# CDX Information Security and Protection Overview

The Compensation Data Exchange system (CDX) is a secure Internet facility for the electronic exchange of workers compensation insurance data between carriers and Data Collection Organizations (DCOs). Primarily, CDX is used to send, receive, and manage transactions. The transmitted data uses the WCIO format standards such as WCPOLS and WCSTAT. Additionally, CDX allows access to CDX's Web-based PEEP and BEEP systems for entering WCPOLS and WCSTAT data and can allow lookup of Rating Worksheets.

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. CDX's Top Tier Data Center Provides Rigorous Physical Security

CDX is hosted at a Top Tier data center that employs state-of-the-art physical access management. Physical access to the data center is continuously controlled and monitored by:

- Onsite 24/7 Uniformed Building Security Services
- Video Camera and Electronic Surveillance with Intrusion Detection
- Data centers comply with industry standards (such as ISO 27001) for physical security and availability.

The data center allows only extremely limited access to the physical site servers. Only authorized personnel are allowed to access the servers and they must be authorized by a two-factor authentication system utilizing both biometric and card readers to enter the data center. All access to the data center is recorded by time-stamped logs and maintained for historical retrieval.

All data center employees must pass criminal and historical background checks and sign confidentiality agreements in order to protect customer data. Access to data is kept to a strict need-to-know-basis.

### 2. CDX's Top Tier Data Center Provides Reliable Operating Environment

The data center 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. CDX's Tier-IV Host Provides State-of-the-Art Network Security

The data center employs state-of-the-art network access management. The network perimeter is monitored on a 7 x 24 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. 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 is in place to handle any severe issues that may occur.

### 6. CDX Systems are Proactively Patched and Upgraded

The CDX security network team 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

The CDX organization 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 site to protect data and to provide critical access and business continuity to our applications in the event of a disaster. The system ensures the ability to reestablish a working data center at a secondary Tier-IV site (ISO-22301 Certified) located in another state if a disaster destroys or renders inoperable the primary data center. 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. The CDX conducts disaster recovery tests annually.

## Applications Security

### 10. CDX Users Can Only Access Associated Data

The CDX system requires that Users have accounts with Data Collection Organizations (DCOs) 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.

August 14, 2019