CDX Information Security and Protection Overview

Compensation Data Exchange, LLC (CDX) was formed in 2003 to provide a common platform for insurance carriers and data collection organizations (DCOs) to exchange data that conforms to the industry approved WCIO format. CDX benefits its customers by providing a single location for SFTP configuration and their fully redundant file transmission architecture ensures secure delivery of data to the recipient. In addition to file transmissions, CDX offers its customers products to satisfy DCO policy and unit statistical data reporting requirements as well as products to distribute experience rating information. While many of the DCOs offer data reporting tools on their respective, secured websites, CDX is committed to providing additional options for customers to meet statutory reporting obligations for policy and unit statistical data.

The purpose of this document is to provide a general overview for all participants of how CDX protects the system and the data. The accessibility, security and integrity of member company data are of the utmost importance to CDX. All CDX systems that hold member data run on a proven infrastructure designed to provide maximum security, performance, and reliability.

The CDX system's security and infrastructure were designed to provide maximum performance and reliability with state-of-the-art physical and data security. Our security employs best practices using multiple layers of security, safeguards and redundancy to block internal and external security threats.

Physical Security

1. Cloud Hosted Data Center - Physical Security

The CDX environment is hosted by one of the top Cloud Hosting providers and the platform was created using some of the most rigorous security and compliance standards in the world. The Cloud Hosting provider adheres to security controls for ISO 27001, ISO27018, SOC 1, SOC 2, SOC 3, FedRAMP, HITRUST, MTCS, IRAP and ENS.

2. Hosted Data Center Provides Reliable Operating Environment

The Cloud Hosting provider's data center is designed to run 24x7x365 and employs various measures to help protect operations from power-outages, fire, and natural disasters. The data center infrastructure includes state-of-the-art fire suppression, multiple redundant power, a self-contained cooling system and automatically switched redundant connections to the Internet.

Network Access and System Integrity

3. Hosted Data Center Provides State-of-the-Art Network Security

The cloud hosting provider's data center employs state-of-the-art network access management and contains extensive multi-layered protections. The network perimeter is monitored on a 24x7x365 basis by experienced information security professionals. An alerting system is in place to ensure quick and active responses to any perceived threat to network security.

4. Cloud Hosting Provider Incident Response and Management

The Cloud Hosting provider has a global incident response service that works every day to mitigate the effects of attacks and malicious activity. The incident response team follows an established set of procedures for incident management, communication and recovery.

4. CDX Uses Managed Firewalls

The CDX system utilizes managed firewalls that continuously monitor and proactively block worms, hackers, and other threats.

5. CDX has active intrusion prevention systems (IPS) and Intrusion detection systems (IDS).

A CDX security team and escalation process are in place to handle any severe issues that may occur.

6. CDX Systems are Proactively Patched and Upgraded

CDX monitors, evaluates, tests and applies security patches, fixes, updates and upgrades to the CDX systems, shortly after release by the software vendor.

7. CDX Systems are Periodically Audited

CDX hires external security experts to conduct periodic security audits and penetration tests.

Backup and Recovery

8. CDX Data and Software is frequently Backed-Up

The CDX system follows industry standard best practices regarding data backup and data replication to assure system recovery in the event of a data loss.

9. CDX Maintains a Disaster Recovery Facility

CDX has implemented a comprehensive Disaster Recovery plan to protect data and to provide critical access and business continuity to our applications in the event of a disaster. The Disaster Recovery plan enables CDX to quickly reestablish operations at a secondary site if a disaster destroys or renders the primary site inoperable. CDX's secondary site resides in a different geographical region, the configuration provides for immediate connectivity and the architecture ensures CDX can meet Recovery Time Objectives and Recovery Point Objectives.

The CDX Disaster Recovery plan clearly describes roles of responsibility and chain of communication among all involved. The plan also incorporates guidelines and procedures to ensure timely action and quick response in the unlikely event of a disaster.

CDX conducts disaster recovery tests annually. Results are documented and the Disaster Recovery plan is updated to address any issues found.

Applications Security

10. CDX Users Can Only Access Associated Data

The CDX system requires that the Data Collection Organizations (DCOs) approve the carrier prior to carrier users obtaining accounts to access the system. Various access levels of User accounts exist within CDX, assuring that DCO and Carrier Users can only see data with which they are associated.

11. CDX Virus-scans All Transferred Data

All CDX servers operate with the latest versions of anti-malware software applications. This software is updated immediately when new threats are found.

12. CDX User Passwords Are Secure

CDX assigns privileges via passwords and adheres to the principle of least privileges. Strong passwords, failed attempts and expirations are enforced by system rules.

13. CDX Supports Secure Processes

The CDX application and file transfers only support secure communications. All transferred files are stored on encrypted drives, providing an Encryption at Rest layer of security.