

ECHOWORX

SERVICES

DE SÉCURITÉ

Comment Echoworx **Garantit la confidentialité et la sécurité**

Echoworx s'engage à offrir le plus haut niveau de sécurité, de contrôles et d'intégrité pour soutenir ses services de sécurité infonuagique. La liste complète suivante des programmes, certifications et accréditations revendiqués par Echoworx démontre l'engagement de notre organisation à intégrer la sécurité et l'intégrité des données dans chaque aspect de ses activités.

Audit et rapports SOC 2 réalisés annuellement

- Les processus, procédures et contrôles d'Echoworx mis en œuvre pour protéger la confidentialité et la vie privée des utilisateurs ont été officiellement évalués et testés par un cabinet indépendant d'expertise comptable et d'audit. L'évaluation a également porté sur la sécurité, la disponibilité et l'intégrité du traitement de nos systèmes.

Certification PCI DSS niveau 1

- Courriel chiffré, plateforme sécurisée
- Renforce la sécurité des données des comptes de paiement
- Élaborée par le PCI Security Standards Council
[Pour plus d'information, consultez le site officiel.](#)

Logiciel qualifié Amazon Web Services (AWS)

- Attribué aux entreprises après la réussite de la revue technique fondamentale AWS (Foundational Technical Review, FTR).
- Garantit que les produits et solutions des partenaires AWS répondent à un ensemble précis d'exigences en matière de sécurité, de fiabilité et d'excellence opérationnelle, telles que définies par le cadre AWS Well-Architected.
- [Cliquez ici pour découvrir ce que couvre la validation AWS.](#)

Inscription au Financial Services Qualification System (FSQS) Registration

- En tant que fournisseur inscrit au FSQS, Echoworx a démontré sa conformité aux normes du FSQS. Ces normes reposent sur un cadre d'évaluation rigoureux conçu pour mesurer le risque inhérent d'Echoworx dans plusieurs domaines clés de contrôle des risques, notamment la cybersécurité, la protection des données, la sécurité de l'information, la continuité des activités, la criminalité financière, le risque de conduite, les volets financiers, juridiques et la responsabilité d'entreprise.
- Cliquez ici pour consulter les certifications FSQS d'Echoworx au [Royaume-Uni, en Irlande](#) et en [Europe du Nord](#).
- Pour en savoir plus sur le FSQS, [consultez le site officiel de Hellios](#).

OpenID Connect RP

- **Un groupe d'élite** de moins de 30 organisations.
Cette reconnaissance est accordée à l'issue réussie d'une série de tests de conformité et de la vérification de son chiffrement de courriels infonuagique.
Elle garantit que le chiffrement des courriels d'Echoworx est conforme aux normes de l'industrie en matière de protocoles d'authentification.
[Pour plus d'information, consultez le site officiel.](#)

Comment Echoworx **Garantit la confidentialité et la sécurité**

Centres de données

- Echoworx dispose de centres de données aux États-Unis, au Royaume-Uni, en Allemagne, en Irlande et au Canada, afin de garantir que les données des clients restent à proximité.
- Tous les centres de données sont conçus selon les normes les plus élevées.
- Ils sont conçus et maintenus sans compromis en matière de sécurité ou de redondance.
- Les centres de données sont certifiés SOC 2, PCI DSS et ISO pour la sécurité physique, la sécurité des systèmes et la sécurité opérationnelle.
- Tous les processus d'affaires suivent les meilleures pratiques en matière de sécurité et limitent l'accès aux renseignements des clients.
- Echoworx évalue en continu la sécurité et les services fournis par ses centres de données afin d'assurer à ses clients le plus haut niveau de sécurité possible.

Cryptographie

Echoworx utilise les normes de chiffrement suivantes dans ses produits

- asymétrique RSA 2048 bits
- protocoles cryptographiques RSA PKCS : PKCS #1, #7, #10 et #12
- chiffrement symétrique AES-256
- algorithme de hachage SHA-2
- certificats ANSI X.509 et listes de révocation de certificats
- normes IETF MIME et S/MIME pour les courriels.

Déploiement

Echoworx fournit des services de chiffrement selon les normes de sécurité les plus élevées.

- Les composants hébergés dans le cloud sont déployés et exploités dans des centres de données certifiés, sécurisés et de niveau 1.
- Les composants du service sont déployés dans des zones de sécurité physique en couches, l'accès public direct étant limité uniquement à la zone la plus externe.
- Les services d'accès en frontal sont séparés des composants opérationnels intermédiaires, eux-mêmes séparés des actifs informationnels les plus sensibles, tels que le matériel de clés privées et les informations d'identification d'accès hachées.
- Cette séparation est mise en œuvre au moyen de plusieurs pare-feu configurés selon des politiques strictes.
- Des systèmes de détection d'intrusion ont été déployés avec des alertes en temps réel afin d'aviser le personnel de tout incident.

Modules matériels de sécurité (HSM)

AWS Key Management Service (AWS KMS) facilite la création et la gestion de clés cryptographiques, ainsi que le contrôle de leur utilisation dans un large éventail de services et d'applications AWS. Echoworx s'intègre à AWS KMS afin de chiffrer et de gérer en toute sécurité des données propres aux applications au moyen de l'API KMS. AWS KMS repose sur des modules matériels de sécurité (HSM) résistants à l'altération, validés au niveau 3 de la norme FIPS 140-3.

Les clés gérées par AWS KMS, y compris celles utilisées pour le Portail, PGP et S/MIME, ne sont conservées qu'en mémoire dans les HSM, ce qui garantit un niveau de sécurité élevé. Reposant sur l'infrastructure éprouvée d'AWS KMS, ces fonctionnalités s'alignent sur des normes de chiffrement telles qu'AES-256, offrant confiance et conformité pour vos charges de travail les plus sensibles. Pour en savoir plus sur AWS KMS, [cliquez ici](#).

Politiques et procédures Points saillants

Exemples des politiques et procédures d'Echoworx présentés ci-dessous :

Gestion de la sécurité

Echoworx maintient une politique de sécurité d'entreprise qui est publiée et communiquée dans le cadre du programme de sensibilisation des employés à la sécurité. Cette politique définit les objectifs, la portée, l'intention et les principes de la sécurité de l'information, et veille au respect des exigences réglementaires.

Plus précisément, la politique de sécurité couvre les domaines suivants de la sécurité de l'information :

- la conformité aux exigences réglementaires, législatives et contractuelles
- les orientations relatives aux exigences de formation du personnel en matière de sécurité
- la sécurité informatique visant à réduire les vulnérabilités et les expositions, par exemple pour prévenir les virus informatiques ou les logiciels malveillants et pour protéger contre la perte de données
- la continuité des activités ainsi que les responsabilités de la direction et du personnel
- l'application des exigences de conformité et les conséquences en cas de non-respect des politiques.

Le système de gestion de la sécurité de l'information d'Echoworx repose sur un modèle d'amélioration continue qui consiste à :

- élaborer des politiques, des procédures et des normes pour maintenir la sécurité physique et logique dans les installations d'Echoworx
- réaliser des évaluations annuelles des risques afin d'identifier les impacts sur la sécurité et les exigences en matière de contrôles de sécurité
- faire appel à des auditeurs externes pour évaluer nos contrôles et rendre compte de toute faiblesse éventuelle
- encadrer les exigences et responsabilités en matière de sécurité au moyen de contrats et de procédures entre les parties
- mettre à jour les politiques, procédures et normes en fonction des résultats des évaluations des risques et des audits.



Politiques et procédures **Points saillants**

Contrôles de sécurité physique

Toutes les opérations de sécurité critiques ont lieu dans une installation physiquement sécurisée comportant au moins quatre couches de sécurité pour accéder au matériel ou aux logiciels sensibles. Les composants sensibles du système sont physiquement séparés des autres systèmes de l'organisation, de sorte que seuls les employés autorisés d'Echoworx peuvent y accéder.

L'accès physique au système est strictement contrôlé et fait l'objet d'une surveillance électronique continue, 24 heures sur 24 et 7 jours sur 7. Seules les personnes de confiance ayant une raison professionnelle valable obtiennent un accès. Le système de contrôle d'accès est en permanence opérationnel, et des lecteurs de badges électroniques ainsi qu'une authentification biométrique sont également utilisés.

Tous les systèmes de sécurité d'Echoworx sont dotés de systèmes redondants d'alimentation électrique et de climatisation conformes aux normes de l'industrie afin d'assurer un environnement d'exploitation adéquat.

Des précautions raisonnables sont prises pour minimiser les effets d'une exposition à l'eau sur l'ensemble des systèmes de sécurité d'Echoworx. Tous les systèmes de sécurité sont également équipés de mécanismes de prévention et de protection contre l'incendie conformes aux normes de l'industrie.

Les déchets sont éliminés conformément aux exigences d'Echoworx en matière d'élimination. Les dispositifs cryptographiques sont détruits physiquement ou remis à zéro conformément aux directives du fabricant avant leur mise au rebut.

Contrôles de gestion de la continuité des activités

Echoworx dispose d'un plan de continuité des activités et de reprise après sinistre conçu pour réduire au minimum, voire éliminer, les interruptions à la suite d'une perturbation ou d'une défaillance de processus et de systèmes d'affaires critiques.

Les services d'Echoworx sont entièrement redondants au sein de chaque région géographique donnée, et les données sont répliquées en temps réel à des fins de reprise après sinistre.

L'efficacité des plans de continuité des activités et de reprise après sinistre est testée au moins une fois par an au moyen de méthodes appropriées.

Politiques et procédures **Points saillants**

Accréditations du fournisseur de services

La gestion des clés de l'autorité de certification racine, y compris leur génération, leur protection et leur destruction, ainsi que la gestion des clés des abonnés, y compris la génération des clés subordonnées, leur stockage, leur sauvegarde, leur récupération et leur destruction, sont assurées par un module matériel de sécurité Luna C3 Hardware Services Module (HSM). Cet appareil est conforme à la norme FIPS 140-2 niveau 3 et a été validé selon le niveau 4+ de la Common Criteria Evaluation Assurance Level (EAL 4+).

Echoworx services are delivered utilizing a globally recognized and trusted data centre service provider, which has achieved the following audited accreditations: Les services d'Echoworx sont fournis par l'intermédiaire d'un fournisseur de centres de données reconnu et de confiance à l'échelle mondiale, ayant obtenu les accréditations vérifiées suivantes :

- Payment Card Industry Data Security Standard — fournisseur de services conforme au niveau 1 ;
- SSAE 16 SOC 2 Type II (remplace l'audit SAS 70 hérité) ;
- ISO 27001:2022.

Sécurité du personnel

Les rôles et responsabilités en matière de sécurité au sein de l'équipe Echoworx sont documentés en détail dans les descriptions de poste de l'entreprise. Des vérifications sont effectuées auprès des membres clés du personnel d'Echoworx au moment de leur candidature. Les politiques et procédures d'Echoworx précisent que des vérifications d'antécédents et des procédures d'habilitation sont requises pour le personnel occupant des rôles de confiance, ainsi que pour les autres employés. Tous les employés d'Echoworx doivent signer un accord de confidentialité (non-divulgaration) dans le cadre de leurs conditions initiales d'emploi.

Les contrôles applicables au personnel contractuel comprennent notamment :

- des exigences de cautionnement pour le personnel contractuel ;
- des exigences contractuelles, y compris une indemnisation pour les dommages résultant des actions du personnel contractuel ;
- l'audit et la surveillance du personnel contractuel.

Tous les employés d'Echoworx ainsi que les membres du personnel contractuel reçoivent une formation appropriée visant à renforcer la sensibilisation et à assurer la conformité aux politiques de sécurité de l'entreprise. Cette formation est alignée sur des exigences claires en matière de conformité et de formation fondées sur les rôles.

Un processus disciplinaire formel existe et est appliqué pour les employés ayant enfreint les politiques et procédures de sécurité de l'organisation. Les politiques et procédures d'Echoworx précisent les sanctions applicables au personnel en cas d'actions non autorisées, d'usage non autorisé de l'autorité ou d'utilisation non autorisée des systèmes. Des mesures appropriées et prises en temps opportun sont appliquées lorsqu'un employé quitte l'entreprise, afin que les contrôles et la sécurité ne soient pas compromis par une telle situation.

ECHOWORX™

IT PAYS TO BE SECURE

Echoworx protège la confidentialité des personnes et des entreprises partout dans le monde en simplifiant la protection des données de messagerie. Notre plateforme de chiffrement des courriels, hautement configurable, aide les organisations à partager facilement des courriels, relevés et documents protégés, où qu'elles se trouvent et depuis n'importe quel appareil. Nos experts passionnés en chiffrement transforment le chaos des communications en ordre pour des organisations de premier plan à travers le monde qui le savent bien : la sécurité est un investissement rentable.

Le chiffrement est un investissement dans la marque qui maximise l'avantage concurrentiel.

Des clients dans 30 pays utilisent Echoworx, et plus de 5 000 déploiements au sein d'entreprises, du secteur public et d'institutions sont pris en charge par nos centres de données situés aux États-Unis, au Canada, en Allemagne, en Irlande et au Royaume-Uni.

Pour en savoir plus www.echoworx.com