SECURITY STANDARDS

Paycom's single-database software employs comprehensive, in-depth and industry-proven standards and technologies to protect and defend customer data and its privacy in our environment. As one of the few payroll processors to be ISO 27001, ISO 27701, ISO 9001, ISO 22301, SOC 1 and SOC 2-certified, Paycom's information security and privacy management and quality management systems are formally audited and verified for compliance annually. Plus, Paycom is conformant with CIS Cyber 18 control framework with increased frequency of and enhanced internal security assessment to meet and exceed organization-wide IT security policies.

OUR COMMITMENT AND ENHANCEMENTS

- AES-256 encryption technology to protect all data at rest and TLS encryption method to protect data in transit
- Latest tech on endpoints, servers and perimeter for protection of software and employees
- Intrusion-detection system with enhanced tabletop and simulation exercises for team readiness in the event of a cybersecurity incident
- Least-privilege principles in provisioning access
- Use of Next-Gen firewalls to control access and block modern threats
- Redundant infrastructure for high performance and fail-over capabilities
- Diverse, load-balanced internet lines serviced by multiple network providers
- Augmented data loss prevention tools and traffic monitoring
- Multifactor authentication
- Weekly targeted website penetration testing for vulnerabilities with technology
- Annual third-party penetration testing and tabletop exercises
- Weekly, monthly and annual disaster-recovery testing
- Real-time backups to off-site locations
- Secured, monitored and redundant data centers with full battery and generator power
- Employee accountability for complying with our Information Security Policy and Procedures, including pre-hire background checks
- Formal risk management program, including vendor management and security awareness training and exercises
- 24/7/365 security command center
- Vulnerability and patch management program
- Enhanced security awareness program including simulations to train Paycom employees on: phishing (email), vishing (voice calls) and quishing (QR codes)

SECURITY FEATURES INCLUDED

IP Filtering for Time Clocks: This optional feature prevents employees from punching in/out via home PC, smartphone, or unauthorized location outside your company's network that has not been registered with Paycom. This feature allows a user to clock in to the system from a computer whose IP address has been registered with Paycom.

IP Filtering for Direct Deposit Changes: Direct deposit routing and account numbers can be changed only from a computer whose IP address has been registered with Paycom.

Security Questions: Security questions allow for an alternative way of identifying your employees/clients when they have forgotten their password, entered the wrong credentials too many times, or tried to log in from an unfamiliar device or location.

Customizable Access Profiles: Custom access profiles can be assigned to administrators or personnel who have the need to access sensitive fields, such as Social Security numbers and direct deposit account numbers. Paycom, by default, does not allow users to view sensitive fields, but any of our customers' User Administrators can enable it for any of their users.

Authorized Administrators: Users who can discuss sensitive information, including Social Security numbers, direct deposit numbers, pay rates, etc., must have three personal answers registered with Paycom.

YOUR EMPLOYEES' DATA AND OUR MOBILE APP

Paycom holds all confidential information in strict confidence. We take the same degree of care and caution to prevent its unauthorized disclosure as we do with our own, including measures required by applicable privacy law.

To ensure security of your employees' nonpublic personal information, data is encrypted while in transport over the internet and while in storage. Paycom employs enhanced third party privacy impact monitoring with more vigorous assessment and engagement with consultants and auditors to manage material risks from cybersecurity threats, based on international data privacy standards.

Changes to Direct Deposits: After a direct deposit routing number or account number is changed, the next payroll will include a screen detailing which direct deposit changes have been modified since the last payroll.

Payroll Confirmation Email: After a payroll has been run, an email is sent to all User Administrators, along with anyone else they designate, informing them that a payroll has processed.

2FA: When logging into Paycom, users are required to enter a passcode sent to an authorized phone number or email address, further protecting your sensitive HR and payroll information. This may only be bypassed when a device is authorized after 2FA is used to log in.

CAPTCHA: Paycom leverages CAPTCHA technology to ensure a human is attempting to log in to the application. Most users are presented with CAPTCHA once per year, while the security service continuously runs behind the scenes.

One-Time Passwords: When a user attempts to change high-value data, including banking information, a verification code is sent to the user's authorized contact information. The user is required to enter this code prior to completing the change.

CUSTOMER CONTRIBUTIONS

Paycom is committed to protecting the security and privacy of all customer information. Customers are responsible for adopting their own effective internal controls regarding access to Paycom's payroll system and their sensitive information. Paycom recommends the following to help you protect your information when accessing our services:

- protect your ID (username) and password, by keeping it unique and known only to you
- choose a password that is at least eight characters, alphanumeric and difficult to guess
- avoid using an easily guessed password, such as birthdates or a child's name
- change your password at least every 90 days
  avoid writing your password down and keeping it in places where others can find it
- always use the "LOGOUT" button to log out of Paycom's online system, and close the browser
- do not allow your browser to save usernames and/or passwords
- utilize all of Paycom's enhanced security features, including security questions and IP filtering
- install antivirus software and keep system security patches up to date

PAYCOM WILL NEVER

- ask you to submit or change your account information through email
- ask for your online password
- ask you to log on to our site through email
- email you about a digital certificate to access the system

Contact Paycom to learn more. | paycom.com | 800.580.4505

paycom®