ECHOWORX™

IT PAYS TO BE SECURE

# Echoworx Security Services

# Table of contents

# Introduction

Echoworx commits to offering the highest level of security, controls, and integrity in support of their cloud security services. The extensive list of programs, certifications, and accreditations that Echoworx holds demonstrates their unwavering commitment to integrating security and data integrity into every aspect of their business.

## Security Assurance & Certification Programs

# Security Assurance and Certifications

### Apple Root Certificate Membership

- Protects Apple customers from security issues related to the use of public key infrastructure (PKI) certificates.
- Ensures a seamless experience for users on Mac OS and iOS devices when making secure web connections, generating secure emails, and performing other PKI interactions.
- Echoworx's membership in the Apple Root program establishes them as a trusted CA.

### AWS Qualified Software Certification

- Awarded to companies that successfully complete the AWS Foundational Technical Review (FTR).
- It ensures that Echoworx's products and solutions meet specific requirements based on security, reliability, and operational excellence, as defined by the AWS Well-Architected Framework.
- For more information on AWS Qualified Software certification, please visit the official site of AWS.

### Financial Services Qualification System (FSQS) Registration

- Echoworx, a registered FSQS supplier, demonstrates compliance with FSQS standards. The company adheres to strict guidelines that assess its inherent risk across key risk control areas, including cybersecurity, data privacy, information security, business continuity, financial crime, conduct risk, financial, legal, and corporate responsibility.
- FSQS evaluates Echoworx on an annual basis.
- Echoworx's FSQS certification can be viewed here.
- For more information on FSQS, please visit the official website of Hellios here.

# Security Assurance and Certifications

### G-Cloud 13 Approved Supplier for Cloud Software (SaaS) UK

- The Crown Commercial Service (CCS) acts as the largest public procurement organization in the UK, promoting the adoption of cloud-based services across the government.
- The primary purpose is to focus on security and maintain stringent standards to protect against cyber-attacks. CCS suppliers are required to have the most up-to-date security technology and software. Echoworx, as an approved CCS supplier, demonstrates its commitment to providing best-in-breed encryption services.
- Echoworx's CCS approval qualifies it as a trusted SaaS provider for UK public sector organizations.
- CCS evaluates Echoworx on an annual basis.
- For more information on CCS G-Cloud 13, visit the official website.

### Microsoft Trusted Root Certificate Program

- Consists of an elite group of less than 100 organizations.
- Microsoft performs Trusted Root evaluations of Echoworx on an annual basis.
- It guarantees trust in certificates issued by Echoworx.
- Subscribers can have confidence that the certificates issued by Echoworx are recognized and trusted.

### PCI DSS Level 1 Certified

- Secure Platform with Encrypted Mail
- Improves payment account data security.
- Requires annual assessments for certification, with stricter validation demands.
- Reserved for organizations processing more than six million transactions per year.

# Security Assurance and Certifications

### SOC 2 Type II Audits and Reports

- Formal evaluations and tests of processes, procedures, and controls are conducted by Echoworx on a yearly basis to ensure the protection of users' privacy and confidentiality.
- A security, availability, and processing integrity assessment of our systems is performed by an independent accounting and auditing company.
- The SOC2 Type II report specifically evaluates how well customer data is protected on our systems.

### Web Trust Certified

- The Echoworx Root CA integrity is assured.
- Key and certificate life cycle management controls are established.
- Ongoing maintenance and monitoring of controls.
- To access the WebTrust Seal of assurance, visit here and click on the WEB TRUST CERTIFIED logo.
- The full copy of the Echoworx Root CA2 Certificate Policies and Practices Statement, used in the annual audit process, can be found here.

# Data Centers

- Echoworx operates within the global infrastructure of AWS, spanning 32 geographic regions worldwide, including data centers located in the US, UK, Germany, Ireland, and Canada. Customer data remains in close proximity.
- The highest standards engineer and maintain all data centers, ensuring security and redundancy without compromise.
- Data centers have SOC2, PCI DSS, and ISO certifications for physical, system, and operational security.
- Security best practices are followed in all business processes, limiting access to customer information.
- Echoworx continuously reviews the security and services provided by its data centers to ensure the best possible security for customers.

# Cryptography

**Echoworx employs the following encryption standards in its products:**

- Utilizes RSA 2048-bit asymmetric encryption.
- Implements RSA PKCS cryptographic protocols, including PKCS#1, #7, #10, #12.
- Incorporates AES-256 symmetric encryption.
- Utilizes SHA2 hashing algorithm.
- Supports ANSI X.509 certificates and certificate revocation lists.
- Implements IETF MIME, S/MIME email, and OpenPGP.
- Supports TLS 1.2 protocol.

# Deployment

**Echoworx provides encryption services in the most secure manner.**

- It deploys and operates cloud-hosted components in certified, secure tier one datacenters. The service components are deployed into layered physical security zones, restricting direct public access to the outermost zone only.
- The front-end access services are separated from the mid-tier operational components, which are further separated from the most sensitive information assets, such as private key material and hashed access credentials.
- The company implements segregation using multiple firewalls configured with strict policies.
- Additionally, it has deployed intrusion detection systems with real-time alerts to notify personnel of any issues.

# Security Management

**Echoworx maintains a corporate security policy that it publishes and communicates through the employee security awareness program.** The policy defines the objectives, scope, intent, and principles of information security and ensures compliance with regulatory requirements.
In particular, the security policy addresses the following areas of information security:

- Compliance with regulatory, legislative, and contractual requirements is ensured.
- Staff's security training requirements are guided.
- Weaknesses and exposures in computer security, such as software viruses or malicious software, are reduced to prevent them and protect against data loss.
- Business continuity and responsibility of management and staff are emphasized.
- Policy violations are enforced, and consequences of non-compliance are applied.

**The Echoworx Information Security Management Systems is based on a continuous evolution model.** It achieves this by:

- Creating Policies, Procedures, and Standards to sustain physical and logical security in the Echoworx facilities.
- Performing Annual Risk assessments to identify security implications and security control requirements.
- Engaging External Auditors to evaluate and report on Echoworx's controls and any weaknesses.
- Addressing security requirements and responsibilities with contracts and procedures between parties.
- Updating Policies, Procedures, and Standards based on the results of the Risk Assessments and Audits.

# Physical Security Controls

**Physical security controls are in place at Echoworx to ensure all critical security operations occur within a physically secure facility.**

The facility has at least four layers of security to access sensitive hardware or software. Sensitive system components are physically separated from the organization's other systems, granting access only to authorized Echoworx employees.

Strict control is maintained over physical access to the system, which is continuously monitored through electronic surveillance (24/7). Access is granted only to trustworthy individuals with a valid business reason, utilizing functional access control systems that include electronic badge readers and biometric authentication.

Echoworx security systems are equipped with industry-standard redundant power and air conditioning systems to maintain a suitable operating environment. Additionally, reasonable precautions are taken to minimize the impact of water exposure, and fire prevention and protection mechanisms are implemented as per industry standards.

Waste disposal at Echoworx follows company requirements, ensuring cryptographic devices are physically destroyed or zeroized in accordance with manufacturers' guidance prior to disposal.

# Business Continuity Management Controls

**Echoworx maintains a business continuity and disaster recovery plan that minimizes and eliminates outages following interruptions or failures of critical business processes and systems.**

Within any given geographical region, Echoworx services are fully redundant, and data is replicated in real time for disaster recovery.
Echoworx tests the effectiveness of its business and disaster recovery plans at least once a year using appropriate methods.

# Service Provider Accreditations

Root Certificate Authority Key Management, including generation, protection, and destruction, and Subscriber Key Management, including subordinate key generation, storage, backup, recovery, and destruction, are performed by a Luna C3 Hardware Services Module (HSM). The device is compliant with FIPS 140-2 Level 3 and has been validated according to the Common Criteria Evaluation Assessment Level 4+ (EAL 4+).

Echoworx services utilize Amazon Web Services (AWS), a globally recognized and trusted data center service provider, which has achieved a variety of IT security standards including the following audited accreditations:

- Payment Card Industry Data Security Standards – Compliant Level 1 Service Provider
- SSAE 16 SOC2 Type II (replaces the legacy SAS 70 audit)
- SOC 1, 2, 3
- ISO 9001 / ISO 27001 / ISO 27017 / ISO 27018
- HITRUST
- FedRAMP
- CSA Security, Trust & Assurance Registry (STAR)

# Personnel Security

**The Echoworx team documents security roles and responsibilities in detail within company job descriptions.** Verification checks on key Echoworx staff members are performed during the job application process. Echoworx policies and procedures require background checks and clearance procedures for personnel in trusted roles and other staff members. All Echoworx employees must sign a confidentiality (nondisclosure) agreement as part of their initial terms and conditions of employment.

**All Echoworx employees and contracted staff receive appropriate training to raise awareness and ensure compliance with corporate security policies**. This training aligns with clear role-based compliance and training requirements.

Echoworx follows a formal disciplinary process for employees who violate organizational security policies and procedures. Echoworx policies and procedures specify sanctions against personnel for unauthorized actions, unauthorized use of authority, and unauthorized use of systems. Appropriate and timely actions are taken when an employee is terminated to ensure controls and security are not compromised.

ECHOWORX™

IT PAYS TO BE SECURE

Echoworx ensures top-level security, controls, and integrity for its cloud security services. With numerous programs, certifications, and accreditations, Echoworx unwaveringly integrates security and data integrity.

## Learn more:

Echoworx Email Encryption – Cryptographic Standards and Security

Discover Customer Success Stories

For more information, www.echoworx.com