

Unily is a leading enterprise-grade employee experience platform delivered as a cloud-hosted Software-as-a-Service solution, designed to unify internal communications, knowledge sharing, collaboration, and engagement across web, mobile, and integrated channels. It enables organizations to personalize content, streamline workflows, and connect employees regardless of location, supporting both desk-based and frontline workers.

The platform's business continuity and disaster recovery measures are built entirely on Microsoft Azure's resilient architecture. Customer data is stored in logically segregated Azure SQL databases and storage accounts, encrypted at rest using AES-256 and in transit with TLS 1.2 or above. Continuous backups allow point-in-time recovery for 35 days, and domain controller snapshots are retained for seven days within a secondary availability set. Azure geo-replication and availability-zone failover capabilities ensure high resilience, with regular restore drills verifying recovery point objectives measured in minutes and recovery time objectives aligned to mission-critical uptime. Unily maintains a tested business continuity plan and an annual disaster recovery exercise as part of its ISO 27001:2022 and SOC 2 Type II-certified Information Security Management System.

Comprehensive onboarding support includes a structured, role-based five-phase implementation model (Initiate, Define, Design, Configure, Launch), culminating in steady-state assistance from a named Customer Success Manager. The implementation process incorporates workshops, governance and content strategy sessions, platform configuration, phased rollout (beta, pilot, full go-live), just-in-time training, and adoption planning. Offboarding is conducted under the Master Subscription Agreement, with all customer data returned or deleted within 35 days of contract termination, supported by a single comprehensive data export at no cost.

Service constraints typically relate to planned maintenance and to governance frameworks. Planned maintenance windows average 15 minutes per event and are scheduled out of peak hours with prior notice, while unplanned outages average 40 minutes and are communicated in real time via the Service Portal. The level of customization is governed by the licensed modules and the Extend framework, which supports deep customizations—including bespoke widgets, integrations, and layouts—within enterprise-grade governance and performance safeguards.

Service levels include a 99.95 percent uptime SLA across production, staging, and licensed environments, with global performance monitoring ensuring typical response times under three seconds, subject to client-side customizations. Support hours for standard service are 9x5 for P2–P4 priorities, with 24x7 coverage for critical P1 incidents; Premium Support extends hours and accelerates SLAs. Availability and SLA metrics are tracked via Datadog and custom tooling, and breaches are visible through the Service Portal.

After-sales support is delivered through the Customer Success Program, which includes adoption reviews, analytics insights, regular business reviews, roadmap access, training resources, and a secure customer portal (Universe) containing release notes, guides, and a Feature Store for self-service enablement.

Technical requirements focus on integration with the customer's identity provider (Azure Entra ID or equivalent SAML/OIDC solution) for single sign-on, MFA, and user provisioning. Unily is accessed via modern web browsers and native iOS/Android apps, with optional mobile device management integration.

Outage and maintenance management follows formal change-control processes with feature toggles, staged rollouts, and root-cause analysis for major incidents. Planned outages are announced with at least seven days' notice; unplanned outages trigger immediate incident response aligned to SLA priorities.

Hosting is exclusively in Microsoft Azure, with regional data center options in the UK/EMEA, US, and APAC to meet data residency requirements.

Access to data upon exit is via a full export at the point of termination, allowing retrieval of all platform content, user data, and media in a structured format, with secure transfer under customer instruction. This is in the form of a BacPac file.

Security is enforced through ISO 27001:2022 and SOC 2 Type II-certified controls, including role-based access, least-privilege administration, MFA, segregated environments, industry-standard encryption, continuous vulnerability management, SIEM-monitored audit logging, and a documented incident response plan. Customer data is processed within chosen legal boundaries, governed by data protection

agreements that meet GDPR, CCPA, and HIPAA requirements, ensuring confidentiality, integrity, and availability throughout the service term.