information security

Controls Overview

paylocity

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 client's and our own data.

ISO 27001:2013 Certified
Paylocity has certification for compliance with ISO 27001:2013. This certification is performed by an independent third-party auditor. Our compliance with this internationally-recognized 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.

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 and the results reviewed by senior management.

HIPAA
Paylocity has completed all necessary requirements and activities for compliance with HIPAA as it relates to safeguarding the privacy of personal health information as shown by our independent third-party audit.

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 established an 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 Risk Register of threats and vulnerabilities that have a high likelihood of occurring and/or would cause a major impact to business objectives. Management performs an annual risk assessment to identify internal and external threats, analyze the significance of these threats, and develops a mitigation strategy to lower these risks. 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. The risk assessment includes the analysis of potential threats and vulnerabilities arising from vendors providing goods and services.

Information Security Policies

Paylocity maintains formal and documented information security policies. Our 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 IT and Information Security departments. Paylocity invests in their 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

Paylocity provides annual training for employees on data security and privacy. This mandatory training course is designed to educate our employees on safe handling of sensitive information, appropriate response to a suspected data security breach and awareness around responsibilities for security. Our robust Security Awareness Program advances and promotes a healthy culture of security awareness throughout the organization with supplemental education and training courses and videos, internal and external publications, and supporting activities.

High Availability & Disaster Recovery

Paylocity applies best practices from The Business Continuity Institute (BCI), Disaster Recovery Institute International (DRII), and International Organization for Standardization (ISO) 22301 for developing plans that are resilient, effective, and considerate of multiple scenarios that may affect the availability of critical resources. Our infrastructure is hosted at enterprise-class data centers to ensure both the physical security of client data and a consistent uptime for our product suite. 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 relies on a multi-tiered, redundant backup strategy to help ensure recovery of archived data. Backup procedures include daily snapshots of all critical client data to multiple catalog stores, review of daily backup logs, full monthly backups and daily differential backups. Backups are tested regularly to ensure recovery reliability. Offsite data backups are encrypted and securely transported to our secondary data center location.

Data Security Safeguards & Encryption

We protect our client data with industry-accepted solutions and practices, including:

- Intrusion Prevention System (IPS)/Intrusion Detection System (IDS)
- Web Application Firewalls (WAF)
- Network firewalls
- Security Information and Event Management (SIEM)
- Virus /Malware detection
- Data Loss Prevention (DLP)
- Penetration Testing
- Vulnerability Scanning

Clients access our private-cloud SaaS environment via encrypted TLS sessions using unique user IDs. Our product suite provides the client with configurable application security features and logical access based on the client's business processes including multi-factor authentication. Sensitive client information is encrypted 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.

paylocity
Forward Together.

About Paylocity

Paylocity (NASDAQ: PCTY) is a leading provider of cloud-based HR and payroll software solutions headquartered in Schaumburg, IL. Founded in 1997 and publicly traded since 2014, Paylocity offers an intuitive, easy-to-use product suite that helps businesses tackle today's challenges while moving them toward the promise of tomorrow. Known for its unique culture and consistently recognized as one of the best places to work, Paylocity accompanies its clients on the journey to create great workplaces and help people achieve their best through automation, data-driven insights, and engagement.

For more information, visit paylocity.com.

160301B