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
Security Information & Event Management (SIEM)	SIEM platform administration, log onboarding, and alert triage
Identity Threat Detection and Response (ITDR)	Monitoring and response for identity-based threats (AD/AAD)
Vulnerability Management	Risk-based vulnerability scanning and remediation guidance

2. Inclusions & Deliverables

2.1. Security Information & Event Management (SIEM)

SIEM services include tool-supported data ingestion, correlation, and analytics for supported systems and applications, providing near real-time visibility and alerting through the Security Operations Center ("SOC"). Included SIEM services consist of the following:

- Onboarding and ingestion of supported log sources, which may include firewalls, servers, Microsoft 365 (M365), endpoint detection and response (EDR), and identity platforms, as applicable;
- Application of correlation rules from Usherwood's standard detection catalog;
- Security alerts and notifications delivered through the ticketing system and associated communication channels;
- Security alerts are communicated through the ticketing system and associated escalation procedures. Alert delivery methods, frequency, and timing may vary based on severity, classification, and operational considerations;
- SOC-based alert triage and investigation with recommended response actions;
- Periodic coverage reviews to assess data sources, detection effectiveness, and alert relevance; and
- Generation of SIEM reports upon Client request.

SIEM services are limited to event detection, analysis, and reporting and do not include log retention guarantees, custom rule development, or forensic investigation unless expressly defined in the SOW.

2.2. Identity Threat Detection and Response (ITDR)

ITDR services include tool-supported monitoring of identity-based threats with near real-time alerting through the SOC. Included ITDR services consist of the following:

- Detection of risky or anomalous sign-in activity;
- Monitoring for privilege escalation attempts and abnormal access patterns;
- Identification of indicators associated with lateral movement or credential misuse;
- Use of deception technologies (such as honeytokens), where supported by the platform and Client environment; and
- Execution of predefined identity response actions, which may include disabling user accounts, revoking authentication tokens, or enforcing password resets or multi-factor authentication (MFA) re-registration, in accordance with approved response playbooks.

Identity governance, access policy design, and user provisioning remain the Client's responsibility unless expressly included in the SOW.

2.3. Vulnerability Management

Vulnerability Management services include tool-supported identification, analysis, and tracking of vulnerabilities within the Client environment. Usherwood will work collaboratively with Client's designated IT personnel to plan and remediate operating system (OS) vulnerabilities classified as Critical and High, as identified by Usherwood's designated vulnerability scanning tools, on in-scope systems. Remediation activities are limited to OS-level vulnerabilities that can be addressed through standard patching or mitigation processes.

Usherwood may provide limited patching for select third-party applications where such applications are supported within Usherwood's designated patch management tools and approved policies. Such third-party patching is performed on a best-effort basis and is not guaranteed.

Application-layer vulnerabilities, including those related to third-party applications, runtimes, frameworks, redistributables (e.g., Java, .NET, Visual C++), firmware, or custom configurations, are otherwise excluded from standard remediation services unless explicitly defined in a SOW or authorized through a separate written Change Order.

Additional remediation efforts or configuration changes involving advanced fixes will be evaluated on a case-by-case basis and may be subject to a project and billed separately under a SOW.

Included in Vulnerability Management services consist of the following:

- Authenticated internal and/or external vulnerability scanning, as defined by the Client's contracted scope
- Asset discovery and attribution within the supported environment;
- Vulnerability based on Common Vulnerability Scoring System (CVSS) and the contextual threat profile;
- Tracking and reporting of remediation status and risk acceptance;
- Periodic vulnerability reporting (monthly or quarterly, as applicable); and
- Exception management to document accepted risk or remediation deferrals approved by the Client.

2.4. Zero Trust Enforcement

As part of Usherwood's threat prevention strategy, application control and Zero Trust execution enforcement tools may be deployed where licensed and included in the applicable SOW. These tools enforce policy-based execution controls and generate alerts for unauthorized activity, but do not constitute incident response, forensic services, or breach remediation.

Application control and Zero Trust enforcement services may be offered as a standalone or enhanced service tier and are subject to separate pricing and scope definition.

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. Security Information & Event Management (SIEM)

SIEM services explicitly exclude the following:

- Log sources, systems, applications, or environments not expressly defined as in-scope in the SOW, including custom applications, unsupported or incompatible operating systems, or unintegrated environments;
- Log sources or environments that are not property integrated or accessible to the SIEM platform;
- Unsupported or incompatible log formats or protocols;
- Endpoint or agent failures outside the SIEM provider's control, including Client misconfiguration, unsupported application conflicts, firewall restrictions, or network connectivity issues;
- Events, outages, or security incidents originating from a third-party;
- Detection of exploits and vulnerabilities in zero-day or unreported environments;
- Detection of attacks carried out in unintegrated environments or in applications that do not generate logging;
- Insider threat detection or remediation;
- Monitoring of physical security systems such as alarms, cameras, or other related technologies; and
- Security incidents resulting form vulnerabilities that remain unremedied due to Client-approved exceptions, deferrals, or inaction.

3.2. Identity Threat Detection and Response (ITDR)

ITDR services explicitly exclude the following:

- Identify providers, directories, or authentication platforms not expressly defined as supported or in-scope in the SOW;
- Legacy or unsupported systems;
- Detection gaps created by incomplete or missing identity logs, or other required telemetry data;
- Misconfigurations, policy changes, or access settings implemented by the Client or third parties that impacts the ability of the ITDR to read, access, review, or detect activity;
- Unidentified gaps in privileged access or conditional access policies;
- Insider threat detection or user behavior tracking;
- Network-based lateral movement detection and reporting outside of identity-driven indicators;
- Full incident response, forensic investigation, or breach response activities unless expressly included in the SOW; and
- Security incidents attributable to known vulnerabilities that remain unremediated due to Client-approved risk acceptance or inaction.

3.3. Vulnerability Management

Vulnerability Management services explicitly exclude the following:

- Execution of vulnerability remediation activities unless explicitly defined in the SOW;
- Identification or scanning of unsupported or legacy operating systems, applications, or devices;
- Scanning of systems that are inaccessible, isolated, restricted or otherwise unable to be scanned due to network segmentation, security controls, or environmental limitations;
- Vulnerability assessment of third-party controlled assets and applications not managed by the Client; and
- Delivery of explicit, step-by-step remediation guidance, unless explicitly requested and contracted.

3.4. General Exclusions and Limitations

- Security monitoring services are designed to identify indicators of potential threats but do not guarantee detection of all security events, attacks, or unauthorized activity.
- Security events may occur prior to detection, ingestion, or correlation within the monitoring platform. Detection and alerting timelines are dependent on log availability, system configuration, and platform performance.
- Threat detection and response services do not guarantee prevention, containment, remediation, or recovery from all security incidents.
- Client facing visibility into security events is limited to alerts, reports, and communications provided by Usherwood. Direct access to monitoring platforms, dashboards, or raw telemetry is not included unless explicitly defined in the applicable SOW.
- Not all detected events result in alert generation. Alerts are prioritized based on severity, confidence, and relevance to reduce noise and support effective response.
- Security monitoring and response capabilities are dependent on the availability, accuracy, and completeness of data from in scope systems, as well as the performance and limitations of underlying platforms and third-party services.
- Response actions are limited to predefined playbooks and approved actions within supported systems. Full incident response, forensic investigation, eradication, and recovery services are not included unless explicitly defined in a separate SOW.
- All security services are provided on a commercially reasonable, best effort basis and do not guarantee security or prevention of all threats.
- Notification of security events that do not meet alerting thresholds, are not correlated by detection logic, or are determined to be non-actionable by qualified vendors or other regulatory entities in conjunction with defined risk thresholds.

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

4. Client Requirements

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.
- Access and appropriate configurations to ensure the full functionality of all monitoring tools

and agents.
- Adequate infrastructure to maintain and support the solution(s).
- Reasonable assistance to help diagnose problems.
- To act in a reasonable timeframe when notified of a vulnerability by Usherwood.

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

5. 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.

5.1. Ticket Acknowledgement

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

5.2. Ticket Resolution

Usherwood will attempt to resolve tickets 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.

6. 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.