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 Backup	File/system-state/application-aware backups for physical/virtual servers via agent.
M365 Backup	Backup for Exchange Online, SharePoint, OneDrive, and Teams data (as supported by platform).

2. Inclusions and Deliverables

2.1. Server Backup

Server backup will be primarily conducted through usage of Usherwood's deployed cloud backup provider. On-site backups and physical backup servers will be deployed to required environments at additional cost, and baseline configurations will be applied per Usherwood's standard deployment practices. Additional service obligations for the duration of the product lifecycle and relationship with Usherwood include the following:

- Backup configuration and policy management;
- Daily backup health monitoring;
- Backups are scheduled at one (1) hour intervals, based on system configurations and Usherwood's known best practices;
- Backup failure remediation and notification;
- In transit encryption;
- Backup retention enforcement, up to one calendar year;
- Monthly sampled restore testing of representative systems or data sets to validate backup integrity;
- Documented restore runbooks; and
- Reasonable restoration times based on data load, network stability, and bandwidth; restoration timelines may vary and are not guaranteed.

2.2. Microsoft 365 Backup

Microsoft 365 (M365) backup will be primarily conducted through the native M365 Backup solution and covers the following in scope services:

- SharePoint data and files, subject to platform capabilities, licensing, and service limitations;
- Exchange and Exchange Online;
- OneDrive, up to contracted service limits;

- Microsoft Teams, up to contracted service limits;
- Monitoring and remediation of backup failure;
- Periodic restore tests; and
- Item/site-level restores via ITSM.

3. Exclusions

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

3.1. Server Backup

- Unsupported or end-of-life operating systems not supported by the operating system vendor or backup software provider;
- Backup data that is compromised, encrypted, deleted, or altered due to unauthorized access, administrative actions, or cyber security incidents prior to or during backup operations;
- Data lost between hourly backup windows as a result of a significant downtime event;
- Individual application backup and restoration services;
- Hardware failures not covered under contract or server warranty that results in loss or corruption of backup integrity;
- Network connectivity issues or external infrastructure dependencies not managed by Usherwood that may impact restoration or image generation timelines;
- Incident response, forensic investigation, or remediation activities outside of server backup restoration;
- Custom configuration, maintenance, or engineering tasks not explicitly defined in a Project, Statement of Work, or change order; and
- Compliance or audit driven work, outside of providing proof of backup presence and integrity.

3.2. M365 Backup

- E-Discovery/Legal Hold projects outside platform capabilities;
- Backup data that is compromised, encrypted, deleted, or altered due to unauthorized access, administrative actions, or cyber security incidents prior to or during backup operations;
- OneDrive file backup or restoration of files not yet synced to cloud storage;
- Files exclusively on a users local device;
- Restoration of recycle bin items beyond M365 or backup retention limits;
- Restoration of corrupted files to a usable state;
- Content stored outside of licensed accounts;
- Unsupported M365 applications or services;
- Tenant-level configuration changes, including identity management, security settings, or conditional access policies;
- Third-party applications or integrations not explicitly integrated into the backup solution;
- Remediation of compromised accounts or applications outside of a full, clean recovery from backup, where available;
- Recovery of files beyond defined M365 or backup retention policy limits;
- Large-scale restores beyond vendor bandwidth limits;

- Full tenant rollback; and
- Compliance or audit driven work, outside of providing proof of backup presence and integrity.

3.3.General Exclusions

- Backup services rely on third party platforms and infrastructure. Usherwood is not responsible for outages, limitations, or failures of underlying backup providers that are outside of its control.
- Restoration services under the Backup and Disaster Recovery SLA are limited to data recovery and do not include threat containment, eradication, or breach response activities.

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.

4.1. Server Backup

- 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 operations and quality backups;
- Reasonable assistance to help diagnose problems;
- Maintaining current support contracts with required third-party vendors for business critical server based applications and services; and
- Maintaining active vendor subscriptions and licensing for operational continuity.

4.2. M365 Backup

- 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;
- Reasonable assistance to help diagnose problems; and
- Maintaining 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. Server Backup

- Client: Required vendor subscriptions remain active and in good standing.
- Client: Server hardware is actively supported by the primary hardware vendor.
- Client: Applicable server hardware warranties remain active.
- Client or Usherwood (as applicable under the governing SOW): Server operating systems are supported by the operating system vendor and maintained in good working order.

- Client or Usherwood (as applicable under the governing SOW): Servers are patched and maintained in accordance with reasonable industry standards applicable to the Client's environment.
- Usherwood: Cloud backup connectivity is established, operational, and actively reporting within the backup platform.

5.2. M365 Backup

- Client: Required M365 licenses and related vendor subscriptions remain active and in good standing.
- Client: In-scope M365 applications and services are appropriately updated and maintained within the Client's tenant.
- Usherwood: Backup configuration is completed in accordance with the supported configuration standards of the backup solution.

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 of notification window	• 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 of notification window	• 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 of notification window	• 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.