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 network 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
Firewall Management	Full Lifecycle management for next-gen firewalls.
Switch Management	Configuration and lifecycle management of switches.
Wireless Access Point Management	WLAN policy and performance management.
Server Management	Administration of Windows servers and core OS services.
Remote Access Support	Remote monitoring and tool supported access to in-scope network devices for operations, troubleshooting, configuration, and maintenance.

2. Inclusions and Deliverables

2.1. Firewall Management

Firewall management is performed through the applicable in-scope vendor portal. Usherwood will apply baseline configurations in accordance with Usherwood's standard deployment practices and within the boundaries of the co-managed relationship. Included firewall management services consist of the following:

- Monitoring of firewall service availability and operational health;
- Verification of configured log forwarding;
- Performance of firmware updates and configuration backups to the maximum allowable by the device's OS;
- Execution of approved firewall rule changes with Client approval; and
- VPN configuration support, troubleshooting, and vendor escalation, as appropriate and aligned with current cybersecurity practices.

2.2. Switch Management

Switch management is performed through the in-scope vendor portal. Baseline configurations are applied in accordance with Usherwood's standard deployment practices. Included switch management services consist of the following:

- VLAN configuration in alignment with Usherwood's standard configuration framework;
- Firmware updates and configuration backups, subject to vendor support and device compatibility;
- Monitoring of switch service availability and operational health;

- Port security configuration and activity monitoring where supported by the platform ; and
- Port movement or reconfiguration for standard, approved changes or transitions.

2.3. Wireless Access Point (WAP) Management

WAP management is performed through the applicable in-scope vendor portal. Baseline configurations are applied in accordance with Usherwood's standard deployment practices. Included WAP management services consist of the following:

- SSID configuration and design aligned to Usherwood standards;
- Guest Wi-Fi portal configuration, as required;
- RF tuning and optimization performed through software based configuration and monitoring tools, with performance subject to environmental and physical conditions;
- Monitoring of WAP service availability and operational health; and
- Performance of firmware updates and configuration backups where supported and deemed appropriate based on vendor guidance and operational risk. .

2.4. Server Management

Server management services are delivered through Usherwood's deployed Remote Monitoring and Management (RMM) tool. Baseline configurations are applied in accordance with Usherwood's standard deployment practices whenever possible. Included server management services consist of the following, subject to responsibility allocation defined in the applicable SOW:

- Monitoring of in-scope operating systems and services;
- System service tuning based per system requirements;
- Active Directory management;
- Domain Name System (DNS) and Dynamic Host Configuration Protocol (DHCP) management, where applicable;
- Certificate lifecycle monitoring and renewal coordination;
- Capacity monitoring and alerting;
- Verification of backups within the approved backup solution;
- Coordination with vendors for patch releases and known issues;
- Application of approved patches, as defined by the co-managed patching responsibilities in the SOW; and
- Server incident response activities limited to operational stabilization and service restoration; security incident response and forensic analysis are excluded unless otherwise defined in a separate agreement.

2.5. Remote Access Support

Remote Access Support is provided through Usherwood's deployed RMM or an approved remote access solution, based on Usherwood's standard deployment practices and Client environment limitations. Included remote access services consist of the following:

- Qualified access to remote access solution, per business requirements;
- Configuration and maintenance of the remote access solution, per guidelines and deployment standards;
- Access to approved, in-scope remote applications as defined by the SOW; and
- Reasonable troubleshooting of remote access issues within the supported environment.

3. Exclusions

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

3.1. Firewall Management

- On-site support services, unless expressly authorized by Usherwood and defined in a Project or SOW.
- Implementation of non-standard or custom firewall configuration implementation.
- Deployment or support of Insecure, deprecated, or unsupported network protocols.

3.2. Switch Management

- Cabling modifications or adjustments outside of a defined Project or SOW.
- Firmware patching or updates outside of initial deployment or defined managed scope.
- Replacement of connected hardware, including devices that are out of warranty or no longer supported by the manufacturer.

3.3. Wireless Access Point Management

- Cabling, mounting, or physical placement adjustments outside of a contracted Project.
- Ongoing guest Wi-Fi administration or maintenance beyond initial configuration settings and access needs.

3.4. Server Management

- Application-layer support beyond initial operating system-level triage.
- Database administration, optimization, or tuning.
- Support for out-of-scope applications or remote access requirements not defined in the applicable SOW.

3.5. Remote Access Support

- Deployment or support of unapproved remote access solutions.
- End-user support not expressly included in the SOW, such as: helpdesk services, identity and access management (IAM), user provisioning, access governance, or user training.
- Unauthorized access, misuse, or compromise of remote access systems resulting from credential theft, user behavior, or external attack.

3.6. General Exclusions

- Internet service provider (ISP) outages, latency, packet loss, or performance issues outside of Usherwood's control.
- Limitations, failures, or outages of third-party hardware, firmware, or vendor managed platforms.
- Network performance degradation caused by bandwidth limitations, environmental factors, or external dependencies not managed by Usherwood.
- Any conditions or failures resulting from factors outside of Usherwood's reasonable control, including Client actions, third party systems, or environmental conditions.
- Network management services support the operation and maintenance of network infrastructure but do not guarantee prevention of unauthorized access, cyber incidents, or

security breaches. Comprehensive security requires additional controls including monitoring, endpoint protection, and identity security.
- Security incidents, breaches, or unauthorized access events outside of network configuration scope, including those resulting from compromised credentials, endpoints, or third-party systems.
- Security of remote access usage, including credential management and endpoint security, remains the responsibility of the Client.

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.
- Maintenance of current support contracts with required third-party vendors for business-critical server-based applications and services.
- Maintenance of active vendor subscriptions and licensing for operational continuity.

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. Firewall Management

- Client: Required vendor subscriptions and licenses remain active and in good standing.
- Shared (Usherwood/Client): Firewall devices remain actively supported by the primary hardware vendor; Usherwood will notify the Client when unsupported or end-of-life conditions are identified, and the Client is responsible for remediation, renewal, or replacement.

5.2. Switch Management

- Client: Required vendor subscriptions and licenses remain active and in good standing.
- Shared (Usherwood/Client): Switch hardware remains actively supported by the primary vendor; Usherwood will notify the Client of unsupported or end-of-life devices, and Client is responsible for replacement or upgrade.

5.3. Wireless Access Point Management

- Client: Required vendor subscriptions remain active and in good standing.
- Usherwood to notify/Client to provide: Devices actively supported by primary vendor.

5.4. Server Management

- Client: Required vendor subscriptions remain active and in good standing.
- Client: Server hardware remains actively supported by primary hardware vendor.
- Client: Applicable server warranties remain active.
- Shared (Usherwood/Client): Server operating systems are supported by the operating system vendor and maintained in good working order; Usherwood will identify unsupported or degraded conditions through monitoring, and the Client is responsible for remediation unless otherwise defined in an SOW.
- Usherwood: Server patching is performed in accordance with the patching responsibilities and approval defined in the applicable co-managed SOW.

5.5. Remote Access Support

- Usherwood: Determination that Client environment requires a remote access solution based on the presence of physical, on-premises infrastructure not accessible through cloud-native platforms.
- Shared (Usherwood / Client): The remote access environment complies with applicable security standards and mandated controls; Usherwood implements supported technical configurations, and the Client adheres to required usage, policy, and access controls.
- Shared (Usherwood / Client): Multi-Factor Authentication (MFA) is deployed and maintained for all supported endpoints and critical access gateways; Usherwood configures MFA where supported, and the Client enforces user compliance and access governance

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.