CyberPay and CPO Phoenix Data Security

In the payroll business, data security is essential. Ensuring the safety of bureau and end-client information is a joint effort between CyberPay, Inc. and the bureau. CyberPay, Inc. does not host any payroll data onsite. The data is stored in two places: at the bureau (or your offsite hosting company, if you use one) and in the cloud (if you are using CPO Phoenix).

Bureau

The security of data stored on the bureau premises is the responsibility of the bureau. We encourage you to engage an IT professional to ensure that your CyberPay Data is protected according to industry best practices. Some things to consider: locked server room accessed only by cleared individuals, background checks of employees, regular password changes, offsite backups stored in a secure location, etc.

CyberPay, Inc. - online program

Although we do not host any of your data at our location, our Online Platform does transmit data and store it in the cloud (which syncs with your onsite data.) CPO Phoenix was designed for end-to-end security. We use highly secure data transmissions and have chosen an incredibly secure data center for hosting.

Details:

Transmission

All CPO Phoenix data transmissions are protected by 1024-bit SSL (TSL Encryption) and the user facing website is protected by 256 bit SSL (TLS Encryption).

Security standards

Cloud data is stored in Microsoft datacenters, which meet or exceed U.S. federal government and international security body standards. Microsoft online services and data centers adhere to stringent HIPAA, SOX, and FISMA requirements. The data centers are also Statement on Auditing Standards (SAS) 70/SSAE 16 and International Organization for Standardization (ISO) 27001 certified, and they are audited by independent, third-party security organizations.

Security measures

Security in datacenters employs outer and inner perimeters with increasing security at each level utilizing a combination of technology and traditional physical measures. Technical measures include two-factor access control, badge readers, extensive camera monitoring and integrated alarm systems. Traditional measures can include perimeter fencing, security officers, locked server racks. Hard drives with sensitive info are routinely destroyed when decommissioned.

Uptime

Microsoft guarantees 99.9 percent uptime at its data centers, which are outfitted to operate during power outages and after natural disasters. Microsoft replicates data from its primary data centers to secondary data centers for redundancy, without storing any data off-site.

Backups
Microsoft's network is one of the largest in the world. Large geographically distributed footprint of datacenters allow for geo-redundant backup and failover.

CyberPay, Inc. - internal security
Again, we do not host your data in our location. However for technical support or custom development, there are times when we may work with your data. We follow these internal security procedures:

- All data is filtered for viruses and malware at both a firewall/network level and at the host level
- Virus definition updates are performed daily
- All operating system updates are installed monthly within 72 hours of release
- All personal information transferred over public networks is encrypted with 128-bit SSL (TLS Encryption).
- In the event that a copy of our Client's data is temporarily stored on a company owned computer or on the internal company network, a data shredder application is used to destroy the copy of the Client data using a DoD 5220-22.M wipe algorithm, which is enforced by our internal security policy document.