Your data security is a priority.

Why is data security important?

Security has become increasingly important in recent years. With constant news of compromised customer information, knowing the risks common to today's security landscape is more critical than ever. **Paycor is serious when it comes to keeping client payroll and personal information confidential and secure.**

Security Management Program

Paycor is a firm believer that no security practices are safe without a robust security management program. Continuous improvement, ongoing associate education, and use of best-in-class industry security practices are hallmarks of Paycor's security program. Paycor's security management program includes:

- Reinforcing employee responsibility through security education, training, and awareness.
- Utilizing security analytics programs to continuously scan our internal network for vulnerabilities.
- Employing a staff of security professionals certified in industry-recognized certifications like CISSPs (Certified Information Systems Security Professionals) and ECSPs (EC-Council Certified Secure Programmers).
- Performing quarterly internal and semiannual external penetration tests of our software suite to proactively identify and remediate potential threats.
- Conducting internal and third party enterprise risk assessments on a regular basis.

A quality security program is comprised of two areas of focus: physical and financial security, and technical security.

Physical and Financial Security

Physical and financial security is defined as the protection of financial resources, personnel, hardware, programs, networks, and data from physical or financial events that could cause serious losses or damage to an organization, its clients, or any other stakeholder. Physical and financial security is the foundation of good data security. It means doing "the basics." Paycor covers the basics and much more, including:

- Requiring employees and guests to abide by badge access policy, and mandating visible identification for employees and visitors in offices and data centers.
- Utilizing security guards and camera systems to deter illegal activity and monitor vital areas where client information is stored.
- Engaging a national public accounting firm to perform an SSAE16, or SOC 1 Type 2, audit on Paycor's payroll services processes and controls on an annual basis. SOC 1 audits, and the reports that are issued upon completion of the audit, are designed to help service organizations like Paycor build trust and confidence in their service delivery processes and controls. The SOC 1 report is intended for clients and their financial statement auditors to evaluate the effect of the service organization's controls on the user entity's financial statements.

- Maintaining and regularly conducting exercises of our Business Continuity and Disaster Recovery Plans, along with other security procedures.

Technical Security

Technical Security is the protection of information achieved through the use of multi-layered information systems. Technical Security identifies gaps in security systems and implements plans to reduce the risk of hacking or technical failure in order to provide data confidentiality, integrity, and availability. Paycor follows a defense-in-depth strategy that employs multiple layers of security that work together to protect confidential data, such as:

- 256-bit TLS 1.2 data encryption for data transmission
- Anti-virus and endpoint protection for internal computing assets
- Multi-factor authentication (MFA)
- Automatic notifications for changes of critical account information
- Next-gen, high-availability firewall technology
- Automated fraud detection software
- IP Filtering for time clocks

Paycor is recognized by an “A” grade from Qualys SSL Labs on its SSL Server Test Overall Rating, a test that analyzes and rates the configuration of SSL web servers on the Internet based on Certificate, Protocol Support, Key Exchange, and Cipher Strength.

Your Security Responsibility

Paycor has adopted a best-practices security program that is proactive and dynamic. We strive to keep your data safe, but it is important to remember that all of us have a role to play in information security. We recommend that clients adopt the following security standards to further protect their information:

- Keep your username and password confidential
- Use a different password for each system
- Always confirm you have logged out after using a website
- Be mindful on shared computers
- Install anti-virus software and keep it updated

Summary

Paycor’s systems are developed internally making use of proven security controls to ensure the confidentiality, integrity, and availability of your data. Paycor has developed a robust security management program to protect your data. At Paycor, we pride ourselves on the security we provide to our clients and their employees.