ECHOWORX

TECH BRIEF

Echoworx Security Cloud Services

Providing credential management and encryption integration for instant implementation across all platforms.

Echoworx Security Privacy Policy and Procedures

Echoworx is committed to providing the highest level of security, controls and integrity to support our cloud security services. To that end, we have subjected our business practises to the highest level of audit in the form of the AICPA/CICA WebTrust for Certification Authorities.

Certified Type II Service Organization Control – SOC2 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
- The SOC 2 report is available upon request to customers and prospects

Web Trust Audited by Richter

- Assured integrity of the Echoworx CA root
- Established key and certificate life cycle management controls
- Controls are maintained and monitored on an ongoing basis
- For more information: https://cert.webtrust.org/ViewSeal?id=2053
- A full copy of the Echoworx Root CA2 Certificate Policies and Practices Statement, used as part of the annual audit process can be found here: http://www.echoworx.com/ca/root2/cps.pdf

Microsoft Root CA Program

- Microsoft Root CA Program Member
- An elite group of less than 100 organizations
- Guarantees trust in certificates issued by Echoworx
- Subscribers can be confident that certificates issued are recognized and trusted

Apple Root Certificate Member

- Protects Apple customers from security issues related to the use of public key infrastructure (PKI) certificates
- Guarantees a seamless user experience for all users on Mac OS and iOS devices who are making secure web connections, generating secure emails and performing other PKI interactions

PCI Certified with AT&T

- Encrypted Mail, Secure Platform
- Enhances payment account data security
- Developed by PCI Security Standards Council
- For more information: https://www.pcisecuritystandards.org/index.php

Data Centers

- Echoworx has data centers in the US, UK, Mexico, 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 SSAE 16 SOC2 Type II, 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

North America 1 800.346.4193 | UK 44 800.368.5334 | Mexico 52 800.123.9553

Cryptography

Echoworx utilizes trusted cryptographic standards recognized by international bodies such as NIST and ANSI.

Those standards include:

- RSA 2048-bit asymmetric encryption
- RSA PKCS cryptographic protocols; PKCS#1, #7, #10, #12
- AES-256 symmetric encryption
- Triple DES 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. Accesses to services are permitted and controlled via reverse proxy servers ensuring there is no direct access to any secure service components.

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 principals of information security and ensures compliance to 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
- Business continuity and responsibility of management and staff
- Compliance enforcement and consequences of policy violations

Information security is constantly managing and updating polices by:

- Creating procedures to sustain physical security in the Echoworx facilities and systems keeping in mind access by third-parties
- Risk assessments to identify security implications and security control requirements
- Addressing security requirements and responsibilities with contracts and procedures between parties
- Delegating roles and responsibilities to the Echoworx team

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 conventional combination locks are also used.

All Echoworx security systems have industry standard 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 data center and additionally replicated real time to a disaster facility.

Echoworx maintains a recovery site apart from the primary site.

Effectiveness of business and disaster recovery plans are tested minimum once a year with 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 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)
- ISO27001:2005

North America 1 800.346.4193 | UK 44 800.368.5334 | Mexico 52 800.123.9553

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, including janitorial staff.

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.