

Agile Unternehmen

Digitale Arbeit: zwischen Mensch und KI

AGILETICS AG | CLOUDSERVICECHECK MUSTERAKTE

Sicherheits- und Betriebskonzept

NimbusCollab Enterprise - EU-Service-Region

Wichtiger Demo-Hinweis

Das Dokument beschreibt fiktive technische und organisatorische Massnahmen. Es ist kein Nachweis ihrer tatsächlichen Wirksamkeit.

Metadatum	Angabe
Dokument	NW-SEC-CONCEPT-2026
Herausgeber	NimbusWorks GmbH - Security Engineering
Version	Version 5.1
Stand	2. Juli 2026
Klassifizierung	Kundenvertraulich - Demo

Dieses Musterdokument wurde ausschliesslich fuer die CloudServiceCheck-Kundendemo erstellt. Aussagen, Organisationen, Leistungen, Pruefungen und Vertragsklauseln sind vollstaendig fiktiv.

1. Shared Responsibility

Verantwortlichkeiten im Betriebsmodell

Anbieter und Kunde tragen unterschiedliche, miteinander verbundene Verantwortlichkeiten.

Bereich	NimbusWorks / Musterwerke
Infrastruktur	NimbusWorks: Plattform, Netzwerk, Hostsysteme und Basisdienste
Tenant-Konfiguration	Musterwerke: SSO, MFA-Policy, Rollen, Freigaben und externe Partner
Datenklassifizierung	Musterwerke: zulaessige Inhalte, Aufbewahrung und fachliche Loeschregeln
Protokollierung	NimbusWorks: Erzeugung; Musterwerke: Export, Langzeitaufbewahrung und Auswertung
Vorfallbearbeitung	Gemeinsam: Anbieteranalyse und Kundenbewertung/Meldung

Positive Abgrenzung

Die Responsibility-Matrix benennt die wichtigsten technischen Schnittstellen und verhindert eine pauschale Verantwortungsuebertragung.

2. IAM

Identitäten und privilegierte Zugriffe

NimbusCollab Enterprise unterstützt SAML-SSO und SCIM; privilegierte Rollen unterliegen erhöhten Schutzmassnahmen.

- MFA ist fuer alle privilegierten Anbieteradministratoren technisch erzwungen.
- Im Enterprise-Tenant ist MFA fuer Kundenadministratoren verpflichtend und kann nicht deaktiviert werden.
- Supportzugriffe sind ticketgebunden, zeitlich befristet und werden protokolliert.
- Musterwerke muss Fachrollen und externe Projektpartner mindestens quartalsweise pruefen.
- Notfallzugriffe werden durch ein getrenntes Bereitschaftsteam freigegeben und nachtraeglich kontrolliert.

Starker Nachweis

Die verpflichtende privilegierte MFA ist fuer die eingesetzte Enterprise-Edition eindeutig beschrieben.

3. Kryptografischer Schutz

Verschluesselung und Schluessel

Kundendaten werden bei Uebertragung und Speicherung mit dokumentierten Verfahren geschuetzt.

Schutz	Umsetzung
Transport	TLS 1.2 oder TLS 1.3; veraltete Protokolle sind deaktiviert
Speicherung	AES-256 fuer Datenbanken, Objekt- und Sicherungsspeicher
Schluessel	Getrennte Verwaltung in einem zentralen Key-Management-System
Rotation	Regelmaessige Rotation nach internem Kryptokonzept
BYOK	Optionales Enterprise-Zusatzmodul, nicht im Basispreis enthalten

Die Verschluesselung schuetzt nicht vor berechtigten Anwendungs- oder Supportzugriffen. Rollen, Freigaben und Protokollierung bleiben deshalb erforderlich.

4. Audit Logs

Protokollierung und Aufbewahrung

Administrative und sicherheitsrelevante Tenant-Ereignisse werden zentral erzeugt und ueber eine Export-API bereitgestellt.

- Standardaufbewahrung im Dienst: 90 Tage.
- Zeitstempel werden ueber zentrale, ueberwachte Zeitquellen synchronisiert.
- Export ueber API oder taegliche Dateiablage ist in Enterprise enthalten.
- Musterwerke muss den Export aktivieren, Zielsystem und laengere Aufbewahrungsdauer konfigurieren.
- NimbusWorks ueberwacht nicht, ob ein kundenseitiges SIEM die exportierten Ereignisse tatsaechlich empfaengt.

Offene Kundenmassnahme

Die Anbieterfunktion ist vorhanden. Die geforderte Aufbewahrung und End-to-End-Ueberwachung werden erst durch die Kundenkonfiguration wirksam.

5. Backup

Datensicherung und Wiederherstellung

NimbusWorks erstellt laufende Sicherungen und prueft die technische Wiederherstellbarkeit nach einem internen Testplan.

Merkmal	Beschreibung
Sicherungen	Taegliche inkrementelle und woechentliche Vollsicherung
Region	Verschlusselte Speicherung innerhalb EU/EWR
Restoretests	Quartalsweise Stichproben mit technischer und fachlicher Abschlussbestaetigung
Internes Ziel	RTO 8 Stunden, RPO 24 Stunden; keine vertragliche Zusage
Kundenexport	Optionaler Export fuer kundeneigene Sicherung

Widerspruch pruefen

Das Konzept beschreibt vollstaendige Abschlussbestaetigungen. Der fiktive C5-Bericht nennt fuer zwei Stichproben fehlende Nachweise.