This Service Level Agreement ("SLA") is incorporated by reference into, and governed by, the applicable Statement of Work ("SOW") and the underlying agreement between Usherwood and the Client (collectively, the "Agreement"). This SLA describes service level targets and support expectations applicable to Usherwood's managed services, as further detailed in the relevant SOW, and is intended to promote clear communication, accountability, and consistent service delivery.

This SLA does not modify or expand the scope of services, fees, or other contractual terms set forth in the Agreement or SOW. Unless otherwise expressly stated, all time references are in Eastern Time and exclude Usherwood-observed holidays.

1. Service Summary

Service Name	Service Summary
Server Patch Management	OS and approved third-party patch cycles for servers.
Workstation Patch Management	Windows/macOS OS patching and common third-party updates.

2. Inclusions and Deliverables

2.1. Server Patch Management

Approved server patches are deployed on a scheduled basis in accordance with defined patching policies and include the following components:

- Defined patch baselines aligned to supported operating system and application versions;
- Use of staged deployment methodologies, where supported, to reduce risk prior to broader release;
- Scheduled maintenance windows for patch deployment;
- Scheduled patch deployment and installation activities on a best effort basis;
- Documented patch rollback plans;
    - Patch rollbacks are initiated upon confirmation of critical infrastructure impacts at a Severity 2 event or higher. Patch rollback decisions for lower severity events are evaluated on a case-by-case basis based on impact and root cause analysis.
- Patch compliance and deployment reporting, based on available system and platform data; and
- Deployment of out-of-band critical patches, where required to address active security risks or stability issues.

2.2. Workstation Patch Management

Approved workstation patches are deployed on a scheduled basis in accordance with defined patching policies and include the following components:

- Deployment or update rings to control rollout timing and exposure;
- Deferral policies aligned with system stability and compatibility requirements;
- Patch compliance and deployment reporting; and
- Supported remediation of patch failures through rollback, reapplication, or vendor-recommended corrective actions, as applicable.

3. Exclusions

Unless expressly stated otherwise in a SOW or Project, the following services and circumstances are excluded from the Patch Management Services under this SLA.

3.1. Server Patch Management

- Application compatibility testing prior to patch deployment, which remains the responsibility of the Client or the applicable software vendor.
- Remediation of patch failures beyond supported patch rollback procedures or restoration from an approved backup solution, subject to the Threat Detection, Monitoring, and Response SLA.
- Patching of unsupported, end-of-life, or out-of-scope operating systems or applications.

3.2. Workstation Patch Management

- Patching or support for unsupported, end-of-life, or non-standard workstation operating systems or devices.
- Remediation of issues resulting from interference, modification, or circumvention of patching processes by the Client or third parties.

3.3. General Exclusions

- **Patch Timing Limitations**: Newly disclosed vulnerabilities may exist in the environment prior to patch availability, testing, or deployment. Usherwood does not guarantee protection from all vulnerabilities at all times.
- **Security Scope Limitation:** Patch management is one component of a broader security strategy and does not eliminate all security risks. Additional controls such as endpoint protection, monitoring, and identity security are required for comprehensive protection.
- Issues, outages, or performance degradation resulting from vendor supplied patches, updates, or hotfixes.
- Vulnerabilities for which no patch or vendor-supported remediation is available.
- Delays in patch deployment caused by vendor release schedules, compatibility concerns, or risk-based deferral decisions.
- User disruption resulting from required system restarts, application updates, or patch related changes.
- Patch deployment failures or inconsistencies caused by endpoint conditions, agent health, or third party platform limitations outside of Usherwood's direct control.
- System downtime, restarts, or temporary service interruptions required to complete patch installation.
- Compliance with specific regulatory, audit, or industry requirements unless explicitly defined in the applicable SOW.

Excluded services may be provided under a separate Project or SOW.

4. Client Responsibilities

To support reliable delivery of the Services, the Client agrees to the following responsibilities.

- Payment for all Support costs at the agreed interval and rate.
- An available designated representative and backup contact to communicate incidents,

reports, requests, and events requiring communication and resolution.
- Adequate infrastructure to maintain and support regular, in-scope patching.
- Reasonable assistance to help diagnose problems.

Failure to meet these responsibilities may result in Service delays, limitations, or outcomes that fall outside the scope of this SLA.

5. Service Assumptions and Client Dependencies

The delivery and effectiveness of the Services under this SLA are dependent upon the following assumptions and conditions being met by the responsible party.

5.1. Server Patch Management

- Usherwood: Deployment and continued availability of required Remote Monitoring and Management (RMM) tools, agents, or administrative access necessary to perform patching services.
- Client: Servers remain powered on, accessible, and connected to reliable network and data services sufficient to allow uninterrupted patch deployment during approved maintenance windows.

5.2. Workstation Patch Management

- Usherwood: Deployment and continued availability of required RMM tools, agents, or administrative access necessary to perform patching activities.
- Client: Workstations are powered on, connected to the network, and available during scheduled patching windows to allow patches to be applied successfully.

Failure to meet these assumptions and dependencies may result in Service limitations, delays, or outcomes that fall outside the scope of this SLA.

6. Services Availability

Client Portal	Email	Phone	After Hours*
- Tickets submitted via portal will be monitored 8:00 AM-5:00 PM, Monday-Friday - Tickets received during non-business hours will be responded to during regular business hours.	- Email ticket submissions will be monitored 8:00 AM – 5:00 PM, Monday – Friday - Tickets received during non-business hours will be responded to during regular business hours. - Contact: service-request@usherwood.com	- Calls will be accepted 8:00 AM – 5:00 PM, Monday – Friday - Calls received during non-business hours will have voicemail available and will be responded to during normal business hours. - Contact: (800) 724-2119	- Severity 1 Tickets Only - Available from 6:00 AM – 8:00 AM, 5:00 PM – 10:00 PM Monday – Friday, 6:00 AM – 10:00 PM weekends and holidays. - Key contact(s) will be provided the on-call number.

6.1. Ticket Acknowledgement

Usherwood will log end-user issue(s) and supply a trouble-ticket case number based on the standard coverage parameters listed above.

6.2.Ticket Resolution

Usherwood will attempt to resolve ticket remotely as outlined below. On-site resources may be engaged contingent upon ticket severity at Usherwood's discretion. Resolution times are dependent on problem severity and complexity.

7. Ticket Severity Level Definitions & Response Targets

Severity level indicates the relative impact of an issue on end-user systems or business processes that are related only to supported infrastructure and technology. Usherwood uses the following severity level definitions to classify all support requests:

Severity Level	Response Priority and Time	Target Response Time	Definitions
Severity 1	Emergency*	Within fifteen (15) minutes	• Widespread impact, typically greater than 90% of employees impacted. • A mission critical supported product or service is down, and no workaround is immediately available (i.e. ISP outage or application failure). • A crucial supported infrastructure component is not functioning, resulting in significant operational and critical business impact (i.e. a critical server failure).
Severity 2	Quick	Within thirty (30) minutes	• A critical end-user is unable to use a component or business-critical application or feature. • A failure of supported infrastructure that affects a significant number of end-users or a key function. • A significant issue with a key application that causes a high impact on business operations for a significant number of end-users.
Severity 3	Normal	Within one (1) hour	• Non-critical issues isolated to specific end-users. • Infrastructure failure resulting in non-critical challenges without significant business impact. • Issues to applications where an end-user is able to use the solution; however, there is a non-critical loss of functionality.