# Information Security Controls

## How We Protect Client Data

This document serves as an overview of notable information security controls and practices that we have in place to foster a culture of security and protect data for our clients, partners, and employees.

**SOC Reports**
Paylocity engages reputable audit firms who perform annual independent audits and provide attestations including SOC 1 and SOC 2 Type II reports covering internal controls over financial reporting along with security controls spanning the confidentiality, integrity, and availability triad. Each control is tested to provide reasonable assurance that it is designed appropriately and operating effectively, and the results of testing are reported to clients on an annual basis.

**ISO 27001:2022**
Paylocity is certified against ISO 27001:2022, which is an internationally recognized framework for managing information security. This certification further demonstrates that Paylocity has established, implemented, maintains, and continuously improves its Information Security Management System. The annual audit for this certification is performed by an independent, reputable audit firm, and documentation of this certification is continuously available to clients.

## Data Privacy

We have invested in a global privacy program, with dedicated privacy compliance professionals, to ensure privacy is embedded in our activities. For additional information, please refer to our Privacy Center.

## Risk Management

Paylocity has a dedicated team of information security risk management personnel along with multiple established information security risk committees, comprised of key organizational stakeholders and senior executives. Formal risk assessments are performed no less than annually, with continuous risk management and monitoring performed in the interim period. Risk management personnel are responsible for framing, assessing, responding to, and monitoring information security risks for the organization. These risks are tracked in a documented risk register and reported to the company's various information security, technology, and enterprise risk management committees.

In addition to these organizational risk management practices, Paylocity also has dedicated personnel, processes, and tools for assessing and managing the risk of third party relationships. This includes reviewing and assessing documentation of information security controls and reviewing the information security language contained within agreements for relevant third party relationships.

Our risk management stakeholder practices and groups include subject matter experts across information security, product and technology, privacy, business resilience, and enterprise risk management disciplines.

## Information Security Policies

Paylocity maintains formal and documented information security policies and standards. This governance documentation is based on industry standard frameworks from organizations such as the National Institute of Standards and Technology (NIST), the Committee of Sponsoring Organizations (COSO), and the International Organization for Standardization (ISO) to establish structured governance, policies, standards, and control requirements where applicable. Information security policies and standards, including updates and revisions, are formally reviewed and approved by management on an annual basis.

 Copyright © 2025 Paylocity. All Rights Reserved.

## Security-Focused Roles

The Paylocity technology risk management organization is comprised of multiple specialized teams, each led by subject matter experts in their respective domains. This intentional team structure ensures that we have dedicated professionals, managed by a CISO, focusing on key areas such as application security; vulnerability management; cloud and architecture security; identity and access management; security operations; threat intelligence; incident detection and response; governance, risk and compliance; and business resilience. Paylocity invests in our information security professionals with continued training and certifications from reputable organizations and memberships with security interest groups.

Maintaining a dedicated subject matter disciplinary approach allows us to provide deep expertise and tailored solutions to meet evolving security challenges, rather than relying on a single team to manage all aspects of information security.

## Security Awareness & Training

Our people are at the heart of a healthy security culture. We perform background checks on every prospective Paylocity candidate before confirming their employment. Required security and privacy training is assigned to Paylocity employees during the onboarding process and annually thereafter. These mandatory trainings include the safe handling of sensitive information, appropriate responses to a suspected data security breach, and awareness of employee security responsibilities as front-line workers.

Our Information Security Awareness Program advances and promotes a healthy security awareness culture throughout the organization through supplemental education, training courses, informational videos, internal and external publications, regular phishing tests, and supporting activities.

## Business Resilience

Paylocity applies controls from best practices such as, but not limited to, The Business Continuity Institute (BCI), Disaster Recovery Institute International (DRII), and International Organization for Standardization (ISO) for developing and maintaining threat-agnostic plans with strategies to continue client services and critical business operations in the event of a disruption to critical dependencies. As part of program governance, the Business Resilience (BR) team reviews updates from these and other industry standards, such as those regarding information security and data privacy, to assess the need to adjust our program. The business resilience planning process includes business impact analysis, risk assessments, and continuity strategies for the most critical Paylocity processes.

The BR team conducts regular exercises to validate and continuously improve the plans and strategies. Paylocity has multiple call centers distributed among different U.S. geographic regions, and each site can operate independently in the event of a disruption.

Backup procedures include daily snapshots of all critical client data to local storage media, as well as tiering backups to alternate locations. The snapshots are stored on redundant storage arrays and are retained for long-term data retention compliance. Client data is also replicated between the primary and secondary data centers for business continuity. These data centers are geographically separated. Backups are tested regularly to ensure recovery reliability. Backups are encrypted using AES-256 and are retained for long-term data retention compliance. Additionally, Paylocity team members annually test restore capabilities. Automated software is set to alert in the event any backup process fails, and these alerts are ticketed and investigated through resolution. The automated data backup software has a data retention field that is utilized to determine when storage media should be processed for destruction.

Paylocity's data centers are connected to multiple independent Internet Service Providers (ISPs). Redundant hardware is in place throughout the network infrastructure to support resilient network traffic delivery. The environment is protected from hardware failure by utilizing load balancing and clustering technologies.

 Copyright © 2025 Paylocity. All Rights Reserved.

## Data Security Safeguards & Encryption

We protect our client data with commercially-reasonable tools and practices in our private SaaS cloud, including:

- Deployment of Intrusion Prevention Systems (IPS) to detect and block malicious traffic
- Web Application Firewalls (WAF) that protect our application from attacks
- Network Firewalls
- Security Information and Event Management (SIEM)
- User and Entity Behavior Analytics (UEBA)
- Endpoint Detection and Response (EDR) to protect our workstation and server population
- Data Loss Prevention (DLP) at multiple layers of our dataflow stack
- Regular Penetration Testing from both our internal teams and external providers
- Multi-layered vulnerability management program to identify, assess, and remediate vulnerabilities within our product and infrastructure

Additionally, our product suite provides configurable application security features and logical access control mechanisms based on the client's business processes and needs. We encrypt sensitive client information both during transmission and at rest using industry standard protocols.

## Web Application Security

Paylocity has built a mature Application Security Program that aligns with standard frameworks, such as the Building Security In Maturity Model (BSIMM) and Open Software Assurance Maturity Model (OpenSAMM), and promotes security champions within the developer community to instill strong, secure coding practices for reducing vulnerabilities and delivering a secure web application.

Core areas within the program include:

- Specific developer-focused security training
- Secure coding practices
- Static and dynamic scans
- Continuous monitoring of vulnerable third party libraries
- API security scans
- Internal and external penetration testing

Furthermore, critical security web application vulnerabilities are responded to immediately in compliance with our information security policies.

 Copyright © 2025 Paylocity. All Rights Reserved.