ECHOWORX

SECURITY SERVICES

ECHOWORX™

IT PAYS TO BE SECURE

How Echoworx **Ensures Privacy & Security**

Echoworx is committed to providing the highest level of security, controls, and integrity to support our cloud security services. The following comprehensive list of programs, certifications, and accreditations claimed by Echoworx demonstrates our organization's commitment to integrating security and data integrity into every facet of our business:

Established Annual – SOC2 Auditing and Reporting

- Echoworx's processes, procedures, and controls employed to protect the privacy and confidentiality of users have been formally evaluated and tested by an independent accounting and auditing company, as well as the security, availability, and processing integrity of our systems.

PCI DSS Level 1 Certified

- Encrypted Mail, Secure Platform
- Enhances payment account data security
- Developed by PCI Security Standards Council
  For more information, visit the official website.

AWS Qualified

- Awarded to companies upon successful completion of the AWS Foundational Technical Review (FTR).
- Ensures that AWS Partner products and solutions meet a specific set of requirements based around security, reliability and operational excellence, as defined by the AWS Well-Architected Framework.
- For more information on AWS Qualified Software certification, visit the official AWS website.

Financial Services Qualification System (FSQS) Registration

- As a registered FSQS supplier, Echoworx has demonstrated compliance with FSQS standards. These standards are organized into a strict rubric of guidelines designed to assess the inherent risk of Echoworx across key risk control areas, including cybersecurity, data privacy, information security, business continuity, financial crime, conduct risk, financial, legal, and corporate responsibility.
- Click here to see Echoworx's FSQS certification.
- For more information on the FSQS, visit the official Hellios website.

OpenID Connect RP

- An elite group of less than 30 organizations. Awarded upon successful completion of a series of conformance tests and verification of its cloud-based email encryption. Ensures that Echoworx email encryption complies with industry standards for authentication protocols. For more information visit the official website.

How Echoworx **Ensures Privacy & Security**

Data Centers

- Echoworx has data centers in the US, UK, Germany, Ireland, and Canada, ensuring customer data stays close to home.
- All the data centers are engineered to the highest standards.
- They are designed and maintained without compromise for security or redundancy.
- Data centers are SOC2, PCI DSS and ISO certified for physical, system, and operational security
- All business processes follow security best practices and limit access to customer information.
- Echoworx continuously reviews the security and services provided by their data centers to ensure the best possible security for their customers.

Cryptography

Echoworx utilizes the following encryption standards in its products:

- RSA 2048-bit asymmetric encryption
- RSA PKCS cryptographic protocols; PKCS#1, #7, #10, #12
- AES-256 symmetric encryption
- SHA2 hashing algorithm
- ANSI X.509 certificates and certificate revocation lists
- IETF MIME and S/MIME email

Deployment

Echoworx provides encryption services in the most secure manner.

- Cloud-hosted components are deployed and operated in certified, secure tier one datacenters.
- Service components are deployed into layered physical security zones, with direct public access restricted to the outermost zone only.
- Front-end access services are separated from mid-tier operational components, which are separated from the most sensitive information assets, such as private key material and hashed access credentials.
- Segregation is implemented using multiple firewalls configured with strict policies.
- Intrusion detection systems have been deployed with real time alerts to notify personnel of any issues.

Hardware Security Modules (HSM)

AWS Key Management Service (AWS KMS) makes it easy to create and manage cryptographic keys and control their use across a wide range of AWS services and applications. Echoworx integrates with AWS KMS to securely encrypt and manage application-specific data using the KMS API. AWS KMS is powered by tamper-resistant hardware security modules (HSMs) that are FIPS 140-3 Security Level 3 validated.

Keys managed by AWS KMS, including those for Portal, PGP, and SMIME, are only ever held in the memory of the HSMs, ensuring high levels of security. Built on proven AWS KMS infrastructure, these features align with encryption standards such as AES-256, providing trust and compliance for your most sensitive workloads. Learn more about AWS KMS here.

Policy and Procedure **Highlights**

Examples of the Echoworx policy and procedures are highlighted below:

Security Management

Echoworx maintains a corporate security policy which is published and communicated via 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
- Guidance for security training requirements of staff
- Computer security to reduce weaknesses and exposures, e.g., to prevent software viruses or malicious software and to protect against data loss
- Business continuity and responsibility of management and staff
- Compliance enforcement and consequences of policy violations

The Echoworx Information Security Management Systems is based on a continuous evolution model 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 our 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 Risks Assessments and Audits

Policy and Procedure **Highlights**

Physical Security Controls

All critical security operations take place within a physically secure facility with at least four layers of security to access sensitive hardware or software. Sensitive system components are physically separated from the organization's other systems so that only authorized Echoworx employees can access them.

Physical access to the system is strictly controlled and is subject to continuous (24/7) electronic surveillance monitoring. Only trustworthy individuals with a valid business reason are provided access. The access control system is always functional and electronic badge readers in addition to biometric authentication are also used.

All Echoworx security systems have industry standard redundant power and air conditioning systems to provide a suitable operating environment.

All Echoworx security systems have reasonable precautions taken to minimize the impact of water exposure.

All security systems have industry standard fire prevention and protection mechanisms in place.

Waste is disposed of in accordance with Echoworx waste disposal requirements. Cryptographic devices are physically destroyed or zeroized in accordance with the manufacturers' guidance prior to disposal.

Business Continuity Management Controls

Echoworx has a business continuity and disaster recovery plan designed to minimize and vastly eliminate outages following interruptions to, or failure of, critical business processes and systems.

Echoworx services are fully redundant within any given geographical region and data is replicated in real time for disaster recovery.

The effectiveness of business and disaster recovery plans are tested a minimum of once a year with appropriate methods.

Policy and Procedure **Highlights**

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 are delivered utilizing a globally recognized and trusted data centre service provider, which has achieved 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)
- ISO27001:2022

Personnel Security

Security roles and responsibilities for the Echoworx team are documented in detail in company job descriptions. Verification checks on key Echoworx staff members are performed at the time of job application. Echoworx policies and procedures specify that background checks and clearance procedures are required for the personnel filling the trusted roles, and other personnel. All Echoworx employees are required to sign a confidentiality (nondisclosure) agreement as part of their initial terms and conditions of employment.

Contracted personnel controls include the following:

- Bonding requirements on contract personnel
- Contractual requirements including indemnification for damages due to the actions of the contractor personnel
- Audit and monitoring of contractor personnel

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

A formal disciplinary process exists and is followed for employees who have violated organizational security policies and procedures. Echoworx policies and procedures specify the 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 so that controls and security are not impaired by such an occurrence.

ECHOWORX™

IT PAYS TO BE SECURE

Echoworx protects the privacy of people and businesses throughout the world by making email data protection easier. Our customizable email encryption platform helps organizations easily share protected email, statements, and documents from anywhere and from any device. Our passionate encryption experts transform communication chaos into order for world leading organizations who understand — it pays to be secure.

Encryption is an investment in brand, maximizing competitive advantage.

Clients in 30 countries use Echoworx and more than 5,000 business, public sector, and institutional deployments are serviced through our data centers in the U.S., Canada, Germany, Ireland, and the U.K.

For more information www.echoworx.com

✉ info@echoworx.com
North America 1 800.735.8916 | UK 44 808.134.9538