclusions:

- Full network redesign or re-architecture
- Multi-site L2 topology design
- Complex campus switching architecture, switch stack redesign, spanning-tree redesign, NAC deployment, QoS design, multicast design, or major segmentation projects
- Fibre uplink remediation, optics compatibility work, or structured cabling faults

Purpose: Ensures stable and secure switching across business networks where segmentation and performance matter.

Coverage Behaviour: BH support covers configuration and routine issues. 24×7 applies to major LAN disruptions or switch failures.

6.6 Wireless Access Point and Controller Support

Wireless support includes configuration, performance tuning, and troubleshooting for supported wireless access point environments.

Inclusions:

- SSID creation/modification
- Wireless security configuration
- Firmware updates
- RF optimisation and channel planning
- Troubleshooting interference, roaming, and coverage

- Administration and troubleshooting of supported controller-based or standalone wireless platforms, including cloud-managed platforms where the controller function is integral to the supported wireless solution

Exclusions:

- Wireless heat-mapping or large-scale RF design (scoped separately)
- Mesh network design beyond vendor defaults
- Guest portal customisation, captive portal development, or broader wireless/network access architecture changes unless separately scoped
- Wireless onboarding workflows, voucher systems, NAC, identity-based access control, PPSK design, or broader access control architecture unless separately scoped

Purpose: Maintains stable, secure wireless connectivity across office or site environments.

Coverage Behaviour: BH provides configuration and troubleshooting. 24×7 provides urgent assistance where wireless outages critically impact operations.

---

7. Supported Environment Requirements

This section defines the minimum technical standards required for Telair to deliver Managed IT Services reliably and safely. These requirements ensure systems are supportable, secure, and compatible with Telair's monitoring, management, and security tooling. Environments not meeting these standards may fall outside SLA targets or require remediation. Where a supported system fails to meet the minimum standards in this Section, Telair may suspend or limit support until remediation is completed. Required remediation will be quoted separately.

7.1 Operating System, Firmware & Software Standards

Inclusions / Requirements:

- All servers, workstations, network devices, and firewalls must run vendor supported operating systems and firmware.
- Security patches must be installable and supported by the vendor.
- Devices must not be end-of-life (EOL) or end-of-support (EOS).
- Productivity suite versions (Microsoft 365 / Google Workspace) must be current and licensed.

Exclusions:

- Legacy operating systems, including Windows 7/8, Windows Server 2008/2012, Windows versions prior to Windows 10, and macOS versions earlier than v12 (Monterey), where outside vendor support.
- Unsupported firewall or router models.
- Devices with locked down, unmanageable firmware.
- Windows Home is **not** supported.

Purpose: To ensure security, compatibility, and the ability to provide reliable support.

7.2 Hardware Requirements

Inclusions / Requirements:

- Devices must meet minimum performance thresholds for CPU, memory, and storage health.
- Servers must have supported RAID/storage configurations.
- Servers must have supported baseboard management capability, such as iLO or iDRAC.
- Network devices must support modern management protocols.
- Replacement parts should be available from the manufacturer.

Exclusions:

- Grey market, white-box, consumer-grade, or hardware lacking supported manufacturer warranty, firmware, or enterprise support channels.
- Faulty, unstable, or intermittently failing devices.

Purpose: Supportability and uptime rely heavily on hardware stability and availability of replacement components.

7.3 Security Controls

Required Controls:

- MFA must be enabled for all supported accounts.
- Telair-approved or otherwise agreed AV/EDR must be installed and active.
- Supported firewall and network security controls must be in place.
- Adequate password policies must be enforced (length, complexity, expiry, lockout rules).
- Patching must not be deferred or disabled.

Exclusions:

- Environments using unsupported or unmanaged antivirus/EDR products.
- Systems where MFA or basic security controls cannot be applied due to third-party constraints.

Purpose: To maintain baseline security and reduce operational risk.

7.4 Monitoring & Management Agents

Requirements:

- Telair monitoring, RMM, and security agents must be installed and remain active.
- Customers must not disable, interfere with, or remove agents.
- Devices must maintain stable connectivity to monitoring endpoints.
- Where reasonably required to deliver monitoring, remote access, or diagnostic capability, Telair may deploy approved site-based management or monitoring appliances at the Customer site, subject to the Customer's approval and the Customer's accepted Quote.

Exclusions:

- Devices without agent support (e.g., thin clients, unsupported OS versions).

Purpose: Without monitoring and RMM agents, Telair cannot deliver proactive maintenance or alert response.

7.5 Network Infrastructure Stability

Requirements:

- A stable switching and routing environment is required.
- Wireless networks must provide adequate coverage and signal quality.
- LAN/WAN segmentation must be correctly configured.
- DHCP, DNS, and gateway availability must be reliable.

Exclusions:

- Environments materially dependent on unmanaged, consumer-grade, or daisy-chained switching infrastructure in place of appropriate managed network infrastructure.
- Environments with chronic latency, packet loss, or channel congestion.

Purpose: Ensures Telair can deliver reliable remote support and maintain endpoint performance.

7.6 Internet Reliability

Requirements:

- Stable internet connectivity is required for cloud platforms, monitoring, support tools, and remote access.
- Sites must maintain adequate upload and download performance.
- Cellular failover or redundant links recommended for critical environments.

Exclusions:

- Sites with unstable or intermittent connectivity.
- Environments where Telair cannot maintain remote access due to ISP or Customer restrictions.

Purpose: Managed IT relies on internet availability for most support functions.

7.7 Change Management & Configuration Control

Requirements:

- Customers must notify Telair of planned changes in advance.
- No unauthorised changes may be made to Telair managed devices or configurations.
- Customer staff must not install unmanaged software or hardware without approval.

Exclusions:

- Post-change break/fix work caused by unapproved modifications.

Purpose: Prevents configuration drift, instability, and unexpected outages.

---

8. Cloud, SaaS & Tenancy Administration

Applicability: Tenancy administration applies to all supported users and Customer environments where Telair manages identities, mailboxes, licensing, authentication, or collaboration settings. These functions are not standalone services and form part of the standard deliverables across all user support plans. Behaviour under Business Hours and 24×7 Emergency Support applies consistently across all tenancy operations. This section defines the scope, inclusions, exclusions, and operational expectations for Telair's management of Microsoft 365, Google Workspace, and supported SaaS environments. These services support identity, access, licensing, baseline security, and core configuration tasks.

The inclusions and exclusions below define the scope of Telair’s Cloud, SaaS, and Tenancy Administration services. Work outside that scope, including projects, migrations, major changes, and advanced configuration or governance activities, is excluded unless separately scoped and approved.

8.1 Inclusions

User Lifecycle Administration:

- Creation, modification, and deactivation of user accounts
- Password resets, MFA resets, and authentication troubleshooting
- Profile updates and basic identity changes
- Routine administration of supported device objects and baseline endpoint management settings where the Customer already uses a supported UEM platform and the work remains within Telair's standard baseline.

Mailbox & Collaboration Administration:

- Mailbox creation and configuration
- Shared mailbox creation and permissions
- Distribution lists, groups, and basic Microsoft 365 Teams/SharePoint access adjustments within existing teams, groups, libraries, and sites
- Mail flow rules limited to basic routing or redirection tasks

Licensing & Subscription Management:

- Assignment and removal of licences
- Advising on licence utilisation and general optimisation opportunities
- Monitoring of licence counts for billing alignment

Security Baseline Activities:

- Enforcing standard policies such as MFA requirements
- Conditional Access configuration when within the standard Telair baseline
- Basic threat review using built-in dashboards (where part of Customer tenancy)

General Tenancy Maintenance:

- Monitoring of tenancy health alerts
- Basic auditing and review of service status (Exchange, OneDrive, Teams, Workspace services)
- Applying standard Microsoft/Google recommendations where non-disruptive

8.2 Exclusions

The following fall outside standard management and require separate scoping:

- Advanced Conditional Access and granular identity policy design
- Zero Trust frameworks or enterprise security architecture
- Advanced Intune, JAMF, or other UEM architecture, enrolment design, compliance framework design, application packaging, Autopilot / DEP / ABM implementation, or major policy reconfiguration
- Advanced Exchange, SharePoint, OneDrive, or Teams governance
- Multi-tenant migrations or consolidation projects

- SSO/identity integration with third-party identity providers
- SaaS application configuration (e.g. Xero, Salesforce, HubSpot, MYOB)
- Backup of SaaS data (requires SaaS Backup Add-On)
- Retention policies, retention labels, archiving policy design, legal hold, eDiscovery, and broader compliance or governance configuration
- Encryption key management or BYOK implementation
- Structural redesign of Teams, SharePoint, sites, libraries, permission models, or information architecture, and large-scale permissions remediation

8.3 Purpose

To provide consistent, reliable, secure administration of core productivity platforms used by supported users, ensuring identity integrity, access continuity, and appropriate licensing alignment.

8.4 Coverage Behaviour (BH vs 24×7)

- **Business Hours:** All tenancy administration and routine tasks occur during Business Hours.
- **24×7 Emergency Support:** After-hours assistance applies **only** to urgent access blocking incidents such as MFA failures, locked accounts preventing critical operations, or mail flow interruptions impacting business continuity.
- Routine provisioning, configuration, or licensing tasks are handled during Business Hours.

8.5 Customer Responsibilities

- Maintaining valid and sufficient licences for users and services
- Providing timely notification of staff changes (new starters, terminations)
- Ensuring third-party SaaS applications are supported by appropriate vendor licences
- Ensuring MFA devices are available to users during support interactions

8.6 Limitations

- Telair is not responsible for outages within Microsoft or Google platforms
- Changes to global security settings may require Customer approval
- Large-scale permission changes or structural reorganisation of teams, groups, or sites require scoping
- Third-party integrations (line-of-business apps, CRM/ERP systems) must be supported by those vendors

8.7 SaaS Backup Add-On

Applicability: The SaaS Backup Add-On is an optional service applied per protected user or mailbox, as set out in the Customer's accepted Quote. It is not included in standard user support plans by default.

Inclusions:

- Scheduled backup of supported Microsoft 365 and/or Google Workspace services (e.g., Exchange Online/Gmail, OneDrive/Drive, SharePoint, Teams) to a third-party backup platform
- Monitoring of backup job success/failure
- Basic retention policy configuration in line with vendor capabilities

Exclusions:

- RPO/RTO guarantees beyond backup vendor capabilities
- Backup of unsanctioned or unsupported SaaS platforms
- Long-term archival or legal hold configuration (beyond what the backup vendor natively provides)
- End-user self-service restore training or administration (unless separately scoped)
- DR design or business continuity planning (handled under projects or SBR)
- Validation of restored business data, application-level reconciliation, or multiple iterative restore exercises unless separately scoped

Purpose: To provide an additional layer of recoverability for cloud-based productivity data, supplementing (but not replacing) native retention features in Microsoft 365 or Google Workspace.

Backup success and retention are subject to the third-party backup vendor's platform capabilities. Telair does not warrant data recoverability beyond the vendor's stated guarantees.

8.8 Managed Workstation Backup

Applicability: The Managed Workstation Backup service is an optional add-on applied per protected workstation, as set out in the Customer's accepted Quote. It is not included in standard user or device support plans by default. This service provides managed endpoint backup to an approved offsite backup platform.

Inclusions:

- Deployment and configuration of the approved workstation backup agent
- Monitoring of backup job success/failure and agent health

- Backup management and routine backup issue triage
- Capacity and status reporting
- Offsite backup storage to Telair's approved secure data centre or backup platform
- Included protected storage allowance per covered workstation, as defined in the Customer's accepted Quote
- Initiation and coordination of restore requests for protected workstation backup data, where the requested data is available within the backup platform

Exclusions:

- Backup of unsupported devices, operating systems, or storage targets
- Backup of personal devices not covered under a Telair support plan or Quote
- Disaster recovery planning, business continuity planning, or full device rebuild services
- Validation of restored business data, application-level reconciliation, or multiple iterative restore exercises unless separately scoped
- Guaranteed RPO/RTO beyond the backup platform's native capabilities
- Recovery of data not successfully captured by the backup platform
- Backup of unsanctioned applications, external services, or storage locations not supported by the backup platform
- End-user self-service restore training or administration unless separately scoped

Purpose: To provide managed workstation backup, monitoring, and offsite storage for supported endpoints, improving recoverability of user data and device-level content.

Coverage Behaviour: Backup monitoring and administration occur during Business Hours. Restore requests are coordinated during Business Hours unless separately scoped as emergency recovery work and approved at applicable SBR.

Limitations: Backup success, retention, and recoverability are subject to the capabilities and limitations of the approved backup platform. Additional storage charges apply where protected storage exceeds the included allowance defined in the Customer's accepted Quote.

8.9 Managed Server Cloud Backup

Applicability: The Managed Server Cloud Backup service is an optional add-on applied per protected server, as set out in the Customer's accepted Quote. It is not included in standard Server Support by default. This service provides managed server backup to an approved cloud or offsite backup platform.

Inclusions:

- Deployment and configuration of the approved server backup agent or backup job
- Monitoring of backup job success/failure, repository health, and agent/job status
- Backup management and routine backup issue triage
- Offsite or cloud backup storage to Telair's approved secure backup platform
- Included protected storage allowance per covered server, as defined in the Customer's accepted Quote
- Initiation and coordination of restore requests for protected server backup data, where the requested data is available within the backup platform
- Capacity and status reporting

Exclusions:

- Backup architecture design, disaster recovery orchestration, or business continuity planning unless separately scoped
- Recovery testing, DR simulations, or restore rehearsal exercises unless separately scoped
- Application-level reconciliation, database consistency validation, or line-of-business recovery workflow validation unless separately scoped
- Guaranteed RPO/RTO beyond the backup platform's native capabilities
- Recovery of data not successfully captured by the backup platform
- Backup of unsupported operating systems, applications, appliances, or storage targets
- Backup of Customer-managed systems not listed in the Customer's accepted Quote
- Multiple iterative restores, migration use, or tenant/server relocation use unless separately scoped

Purpose: To provide managed server backup, monitoring, and offsite/cloud storage for supported server workloads, supplementing but not replacing broader disaster recovery or business continuity arrangements.

Coverage Behaviour: Backup monitoring and administration occur during Business Hours. Restore requests are coordinated during Business Hours unless separately scoped as emergency recovery work and approved at applicable SBR.

Limitations: Backup success, retention, and recoverability are subject to the capabilities and limitations of the approved backup platform. Additional storage charges apply where protected storage exceeds the included allowance defined in the Customer's accepted Quote.

8.10 DNS Hosting

Applicability: DNS Hosting is an optional hosted service provided under the applicable plan specified in the Customer's accepted Quote. The purchased plan defines the applicable feature set, entitlements, and service limits.

Inclusions:

- Provision of hosted DNS services on Telair's approved platform
- Management of supported DNS zones and DNS records for covered domains
- Administration of DNS rules and supported security or performance features within the limits of the Customer's purchased plan
- Administration of supported WAF rules and protections within the limits of the Customer's purchased plan
- Platform-based DDoS protection, bot management, caching, optimisation, and related features where included in the Customer's purchased plan
- Monitoring of service availability and basic platform health where supported by the hosting platform
- Business Hours support for covered DNS Hosting services, where included in the Customer's purchased plan

Exclusions:

- Website development, web application development, code fixes, plugin/theme remediation, or CMS troubleshooting
- Redesign of website architecture, SEO, content management, or marketing optimisation
- Application-layer debugging beyond supported platform security and hosting controls
- Custom WAF policy engineering, complex rule tuning, or security architecture work beyond ordinary administration unless separately scoped
- Remediation of vulnerabilities within the Customer's website, application code, plugins, themes, or third-party integrations
- Support for domains, services, or applications not covered by the Customer's accepted Quote
- Guarantees of protection against all attacks, vulnerabilities, bots, abuse, or zero-day threats beyond the capabilities of the underlying platform
- Feature use beyond plan entitlements, including DNS rule, WAF rule, caching, optimisation, or support limits

Purpose: To provide managed DNS hosting and associated platform-based security and performance features for covered domains and web properties.

Coverage Behaviour: Administration and support are provided during Business Hours unless the Customer's purchased plan expressly includes a different support entitlement. Emergency response outside Business Hours is limited to qualifying Severity 1–2 incidents affecting the hosted service and does not extend to general website or application troubleshooting.

Limitations: DNS Hosting protects and manages covered DNS and supported platform-layer services only. It does not replace secure website development practices, application maintenance, or Customer responsibility for web content, application code, plugins, themes, and third-party services.

8.11 Web Hosting

Applicability: Web Hosting is an optional hosted service provided under the Customer's accepted Quote. The applicable plan, resource allocation, and included features are defined in the Customer's accepted Quote.

Inclusions:

- Provision of shared or allocated web hosting services on Telair's approved hosting platform
- Hosting account setup and administration for covered hosting services
- Management of standard cPanel or equivalent hosting access for covered services
- Web hosting platform availability for covered hosting services, subject to platform limitations and maintenance requirements
- Hosting features and resource allocations included in the Customer's accepted Quote, such as storage, bandwidth, databases, email, SSL, security controls, and backups where applicable
- Basic support for hosting account access, control panel access, and standard hosting service administration

Exclusions:

- Website design, website development, code remediation, plugin/theme troubleshooting, CMS administration, or content updates
- Performance tuning of website code, databases, applications, or third-party integrations

- Mail client or user support beyond standard hosting account administration unless separately covered under a Managed IT user or service plan
- Domain registration management unless expressly included in the Customer's accepted Quote
- Malware remediation arising from insecure code, vulnerable plugins/themes, or Customer-managed applications unless separately scoped
- Custom server configuration, root-level administration, or platform engineering unless expressly included
- Recovery validation, application reconciliation, or repeated restore exercises unless separately scoped
- Guarantees of application compatibility, website performance, SEO outcomes, or uninterrupted availability beyond the capabilities of the hosting platform

Purpose: To provide managed web hosting infrastructure and standard hosting administration for covered websites and domains.

Coverage Behaviour: Hosting administration and support are provided during Business Hours unless otherwise stated in the Customer's accepted Quote. Emergency response outside Business Hours is limited to qualifying Severity 1–2 incidents affecting hosting availability and does not extend to website or application development, troubleshooting, or content issues.

Limitations: Hosting backups, firewall protection, anti-malware, SSL, and related platform services are subject to the capabilities and limitations of the underlying hosting platform. Web Hosting does not replace secure application development, website maintenance, or Customer responsibility for website content and code.

---

9. Monitoring & Alerting

Applicability: Monitoring and alerting apply to all supported systems where Telair's monitoring or RMM agents are installed, or where the device has supported telemetry (SNMP, API, cloud connector). These functions operate across all service categories and are not separate products. Behaviour under Business Hours and 24×7 Emergency Support applies consistently across all monitored devices.

This section defines the scope of Telair's monitoring and alerting capabilities, including supported telemetry, alert handling processes, and limitations. Monitoring is essential for proactive identification of issues and timely remediation but does not replace comprehensive systems management or dedicated application monitoring unless separately scoped.

Monitoring is provided on a commercially reasonable basis and may not detect all failures, anomalies, or security events.

9.1 Inclusions

System Health Monitoring:

- CPU, memory, and disk utilisation monitoring
- Disk health, SMART status (where supported), RAID alerts
- Operating system service/daemon status monitoring
- Event log monitoring for critical OS events (Windows/Linux)
- System uptime, reboots, and crash detection

Network & Connectivity Monitoring:

- ICMP/ping-based connectivity checks
- Firewall/device availability checks
- Interface status (up/down)
- Basic bandwidth utilisation alerts (where supported)

Security & Endpoint Monitoring:

- Antivirus/EDR health and event status
- Patch compliance reporting
- Unauthorized software alerts (where supported by agents)
- Login failure monitoring (where supported)

Backup Monitoring (if Telair manages backups):

- Backup job success/failure alerts
- Repository health and capacity warnings
- Agent connectivity and stability

Infrastructure Monitoring:

- Hypervisor resource utilisation (CPU, RAM, datastore capacity)
- Host uptime and failover/HA alerts (where supported)
- Switch port status (where supported)
- Access point connectivity and performance alerts

9.2 Exclusions

The following monitoring functions are outside standard scope and require separate scoping or third-party tools:

- Application-specific monitoring (SQL performance, ERP/CRM, custom apps)
- Deep SIEM/SOC monitoring unless part of a purchased security service

- Detailed wireless heatmapping or RF analytics
- Monitoring of consumer grade devices without SNMP or agent capability
- Alerting for non-standard or proprietary hardware
- Monitoring using Customer-owned tools unless adopted via project
- Telair does not support, configure, or maintain Customer-owned monitoring tools unless separately scoped.

9.3 Purpose

To provide proactive visibility into the health, performance, and stability of supported devices and systems, enabling timely remediation and reduction of unplanned downtime.

9.4 Alert Handling Behaviour

Business Hours:

- Alerts are triaged and handled during standard hours.
- Non-critical alerts may be deferred until BAU windows.

24×7 Emergency Support:

- 24×7 Emergency Support is a reactive emergency support service for Severity 1–2 incidents.
- After-hours response applies where a qualifying incident is raised through Telair's urgent support channels or through any expressly implemented escalation workflow.
- Telair does not provide a continuously staffed NOC/SOC or guaranteed after-hours human review of all alerts unless separately scoped.
- Routine, informational, or low-impact alerts are handled during Business Hours.

9.5 Customer Responsibilities

- Ensure devices remain powered on and connected to the network.
- Notify Telair in advance of planned outages or maintenance.
- Maintain stable ISP connectivity.
- Avoid blocking monitoring agents or SNMP/ICMP traffic (where applicable).
- Where 24×7 Emergency Support applies, maintain an authorised after-hours contact who is reachable by phone and able to approve urgent remediation actions or downtime-related decisions.

9.6 Limitations

- Monitoring depends on reliable connectivity and stable device operation.
- Some alerts may originate from vendor cloud services outside Telair's control.

- Alert accuracy may vary depending on hardware capability and vendor API reliability.
- Certain hardware classes (e.g., unmanaged switches) provide limited telemetry.

---

10. Scheduled Maintenance

Applicability: Scheduled maintenance applies to all supported systems where Telair provides patching, firmware updates, or routine maintenance activities. These controls apply across all user, device, server, and infrastructure plans and are not standalone services. Maintenance behaviour under Business Hours and 24×7 Emergency Support applies consistently across all included systems.

Scheduled Maintenance ensures systems remain secure, stable, and up to date. This section defines the scope, expectations, Customer responsibilities, and behaviour for Business Hours and 24×7 coverage.

Firmware or patching tasks requiring downtime will only proceed with Customer approval unless undertaken as part of emergency maintenance to address critical vulnerabilities.

10.1 Inclusions

Patch Management:

- Deployment of operating system patches on supported servers and workstations
- Deployment of third-party application patches where supported by Telair's patching tools and capable of being applied using standard vendor-supported update methods
- Verification of patch status and remediation of patch failures

Firmware & Device Updates:

- Firmware updates for supported firewalls, routers, switches, access points, and servers
- BIOS and driver updates where required and supported
- Coordination of reboot windows with the Customer

Scheduled Reboots:

- Routine reboots for servers and network devices when required for patching or remediation
- Notification to Customer of upcoming maintenance windows

Maintenance Windows:

- Execution of vendor recommended maintenance activities
- Safe application of non-disruptive updates
- Implementation of best practice routines such as log cleanup, certificate renewal checks, and storage health validation

10.2 Exclusions

The following fall outside standard maintenance unless separately scoped:

- Major operating system or platform upgrades, including new OS generations and feature releases delivered as in-place upgrade workflows, unless expressly included in the Customer's accepted Quote
- Hardware replacement, lifecycle refresh, or disruptive rebuilds
- After-hours maintenance not covered under 24×7 Emergency Support
- Repatching of legacy OS versions no longer supported by the vendor
- Remediation of issues caused by Customer performed changes or blocked updates
- Custom packaging, pilot testing, rollback engineering, or remediation of third-party application update issues requiring vendor-specific investigation unless separately scoped

10.3 Purpose

To maintain a secure and stable operating environment by ensuring patches, firmware, and maintenance tasks are applied in a controlled, predictable manner.

10.4 Coverage Behaviour (BH vs 24×7)

Business Hours Customers:

- All scheduled maintenance (patching, firmware, routine reboots) occurs during Business Hours.
- After-hours maintenance requiring supervision or monitoring is billable at SBR.
- Non-disruptive updates may be applied after hours unattended if safe.

24×7 Emergency Support Customers:

- Routine updates still occur during Business Hours unless otherwise requested.
- After-hours maintenance windows for critical environments may be scheduled without additional labour cost.
- Emergency patching (e.g., zero-day exploitation risk) may be executed outside Business Hours.

10.5 Customer Responsibilities

- Provide approval for reboots or downtime where required

- Notify Telair of blackout periods or change freezes
- Ensure onsite staff are available where physical access is required
- Maintain backup systems to protect against update related issues

10.6 Limitations

- Maintenance may be delayed if Customer approval is not received
- Maintenance may be rescheduled due to vendor outages or other dependencies
- Devices with unsupported firmware or OS versions may require upgrades at Customer cost

---

11. General Exclusions

This section provides overarching commercial clarity. It does not replace or override the specific inclusions and exclusions already defined in each service category but serves as a catch-all to avoid ambiguity.

11.1 General Exclusions

Unless explicitly included within this Service Schedule or the Managed IT Services MSA, the following items are excluded from standard Managed IT Services and may be billable at SBR:

- Any service, activity, or deliverable not expressly defined as an inclusion
- Work arising from Customer negligence, misuse, or unauthorised changes
- Faults caused by third-party providers, carriers, ISPs, vendors, or unmanaged systems
- Rectification of issues originating from unsupported, end of life, or non-standard environments
- Force majeure events, environmental damage, or incidents outside Telair's control
- Recovery work, data restoration, or emergency support not covered under a Customer's 24×7 plan

11.2 Clarifying Statement

Where inconsistencies arise, **specific inclusions and exclusions in earlier sections take precedence** over this General Exclusions clause.

---

12. Support Hours

Business Hours: 8:30am–5:00pm local time, Monday–Friday, excluding national public holidays and any additional public holidays observed at the Customer's primary site, for Australian-based sites.

International Sites: Supported during Australian East Coast Business Hours (8:30am–5:00pm AEST), Monday–Friday, excluding Queensland public holidays.

24×7 Emergency Support: Applies only to Severity 1 and 2 incidents and only where the Customer has purchased the applicable 24×7 Emergency Support add-on. Routine requests raised after hours are handled during Business Hours.

---

13. Severity Levels & Response Targets

Severity levels determine the urgency and priority of incidents. Response targets represent commercially reasonable objectives and do not guarantee resolution within a set timeframe.

Severity	Description	Target Response
Severity 1	Complete outage or critical business impact	1 hour
Severity 2	Major degradation, high operational impact	2 hours
Severity 3	Moderate impact affecting specific users or systems	4 Business Hours
Severity 4	Low impact or routine request	Next Business Day

---

14. Onsite Support

Onsite attendance is provided when remote troubleshooting cannot resolve the issue or where physical intervention is required.

14.1 Included Onsite Support

Included onsite support is limited to in-scope services within metro areas, as defined in the Travel Rates table in Section 17.2, and is subject to Telair's reasonable use / remote-first policy in the MSA. Included onsite support during Business Hours covers:

- Critical response when remote remediation is not possible
- Hardware diagnostics for Telair-supplied devices and supported Customer-owned devices that remain under valid manufacturer warranty
- Escalated network or server troubleshooting requiring physical access

14.2 Billable Onsite Support

The following onsite activities are billable at applicable SBR rates:

- After-hours onsite attendance
- Installations, upgrades, and physical deployments
- Non-metro travel or regional/rural attendance
- Repeated onsite attendance for issues that could be resolved remotely

Metro, regional, and rural boundaries follow the definitions in the Travel Rates section.

---

15. Onboarding

Onboarding is a separately scoped and charged service, as defined in the Customer's accepted Quote. It is required for all new Managed IT Service engagements and is not included in recurring per-user or per-device fees.

Billing Commencement: In accordance with the MSA, billing for Managed IT Services commences immediately upon Telair's acceptance of the Customer order, regardless of onboarding progress or completion. Delays caused by Customer responsiveness, access issues, or environment readiness do not defer billing start dates.

Onboarding prepares the Customer environment for ongoing support. Timelines depend on Customer responsiveness and environment readiness.

Onboarding includes:

- Audit of existing systems and infrastructure
- Deployment of Telair monitoring and security agents
- Licensing and security configuration review
- Collection of documentation and access credentials
- Alignment of user and device lists

Issues identified during onboarding that require remediation may be billable at SBR.

---

16. Offboarding

Offboarding occurs when a Customer transitions away from Telair Managed IT Services. In accordance with the MSA, offboarding is not included in standard Managed IT Services and is delivered on a time-and-materials basis.

Offboarding may include:

- Removal of Telair monitoring, security and management agents
- Removal of Telair remote access tools and administrative accounts
- Handover of available documentation relevant to supported systems
- Coordination with the Customer's new provider for a smooth transition
- Credential resets or administrative updates as required

All offboarding activities are billed at Standard Billable Rates (SBR) with a minimum charge of 10 hours per offboarding engagement, unless otherwise agreed in writing in the Customer's Quote. The Customer remains responsible for transition planning and for any third-party, carrier, or vendor costs.

---

17. Billing & Commercial Terms

User and Device Count Obligations: The Customer must ensure all users and supported devices are accurately listed and kept up to date. Increases to user counts, endpoints, infrastructure devices, or supported peripherals will be billed from the date they are added or discovered, in alignment with the Customer's accepted Quote and the MSA. Internal pricing schedules may be used by Telair to prepare quotes but do not form part of this Agreement unless expressly provided to the Customer.

Billing for Managed IT Services follows the operational rules below.

17.1 Recurring Billing

- Monthly recurring charges (users, devices, infrastructure) are billed in advance.
- User and device counts are reviewed each month and updated accordingly.
- Minimum commitments apply as defined in the Customer's Quote and the MSA.
- Third-party licensing, subscription, vendor support, and supplier-provided service costs are passed through based on vendor pricing and may be adjusted in accordance with the MSA.

Recurring fees for user plans, device coverage, infrastructure support, and optional add-ons are defined solely in the Customer's accepted Quote. This Service Schedule describes how those services are delivered; it does not list all recurring charges.

17.2 Standard Billable Rates (SBR)

SBR applies to work outside the scope of this schedule or the MSA.

When SBR Applies

- Advanced configuration or redesign work
- Firewall or VLAN redesign

- Migrations or project activity not explicitly included
- Onboarding remediation
- Legacy or unsupported systems
- Vendor liaison beyond basic troubleshooting
- Emergency recovery work
- All offboarding activities, including transition coordination and documentation handover

SBR Rates (ex GST)

Tier	Hourly Rate (AUD)
Level 1 Technician	$180
Level 2 Systems Technician	$210
Level 3 Systems Engineer	$240
ICT Specialist	$270
Strategic Consultant	$300

Multipliers

Situation	Multiplier	When Applied
Extended Hours	1.5×	Weekdays 6:00–8:30 & 17:00–22:00
After-hours	2×	Weekdays 22:00–6:00; weekends; public holidays
Regional onsite	1.5×	Within 100 km of a Telair office
Rural onsite	2×	Over 100 km from a Telair office

Additional Charges

Charge Type	Amount	When Applied
Emergency callout	$250 per callout	Urgent unscheduled after-hours onsite attendance. Applies in addition to the applicable SBR rate, multiplier, and travel charges.

Minimum Chargeable Periods

Work Type	Minimum Billable Time
Remote (Business Hours)	15 minutes
Onsite (Metro)	1 hour
Onsite (Regional/Rural)	2 hours plus applicable travel
After-hours	1 hour remote / 2 hours onsite
Offboarding Engagement	10 hours minimum

Travel Rates

Travel Type	Rate	Description
Metro (included)	Included	Within 50 km road distance of the nearest Telair office for included in-scope tasks
Metro (out of scope)	SBR rate	Within 50 km road distance of the nearest Telair office; both directions billed for out-of-scope tasks
Regional	$2/km + 1.5× SBR time	More than 50 km and up to 100 km road distance from the nearest Telair office
Rural	$2/km + 2× SBR time	More than 100 km road distance from the nearest Telair office
After-hours travel	Multiplier applies	1.5× or 2× based on time
Parking & tolls	Cost + 25% admin (min $10)	Admin applies to expense only
Accommodation	Cost + 25% admin	No minimum admin fee applies

Contractor & Specialist Rates

Scenario	Billing Rule
Subcontractor attendance	Subcontractor rate + 25% admin if higher than SBR
Specialist engineer	Vendor or specialist rate + 25% admin
Remote area subcontractor	Subcontractor rate + travel multipliers
Subcontractor expenses	Cost + 25% admin (minimums apply)
Vendor engineering	Vendor rate + 25% admin; multipliers apply