Paycor

Can Your HCM Provider Protect Your Data?

Why Data Security Is Important

Your employees trust you to keep their information safe. But do you have the same level of faith in your HCM provider? HR databases are the ideal target for hackers. They contain the critical information hackers prey on including: Social Security numbers, bank account numbers, check stubs, and family information.

With hackers collecting more information by the day, does your HCM provider have the right defenses in place to protect your data?

Does Your Provider Utilize These Security Measures to Keep Your Data Safe?

Now's the time to ask tough questions about how they're keeping your employee's information secure.

Call toll free
1.800.501.9462

Visit us online
paycor.com

If your provider does not offer the following features, you could be at risk.

Multi Factor Authentication

This safeguard helps to eliminate employees from recycling the same password on multiple platforms. To access the database, users are required to enter their username and password and complete a variety of authentication requirements like email, text message, phone call, or biometric identification.

Google Authenticator

Google Authenticator provides users with a randomized six-digit code that must be retrieved and entered to access information. Increased authentication eliminates the risk of an email or phone number that has been compromised from phishing or hacking.

Data Encryption at Rest/In Transit

Transferring sensitive data across platforms can pose great risk. Most companies and HCM providers encrypt their data in transit to make it useless to hackers, but your sensitive data could still be compromised while idle. Ensure that your HCM provider has database level encryption to protect your information.

Dedicated Risk Assessment Team

Cybersecurity threats are constantly evolving and becoming more complex. It takes a dedicated team to implement and test new security protocols and prevent secure data from falling into the wrong hands.

Company Controlled Laptops

Do you know if your provider allows employees to use their own device or laptop to access your information? Requiring employees to use secure, encrypted, company controlled laptops ensures your data is protected from hackers.

Want to learn more?

For more information on how we make security a priority, visit **Paycor.com/security.**

Paycor Security: How We Protect Your Data

Paycor is serious when it comes to keeping client payroll and personal information confidential and secure.

Intrusion Detection and Intrusion Prevention System

Our servers and networks are stored in enterprise-class data centers that can detect patterns and signatures of malicious activity. Our infrastructure is fully redundant with continuous live backups ensuring data consistency and reliability.

Industry Leading Encryption

Paycor encrypts every endpoint where customer data is stored. This includes disk level encryption to prevent files from being transferred from a company laptop or server if the device is stolen. Paycor also encrypts data at the file level to prevent online database breaches.

Advanced Threat Detection

Our Advanced Threat Detection feature combats "zero day" viruses that are still unknown by the cyber security community. It uses behavioral analytics like file access patterns to proactively isolate the infected endpoints before data breach occurs.

Vulnerability Scanning

Paycor has its own dedicated security team that performs vulnerability scans and penetration tests across our entire network. We also rotate third party software companies to perform software scans on our network twice per year.