Information Security Controls

paylocity
Forward Together.

How We Protect Client Data

This document serves as an overview of some of the notable information security controls and practices we have in place to foster a culture of security to protect clients' and our own data.

SSAE 18 Audit
Paylocity uses a reputable independent accounting firm to perform an assessment of our procedures and controls as part of our annual SSAE 18 audit for SOC 1 and SOC 2. Each control is tested for operating effectiveness and the results reviewed by senior management.

ISO 27001:2013 Certified
Paylocity maintains certification for compliance with ISO 27001:2013 and is assessed by an independent third-party auditor. Our compliance with this internationally recognized information security standard is evidence of our commitment to information security at every level of our organization, and that Paylocity's security program is in accordance with industry-leading best practices.

GDPR
Paylocity has aligned with GDPR compliance obligations and monitors the compliance landscape abroad as well as at the national and state level.

Risk Management

Paylocity has an established Information Security Steering Committee (ISSC) comprised of key executive and operating personnel to oversee the ongoing management of the organization's risks to information systems. To track risks and security initiatives, Paylocity maintains an Information Security Risk Register of threats and vulnerabilities that have a likelihood of occurring and/or would have a significant impact to business objectives. Management performs an annual risk assessment to identify internal and external threats, analyzes the significance of these threats, and develops a mitigation strategy to address these risks. The risk assessment includes the analysis of potential threats and vulnerabilities arising from vendors providing goods and services. The ISSC also maintains a risk matrix and heat map which identifies the significant risks that threaten the achievement of security commitments and identifies controls that mitigate these risks.

Information Security Policies

Paylocity maintains formal and documented information security policies. These policies map to standard industry frameworks such as the National Institute of Standards and Technology (NIST), Committee of Sponsoring Organizations (COSO), and International Organization for Standardization (ISO) 27001 to establish structured governance, policies, standards, and controls. Policy deliverables are formally reviewed and approved by senior management on a periodic basis, as are policy updates and revisions.

Security Focused Roles

Paylocity's deep commitment to safeguard and protect client data from internal and external attacks is reflected in the security-focused roles within the Technology and Information Security departments. Paylocity invests in our Information Security professionals with continued training and certifications from reputable organizations such as Information System Security Certification Consortium, Inc. (ISC2), the Information Systems Audit and Control Association (ISACA), ECCouncil, and others. Members of the Information Security department and select IT management are accredited as Certified Information Systems Security Professionals (CISSPs) and Global Information Assurance Certification (GIAC). Paylocity personnel also maintain relationships with security interest groups, such as the Open Web Application Security Project (OWASP), the Information Systems Security Association (ISSA), and InfraGard.

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. Every Paylocity employee takes security training right from the start, and we require 100% participation that is closely monitored by our Compliance team. From day one, our onboarding process raises awareness that securing your data is critical to everything we do.

Paylocity employees retake annual security and privacy training to maintain our focus on protecting your interests. This mandatory training educates our employees on safe handling of sensitive information, appropriate responses to a suspected data security breach, and awareness of security responsibilities. Our robust Information Security Awareness Program advances and promotes a healthy security awareness culture throughout the organization through supplemental education, training courses, videos, internal and external publications, 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) 22301 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. The business resilience planning process includes business impact analysis, risk assessments, and continuity strategies. Paylocity's Business Resilience (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.

Paylocity relies on a multi-tiered, redundant backup strategy to help ensure recovery of data, reliant on both on-premise data centers as well as cloud services. 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. Paylocity team members annually test restore capabilities. Automated software is set to alert in the event any backup process fails. 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.

We host our solution using enterprise-class data centers to ensure both the physical security of your data and consistent product suite uptime. These data centers undergo a rigorous independent audit in accordance with the AICPA's SSAE 18 standard to ensure compliance and safeguarding of client data. Colocation services consist of 24 hours a day, 7 days a week, 365 days a year physical and environmental protection services. Paylocity's data centers are connected to multiple independent Internet service providers. 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.

Data Security Safeguards & Encryption

We protect our client data with industry-accepted solutions and practices, 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 technical bugs within our product and infrastructure
- Clients access our private-cloud SaaS environment via encrypted TLS sessions using unique user IDs. Our product suite provides configurable application security features and logical access 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 the BSIMM framework 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:

- Specific developer-focused security training
- Secure coding practices
- Static and dynamic scans
- Internal and external penetration testing

Critical and high security web application vulnerabilities are remediated immediately, which complies with our information security policies. We are committed to maintain a 100% closure rate for known vulnerabilities. Our program exercises a force multiplication strategy to ensure security satellites are embedded within our product development.