

ECHOWORX

SICHERHEITS BEHÖRDEN

Wie Echoworx **Gewährleistet Datenschutz und Sicherheit**

Echoworx verpflichtet sich, ein Höchstmaß an Sicherheit, Kontrollen und Integrität bereitzustellen, um seine Cloud-Sicherheitservices zu unterstützen. Die folgende umfassende Liste von Programmen, Zertifizierungen und Akkreditierungen, die von Echoworx geführt werden, unterstreicht das Engagement unseres Unternehmens, Sicherheit und Datenintegrität in jeden Bereich unseres Geschäfts zu integrieren.

Etablierte jährliche SOC 2-Audits und Berichterstattung

- Die Prozesse, Verfahren und Kontrollen von Echoworx zum Schutz der Privatsphäre und Vertraulichkeit der Nutzer wurden formell von einer unabhängigen Wirtschaftsprüfungs- und Auditgesellschaft bewertet und getestet. Dies gilt ebenso für die Sicherheit, Verfügbarkeit und Integrität der Verarbeitung unserer Systeme.

PCI DSS Level 1 Zertifiziert

- Erhöht die Sicherheit von Zahlungskontodaten
- Entwickelt vom PCI Security Standards Council
- Weitere Informationen finden [Sie auf der offiziellen Website](#).

Amazon Web Services (AWS)-qualifizierte Software

- Wird an Unternehmen vergeben, die das AWS Foundational Technical Review (FTR) erfolgreich abgeschlossen haben.
- Stellt sicher, dass Produkte und Lösungen von AWS-Partnern definierte Anforderungen in den Bereichen Sicherheit, Zuverlässigkeit und operative Exzellenz erfüllen, wie sie im AWS Well-Architected Framework festgelegt sind.
- [Klicken Sie hier](#), um zu sehen, was die AWS-Validierung umfasst.

Registrierung im Financial Services Qualification System(FSQS)

- Als registrierter FSQS-Lieferant hat Echoworx die Einhaltung der FSQS-Standards nachgewiesen. Diese Standards sind in einem strengen Bewertungssystem organisiert, das darauf ausgelegt ist, das inhärente Risiko von Echoworx in zentralen Risikokontrollbereichen zu bewerten, darunter Cybersicherheit, Datenschutz, Informationssicherheit, Business Continuity, Finanzkriminalität, Conduct Risk, Finanzen, Recht und unternehmerische Verantwortung.
- [Klicken Sie hier](#), um die FSQS-Zertifizierungen von Echoworx für das [Vereinigte Königreich, Irland](#) oder [Nordeuropa einzusehen](#).
- Weitere Informationen zum FSQS, [Sie auf der offiziellen Website von Hellios](#).

OpenID Connect RP

- Eine exklusive Gruppe von weniger als 30 Organisationen. Diese Auszeichnung wird nach erfolgreichem Abschluss einer Reihe von Konformitätstests und der Verifizierung der cloudbasierten E-Mail-Verschlüsselung vergeben. Sie stellt sicher, dass die E-Mail-Verschlüsselung von Echoworx den Industriestandards für Authentifizierungsprotokolle entspricht. Weitere Informationen finden [Sie auf der offiziellen Website](#).

Wie Echoworx Gewährleistet Datenschutz und Sicherheit

Rechenzentren

- Echoworx verfügt über Rechenzentren in den USA, im Vereinigten Königreich, in Deutschland, Irland und Kanada, sodass Kundendaten geografisch nah am jeweiligen Einsatzort verbleiben können.
- Alle Rechenzentren sind nach höchsten Standards konzipiert.
- Sie werden ohne Kompromisse bei Sicherheit oder Redundanz geplant und betrieben.
- Die Rechenzentren sind für physische, systembezogene und operative Sicherheit nach SOC 2, PCI DSS und ISO zertifiziert.
- Alle Geschäftsprozesse folgen bewährten Sicherheitspraktiken und beschränken den Zugriff auf Kundeninformationen.
- Echoworx überprüft kontinuierlich die Sicherheit und die von den Rechenzentren bereitgestellten Services, um für seine Kunden bestmögliche Sicherheit zu gewährleisten.

Kryptografie

Echoworx verwendet in seinen Produkten die folgenden Verschlüsselungsstandards:

- RSA 2048-Bit asymmetrische Verschlüsselung
- RSA PKCS kryptografische Protokolle: PKCS#1, #7, #10, #12
- AES-256 symmetrische Verschlüsselung
- SHA-2 Hashing-Algorithmus
- ANSI X.509-Zertifikate und Zertifikatsperrlisten
- IETF MIME und S/MIME für E-Mail

Bereitstellung

Echoworx stellt Verschlüsselungsservices auf höchstmögliche sichere Weise bereit.

- Cloud-gehostete Komponenten werden in zertifizierten, sicheren Tier-1-Rechenzentren bereitgestellt und betrieben.
- Servicekomponenten werden in physisch gestaffelten Sicherheitszonen eingesetzt, wobei direkter öffentlicher Zugriff ausschließlich auf die äußerste Zone beschränkt ist.
- Frontend-Zugangsdienste sind von den operativen Mid-Tier-Komponenten getrennt, und diese wiederum sind von den sensibelsten Informationswerten separiert, etwa privatem Schlüsselmateriale und gehashten Zugangsdaten.
- Diese Trennung wird durch mehrere Firewalls mit strikt konfigurierten Richtlinien umgesetzt.
- Intrusion-Detection-Systeme wurden mit Echtzeitwarnungen implementiert, um das zuständige Personal unverzüglich über etwaige Vorfälle zu informieren.

Hardware-Sicherheitsmodule (HSM)

Der AWS Key Management Service (AWS KMS) erleichtert die Erstellung und Verwaltung kryptografischer Schlüssel sowie die Kontrolle ihrer Nutzung über eine Vielzahl von AWS-Services und Anwendungen hinweg. Echoworx integriert AWS KMS, um anwendungsspezifische Daten über die KMS-API sicher zu verschlüsseln und zu verwalten. AWS KMS basiert auf manipulationssicheren Hardware-Sicherheitsmodulen (HSMs), die nach FIPS 140-3 Security Level 3 validiert sind.

Von AWS KMS verwaltete Schlüssel – einschließlich der Schlüssel für Portal, PGP und S/MIME – werden ausschließlich im Speicher der HSMs gehalten, was ein hohes Maß an Sicherheit gewährleistet. Diese Funktionen basieren auf der bewährten Infrastruktur von AWS KMS und entsprechen Verschlüsselungsstandards wie AES-256, wodurch Vertrauen und Compliance für Ihre sensibelsten Workloads unterstützt werden. Mehr über AWS KMS erfahren [Sie hier](#).

Richtlinien- und Verfahrens- Highlights

Nachfolgend sind Beispiele für die Richtlinien und Verfahren von Echoworx aufgeführt:

Sicherheitsmanagement

Echoworx unterhält eine unternehmensweite Sicherheitsrichtlinie, die veröffentlicht und im Rahmen des Programms zur Sensibilisierung der Mitarbeitenden für Sicherheit kommuniziert wird. Die Richtlinie definiert die Ziele, den Geltungsbereich, die Absicht und die Grundsätze der Informationssicherheit und stellt die Einhaltung regulatorischer Anforderungen sicher.

Insbesondere behandelt die Sicherheitsrichtlinie folgende Bereiche der Informationssicherheit:

- Einhaltung regulatorischer, gesetzlicher und vertraglicher Anforderungen
- Vorgaben für die Sicherheitsschulungsanforderungen der Mitarbeitenden
- Computersicherheit zur Verringerung von Schwachstellen und Risiken, z. B. zur Verhinderung von Softwareviren oder Schadsoftware und zum Schutz vor Datenverlust
- Geschäftskontinuität sowie die Verantwortung von Management und Mitarbeitenden
- Durchsetzung der Compliance und Konsequenzen bei Verstößen gegen Richtlinien

Das Information Security Management System von Echoworx basiert auf einem Modell der kontinuierlichen Weiterentwicklung durch:

- die Erstellung von Richtlinien, Verfahren und Standards zur Aufrechterhaltung der physischen und logischen Sicherheit in den Einrichtungen von Echoworx
- die Durchführung jährlicher Risikobewertungen zur Identifizierung von Sicherheitsauswirkungen und Anforderungen an Sicherheitskontrollen
- die Beauftragung externer Auditoren zur Bewertung und Berichterstattung über unsere Kontrollen und etwaige Schwachstellen
- die Regelung von Sicherheitsanforderungen und Zuständigkeiten durch Verträge und Verfahren zwischen den beteiligten Parteien
- die Aktualisierung von Richtlinien, Verfahren und Standards auf Grundlage der Ergebnisse von Risikobewertungen und Audits



Richtlinien- und Verfahrens- Highlights

Physische Sicherheitskontrollen

Alle kritischen Sicherheitsoperationen finden in einer physisch gesicherten Einrichtung statt, die mindestens vier Sicherheitsebenen für den Zugriff auf sensible Hardware oder Software umfasst. Sensible Systemkomponenten sind physisch von den übrigen Systemen der Organisation getrennt, sodass nur autorisierte Mitarbeitende von Echoworx Zugriff darauf haben.

Der physische Zugang zum System ist streng kontrolliert und unterliegt einer kontinuierlichen elektronischen Überwachung rund um die Uhr. Zugang erhalten ausschließlich vertrauenswürdige Personen mit einem legitimen geschäftlichen Bedarf. Das Zutrittskontrollsystem ist jederzeit funktionsfähig; zusätzlich zu elektronischen Kartenlesern wird auch biometrische Authentifizierung eingesetzt.

Alle Sicherheitssysteme von Echoworx verfügen über branchenübliche redundante Stromversorgungs- und Klimatisierungssysteme, um eine geeignete Betriebsumgebung sicherzustellen.

Für alle Sicherheitssysteme von Echoworx werden angemessene Vorkehrungen getroffen, um die Auswirkungen von Wassereinwirkung zu minimieren. Darüber hinaus sind branchenübliche Mechanismen zur Brandverhütung und zum Brandschutz implementiert.

Abfälle werden gemäß den Anforderungen von Echoworx zur Entsorgung beseitigt. Kryptographische Geräte werden vor der Entsorgung entsprechend den Herstelleranweisungen physisch zerstört oder auf Null gesetzt.

Kontrollen zum Business Continuity Management

Echoworx verfügt über einen Business-Continuity- und Disaster-Recovery-Plan, der darauf ausgelegt ist, Ausfälle nach Unterbrechungen oder dem Ausfall kritischer Geschäftsprozesse und Systeme zu minimieren beziehungsweise weitgehend zu vermeiden.

Die Services von Echoworx sind innerhalb jeder jeweiligen geografischen Region vollständig redundant ausgelegt, und Daten werden in Echtzeit für Zwecke der Notfallwiederherstellung repliziert.

Die Wirksamkeit der Business-Continuity- und Disaster-Recovery-Pläne wird mindestens einmal jährlich mit geeigneten Methoden getestet.

Richtlinien- und Verfahrens- Highlights

Akkreditierungen des Service Providers

Das Management der Root-Certificate-Authority-Schlüssel – einschließlich Erzeugung, Schutz und Vernichtung – sowie das Management der Subscriber-Schlüssel – einschließlich der Erzeugung untergeordneter Schlüssel, Speicherung, Sicherung, Wiederherstellung und Vernichtung – erfolgt über ein **Luna C3 Hardware Security Module (HSM)**. Das Gerät ist **FIPS 140-2 Level 3**-konform und gemäß **Common Criteria Evaluation Assurance Level 4+ (EAL 4+)** validiert.

Die Services von Echoworx werden über einen weltweit anerkannten und vertrauenswürdigen Rechenzentrumsanbieter bereitgestellt, der die folgenden geprüften Akkreditierungen erreicht hat:

- **Payment Card Industry Data Security Standard (PCI DSS)** – konformer **Level 1 Service Provider**
- **SSAE 16 SOC 2 Type II** (ersetzt das frühere **SAS 70 Audit**)
- **ISO 27001:2022**

Personalsicherheit

Sicherheitsrollen und Zuständigkeiten für das Echoworx-Team sind in den Stellenbeschreibungen des Unternehmens detailliert dokumentiert. Überprüfungen relevanter Mitarbeitender von Echoworx werden bereits im Rahmen des Bewerbungsprozesses durchgeführt. Die Richtlinien und Verfahren von Echoworx legen fest, dass Hintergrundprüfungen und Freigabeverfahren für Personen in vertrauenswürdigen Rollen sowie für weiteres Personal erforderlich sind. Alle Mitarbeitenden von Echoworx müssen als Teil ihrer anfänglichen Beschäftigungsbedingungen eine Vertraulichkeitsvereinbarung (Geheimhaltungsvereinbarung) unterzeichnen.

Die Kontrollen für externes bzw. vertraglich gebundenes Personal umfassen unter anderem:

- Bürgschafts- bzw. Absicherungsanforderungen für Vertragspersonal
- Vertragliche Anforderungen, einschließlich Schadloshaltung bei Schäden, die durch Handlungen des Vertragspersonals entstehen
- Auditierung und Überwachung von Vertragspersonal

Alle Mitarbeitenden von Echoworx sowie vertraglich gebundene Mitarbeitende erhalten angemessene Schulungen, um das Bewusstsein zu stärken und die Einhaltung der unternehmensweiten Sicherheitsrichtlinien sicherzustellen. Diese Schulungen sind an klar definierten rollenbasierten Compliance- und Trainingsanforderungen ausgerichtet.

Für Mitarbeitende, die gegen organisatorische Sicherheitsrichtlinien und -verfahren verstoßen, besteht ein formaler Disziplinarprozess, der konsequent angewendet wird. Die Richtlinien und Verfahren von Echoworx legen Sanktionen für unbefugte Handlungen, unbefugte Nutzung von Befugnissen sowie unbefugte Nutzung von Systemen fest. Wenn ein Arbeitsverhältnis endet, werden angemessene und rechtzeitige Maßnahmen ergriffen, damit Kontrollen und Sicherheit dadurch nicht beeinträchtigt werden.

ECHOWORX™

IT PAYS TO BE SECURE

Echoworx schützt die Privatsphäre von Menschen und Unternehmen auf der ganzen Welt, indem wir den Schutz von E-Mail-Daten vereinfachen. Unsere anpassbare E-Mail-Verschlüsselungsplattform hilft Unternehmen dabei, geschützte E-Mails, Auszüge und Dokumente einfach von überall und von jedem Gerät aus zu versenden. Unsere engagierten Verschlüsselungsexperten bringen Ordnung in das Kommunikationschaos – für weltweit führende Organisationen, die wissen: Sicherheit zahlt sich aus.

Verschlüsselung ist eine Investition in die Marke und maximiert den Wettbewerbsvorteil.

Kunden in 30 Ländern nutzen Echoworx, und mehr als 5.000 Implementierungen in Unternehmen, im öffentlichen Sektor und in Institutionen werden über unsere Rechenzentren in den USA, Kanada, Deutschland, Irland und dem Vereinigten Königreich betreut.

Für weitere Informationen: www.echoworx.com

✉ info@echoworx.com

☎ Nordamerika 1 800.735.8916 | UK 44 808.134.9538