Our Security Standards

Paycom employs industry-proven standards and technologies to protect customer data in our environment. As one of the few payroll processors ISO 27001- and ISO 9001-certified, Paycom's information security management and quality management systems are formally audited and certified that required standards are met.

Our Committment

Paycom is committed to an information security framework based upon well-recognized international standards:

- ISO 27001 certification,
- 256-bit encryption technology to protect all information transmitted over the Internet,
- intrusion-detection systems to monitor attempts of unauthorized access,
- firewalls to protect our systems and networks,
- redundant infrastructure for high performance and failover capabilities,
- diverse load-balanced Internet lines serviced by multiple network providers,
- activity log monitoring,
- monthly website-penetration audit testing for vulnerabilities,
- real-time backups to off-site locations,
- secured, monitored and redundant data centers with full battery and generator power, and
- employee accountability for complying with our Information Security Policy and Procedures.

Security Features Include

IP Filtering for Time Clocks: This optional feature only allows a user to clock in to the system from a computer whose IP address has been registered with Paycom. This prevents users from clocking in from home, smartphones or other unauthorized locations.

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.

Password Expiration: Set a password-expiration policy that fits your organization's compliance and security needs. Contact your Paycom dedicated specialist for more information.

Security Questions: When logging onto the system for the first time, a user must answer five security questions. Subsequently, if the user attempts to log on from another computer, the user must answer two of the five security questions.

View Sensitive Fields: Sensitive fields include 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.

Verification Questions: 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 payroll specialist will verify this information every time they receive a call or email from that user pertaining to sensitive information.

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.

Security Standards

Paycom Will *Never:*

- ask you to submit or change your account information through email,
- ask for your online password,
- ask you to log onto our site through email, or
- email you about a digital certificate to access the system. Any email addressing this should be considered suspicious and possibly to contain a virus.

If you ever receive an email from Paycom which appears to be suspect, please forward it to *itinfosec@paycomonline.com.*

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. These are keys to access your information on our system. Please protect them.
- Choose a password that is at least eight characters, alphanumeric, and difficult to guess. Avoid using an easily guessed password, such as birth dates 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 view it or would seek it out. Under the keyboard is a classic example of a bad hiding place for a password.
- Always use the "LOGOUT" button to log out of Paycom's online system, and *close the browser* when you are done.
- 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 and virus definitions up to date.
- Use adequate personal or corporate firewall software or hardware.

Paycom provides the workforce management tools you need in *one* cloud-based application.

paycom®

Paycom.com • 800.580.4505

5/17