ALERTUS TECHNOLOGIES SERVICE LEVEL AGREEMENT FOR MANAGED-HOSTED SERVER DEPLOYMENTS

Version: 2026.01.21
Last Updated: **January 21, 2026**

This Service Level Agreement ("SLA") describes certain operational standards applicable to managed-hosted, sometimes referred to as cloud-hosted, deployments of the Alertus Server Software. This SLA is incorporated by reference into and forms part of the Alertus Master Terms and Conditions (the "Master Terms") between Alertus Technologies, LLC ("Alertus") and the purchasing entity ("Customer"). Capitalized terms not defined herein have the meanings set forth in the Master Terms or the End User License Agreement ("EULA").

1. **SCOPE**. This SLA applies solely to deployments of the Alertus Server Software hosted by Alertus in a third-party cloud environment ("Managed-Hosted Deployments"), sometimes referred to in documentation as the Alertus Critical Communication Suite ("ACCS"). Managed-Hosted Deployments consist of a customer-dedicated server environment managed by Alertus as an alternative to an on-premises deployment. This SLA addresses hosting-level operational standards only and does not establish support, response, or resolution commitments.

2. **MANAGED-HOSTED SERVICES.** As part of a Managed-Hosted Deployment, Alertus performs certain managed hosting activities, which may include:

    a. initial server provisioning and configuration;

    b. continuous monitoring of server availability and system health;

    c. installation of generally available Alertus software updates and patches;

    d. operating system updates consistent with standard Windows Server deployment practices; and

    e. routine backup and disaster-recovery preparation.

    Managed-Hosted Deployments are maintained in accordance with Alertus' standard operational practices. Any customer-specific security controls, compliance requirements, or deviations from these practices must be expressly agreed in writing.

3. **HOSTING INFRASTRUCTURE.** Managed-Hosted Deployments are hosted using Amazon Web Services ("AWS") or another third-party hosting provider selected by Alertus. Alertus manages the hosted Alertus Server environment, while the underlying cloud infrastructure remains subject to the hosting provider's own service terms and performance commitments. Customer-dedicated server instances are hosted in AWS regions selected by Alertus based on operational considerations, which may include proximity to Customer's primary operations. Alertus will notify Customer in writing if the third-party hosting provider materially changes.

4. **AVAILABILITY TARGET.** Alertus will use commercially reasonable efforts to make the cloud-hosted Alertus Server Software available approximately 99.0% of the time on a

monthly basis, excluding Excluded Downtime. Availability measurements are provided for transparency purposes only and do not constitute a warranty or guarantee.

5. **SCHEDULED AND EMERGENCY MAINTENANCE.**

    a. **Scheduled Maintenance**. Alertus may perform scheduled maintenance from time to time and will use commercially reasonable efforts to provide advance notice through the Alertus Customer Portal and/or email or other comparable communication methods.

    b. **Emergency Maintenance**. Alertus may suspend or restrict access to a Managed-Hosted Deployment without prior notice to address security threats, system integrity issues, or emergency network repairs. Alertus will use commercially reasonable efforts to restore service promptly.

6. **DISASTER RECOVERY.** For Managed-Hosted Deployments, Alertus maintains the following disaster-recovery objectives:

    a. **Recovery Time Objective (RTO)**: approximately one (1) hour following a qualifying disaster event.

    b. **Recovery Point Objective (RPO)**: restoration to the most recent backup, which is typically performed daily.

    These objectives are targets only and do not constitute guarantees.

7. **CUSTOMER RESPONSIBILITIES.** Customer is responsible for:

    a. maintaining accurate administrative and technical contact information;

    b. managing DNS registration and SSL certificates, if Customer elects to use a Customer-controlled domain;

    c. ensuring Authorized Users maintain appropriate credentials and access controls; and

    d. complying with all usage, configuration, and security obligations set forth in the Master Terms and EULA.

8. **SUPPORT REQUESTS.** This SLA does not establish support response times or resolution commitments. Support services, if purchased, are governed exclusively by the applicable support agreement, Enhanced Notification Services (“ENS”) terms, or SLA referenced in the Master Terms.

9. **EXCLUDED DOWNTIME.** “Excluded Downtime” includes any unavailability, suspension, or degradation caused by:

    a. events beyond Alertus’ reasonable control, including force majeure events, Internet backbone failures, or AWS outages;

    b. actions or omissions of Customer or any third party not under Alertus’ direct control;

c. Customer-managed systems, networks, integrations, DNS configuration, or SSL certificates;

d. scheduled or emergency maintenance; or

e. suspension or termination of services as permitted under the Master Terms.

10. **NO SERVICE CREDITS OR REMEDIES.** Alertus will use commercially reasonable efforts to meet the service levels described in this SLA. No service credits, refunds, or other remedies are provided under this SLA. This SLA is intended solely to describe operational practices and does not modify the warranties, disclaimers, or limitation of liability set forth in the Master Terms or EULA.

11. **RELATIONSHIP TO OTHER AGREEMENTS.** In the event of any conflict between this SLA and the Master Terms or EULA, the Master Terms control. Nothing in this SLA expands Alertus' obligations or Customer's remedies beyond those expressly set forth in the Agreement.