# Paychex Security

## Security Program Overview

PAYCHEX®

HR | Payroll | Benefits | Insurance

# Contents



# Introduction

Paychex takes security seriously. We are committed to protecting the confidentiality, integrity, and availability of client data and we continue to invest in our award-winning security capabilities, including personnel security and physical security; system security, access control, and monitoring; data backup and business continuity management; and vulnerability and intrusion detection. This paper describes the *Paychex Enterprise Security Program and its posture.*

The Paychex Enterprise Security Program is aligned with the National Institute of Standards and Technology (NIST) Version 1.1 Cybersecurity Framework. The NIST Cybersecurity Framework leverages NIST 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations.

Our security policy and standards, which have been ratified and are enforced by executive management, are built upon the five NIST Framework Functions.

# Control Environment

The control environment at Paychex includes a set of standards, processes, and structures that provide the basis for integrating risk awareness and control activities into the daily work routines of employees. Relevant constructs of the control environment are emphasized during the hiring process and employee onboarding and as part of ongoing training and awareness campaigns.

## Code of Business Ethics and Conduct

Paychex publishes a set of standards for acceptable business conduct so that employees, clients, and suppliers can understand the way Paychex conducts business. Paychex has been included on the World's Most Ethical Companies® list by the Ethisphere Institute®, which is dedicated to the research and promotion of profitable best practices in global governance, business ethics, compliance, and corporate responsibility.

Review the Code of Business Ethics and Conduct

## Privacy Statement

Data privacy, and the privacy of the information provided, is important to us. We use reasonable care to protect data provided to us by or on behalf of our clients or prospective clients and their workers or from visitors of our Site from loss, misuse, unauthorized access, disclosure, alteration, and untimely destruction.

Review our full Privacy Statement

## Security Statement

Paychex is committed to protecting the security and integrity of client information through procedures and technologies designed for this purpose. Specifically, we:

- Maintain policies and procedures covering physical and logical access to our workplaces, systems, and records
- Apply physical, electronic, and procedural safeguards aligned with industry-recognized best practices
- Use technology such as backups, virus detection and prevention, firewalls, and other computer hardware and software to protect against unauthorized access to or alteration of customer data
- Encrypt sensitive information transmitted over the internet
- Through formal approval processes, access controls, and internal auditing, limit employee access to customer information to those who have a business reason to know
- Require employees to take information security awareness training upon hire and annually thereafter and apply this training to their jobs every day
- Provide ongoing training and awareness to employees about security best practices, including internal phishing simulations to educate and test employees
- Use advanced technologies for the backup and recovery of customer information
- Monitor compliance with established policies through ongoing security risk assessments and internal audits

## Auditing and Compliance of Control Practices

Periodically, Paychex internal auditors and external accounting and auditing firms review our operations and business practices for compliance with corporate policies and procedures that specify the controls required to safeguard the confidentiality of information.

The Internal Audit department acts as an independent appraiser of the Paychex internal control system, assessing internal control design and operating effectiveness and recommending enhancements. Reporting directly to the Paychex Audit Committee, which oversees the company's internal control structure, the Internal Audit department has the authority to examine Paychex records, reports, and documentation and to use whatever audit procedures are deemed necessary to accomplish its objectives. The department has unrestricted access to the Audit Committee of the Board of Directors and to senior management.

## Vendor Risk Management

Paychex maintains a program designed to assess and manage the risk associated with its third-party relationships (in other words, business partners, contractors, consultants, suppliers, and other business associates). This program includes a signed nondisclosure agreement before any information is shared, an evaluation of the vendor's information security program, and a written contract that stipulates how information must be protected while providing the services.

## Insurance Coverage

Paychex maintains an insurance policy that includes cyber liability coverage for technology products, information security and privacy, regulatory defense and penalties, and payment card industry (PCI) compliance fines and costs.

## Breach Notification

Paychex has established policies and procedures to comply in a timely fashion with applicable federal and state legal requirements related to privacy, data security, and incident notification. Paychex will provide notification to clients with no undue delay and in compliance with individual state and federal regulations surrounding the exposure of personally identifiable information (PII) and/or individual or protected health information (IHI/PHI).

## Regulatory Compliance

Paychex has processes in place to comply with local, state, and federal requirements regarding the security of client data. These processes include comprehensive security procedures that are regularly reviewed and revised as appropriate to reflect regulatory changes.

# Our Dedicated Security Team

The Paychex Enterprise Security organization includes several groups. Each is focused on information protection and uniquely assigned an aspect of the Enterprise Security Program:

## Security Risk Management

- Assesses the risks associated with significant infrastructure and operational changes and the introduction of new technologies
- Administers the vendor risk management program
- Compiles scorecards to assess and improve our subsidiaries' security posture

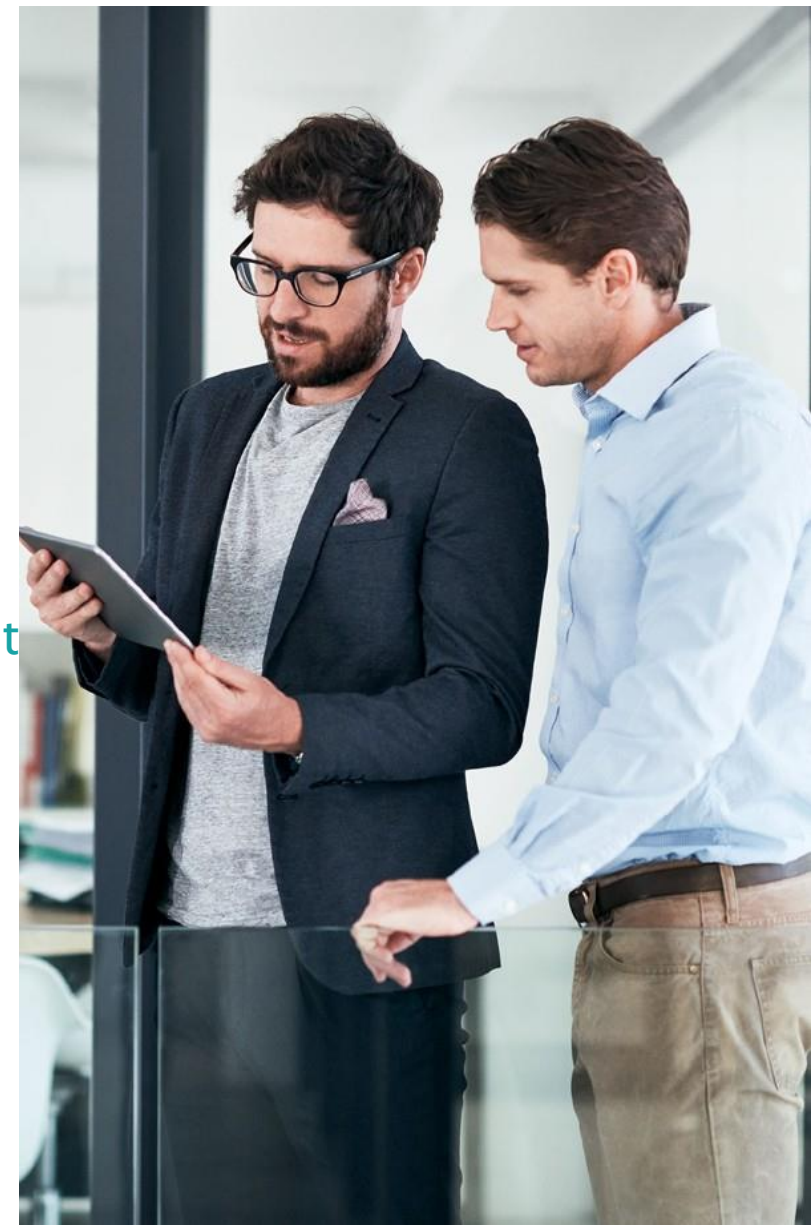
## Security Governance and Compliance Management

- Conducts regulatory compliance reviews
- Assists with external audit testing and evidence collection
- Manages, maintains and enforces security policies and standards

## Security Identity Management

Manages the governance and administration of identity functions, including:

- Privileged access management
- Access auditing and certification
- Provisioning and de-provisioning of user access



## Attack Surface Management

- Identifies security vulnerabilities through automated scanning technologies and tracks remediation commitments against established service-level agreements (SLAs)
- Performs penetration testing and due diligence assessments using security resources and multiple third-party vendors
- Reviews initiatives to provide security requirements and validates that security controls are properly accommodated within software and architecture designs

## Enterprise Managed File Transfer Services

- Ensures the confidentiality, integrity, and availability of Paychex data in transit
- Provides the secure automation, management, and centralization of electronic file transfers in an efficient and reliable manner

## Security Engineering

- Ensures robust technical controls are in place to prevent threats against Paychex systems
- Maintains secure web gateway and next-generation firewall platforms
- Collaborates closely with internal and external partners to prepare for and mitigate network security threats such as denial of service attacks
- Provides around-the-clock operational support for network security infrastructure

## Security Fusion Center

- 24/7/365 Security Incident Response function to collect and analyze information about potential system security violations and anomalous activity; works closely with human resources, corporate counsel, internal audit, risk management, external authorities, and other groups to record, report, and mitigate computer-related incidents
- Cyber Detection capabilities to manage and review security, operations, and application logs to detect malicious behavior
- Cyber Intelligence analysts responsible for gathering intelligence from trusted partners to identify relevant information to provide to other teams for analysis and action
- Cyber Threat Hunt function to actively search applications and infrastructure for indicators of compromise using known adversary tactics and techniques
- Insider Threat & Data Loss Prevention (DLP) function that creates, manages, and monitors all mechanisms designed to reduce risk related to intentional employee abuse or accidental misuse of valuable data

Enterprise Security embraces partnership and collaboration with resources across the company to ensure a consistent, resilient, and secure infrastructure. The department coordinates company-wide governance through consistent and repeatable processes, communicates security requirements for implementing new technologies, and provides visibility of security risk to executive and senior management.

# Personnel Security

## Employee Background, Reference, and Drug Screening

All candidates who are offered a position with Paychex are subject to pre-employment reference checks, drug testing, and background checks.

## Employee Training

Paychex is committed to training as an essential component of employee success. Every year the company's in-house Training and Development Center provides more than one million hours of instruction to employees across the country. Employees are required to complete training to gain the product knowledge and professional skills necessary to maintain the Paychex standard for service excellence. Employees are trained to help protect client confidential information in their possession, be aware of and identify phishing and other social engineering attempts and follow the proper procedures for handling confidential information and reporting suspicious activity.

Paychex is ranked on Training magazine's Training Top 125 list of outstanding international training organizations for continuous dedication to, and investment in, employee development.

## Employee Non-Disclosure and Confidentiality Policies

Employees are required to abide by confidentiality and nondisclosure policies.

## Employee Communication Regarding Changes to the Paychex Security Policy

All relevant changes to the security policy are communicated internally to key stakeholders once they have been approved by Paychex senior management.

## Reporting Perceived Misconduct

Employees are encouraged to contact a direct-access hotline to report financial, accounting, fraud, misconduct, or other concerns. Anonymous reporting is established and coordinated by a confidential and independent third-party service.

# Client Data Protection

## Client Services Security

Security policies and procedures for Paychex client-facing services and applications are specifically designed to ensure the confidentiality of sensitive information in clients' electronic communications and transactions. Paychex stands behind its commitment to protect client data through the following best practices and technologies:

- Paychex uses a modern, innovative, and proven hybrid cloud infrastructure that delivers reliable, highly available software as a service (SaaS) technology to more than 730,000 businesses
- Our all-in-one HR technology and service platform, Paychex Flex®, is available online, on any device, and at any time
- Our technology and U.S.-based service team are accessible 24x7x365. The Paychex Flex® platform has had a consistent availability of better than 99.9% – well above industry standards
- Using market-leading technologies and methodologies, our IT Operations Center tests and monitors Paychex Flex around the clock to proactively identify and respond to any issues before they impact our clients
- Paychex maintains a cyber fusion center that proactively identifies cyber security threats. Our security operations center team also monitors and responds to cyber security threats 24x7x365

## Secure Email Communications

An important component of safeguarding the privacy and security of client, company, and employee information is the Paychex Secure Email Message Center. The Secure Email Message Center provides a vehicle for Paychex to send notifications to regular email accounts containing links to our secure email server, where recipients can register and access confidential emails safely.

## Retention and Destruction of Hard Copy and Electronic Information

The Paychex Records Management Program (RMP) is an organized program to provide effective management of the company's business records. The RMP provides effective life-cycle management of all Paychex records from their generation or receipt to their final disposition. Adherence to the policies of the RMP ensures that Paychex (i) complies with government regulations and legal requirements, (ii) protects the records necessary to Paychex operations, (iii) reduces the cost of maintaining and storing records, and (iv) supports good business practices. All third-party disposition and destruction services are National Association for Information Destruction (NAID) certified and under contract to protect company business records prior to destruction.

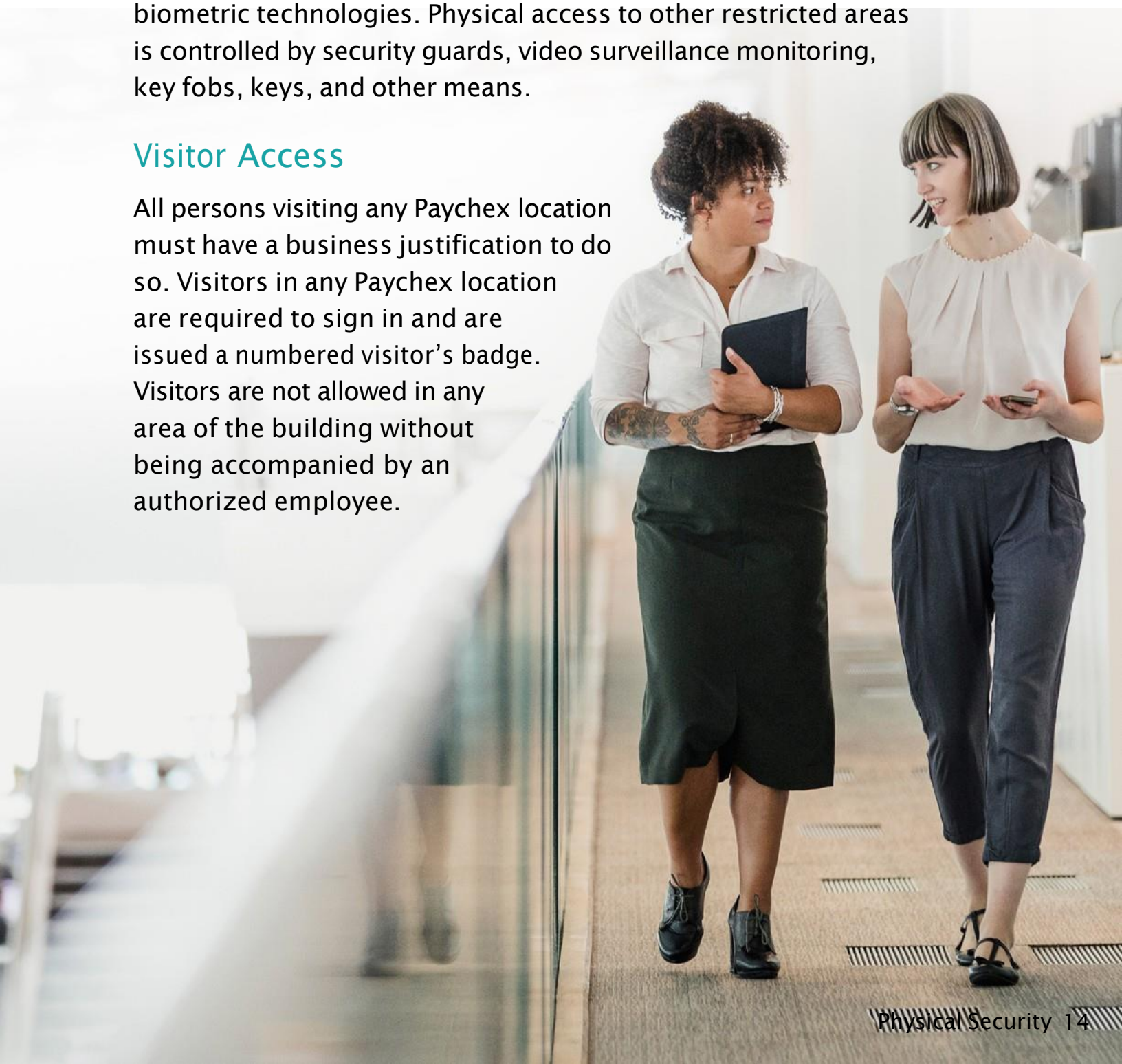
# Physical Security

## General Site/Building Information

Physical access to the corporate data processing centers is limited to employees with a business need to access the centers and is controlled by an electronic key, a personal identification number (PIN), and biometric technologies. Physical access to other restricted areas is controlled by security guards, video surveillance monitoring, key fobs, keys, and other means.

## Visitor Access

All persons visiting any Paychex location must have a business justification to do so. Visitors in any Paychex location are required to sign in and are issued a numbered visitor's badge. Visitors are not allowed in any area of the building without being accompanied by an authorized employee.



# System Security, Access Control, and Monitoring

## Formal Approval Process

To gain access to systems, a Paychex employee must pass a formal approval process. Employees are granted access only to information required to perform their work.

## Unique Access

Each employee is given a unique username and password to gain access to Paychex systems. All transactions are logged, and activity is monitored regularly.

## Separation of Duties

Paychex internal controls include policies and procedures to promote strong business practices and establish clear roles and responsibilities, including the segregation of duties. Segregating duties helps ensure that transactions are valid and properly recorded and controls can only be subverted through collusion.

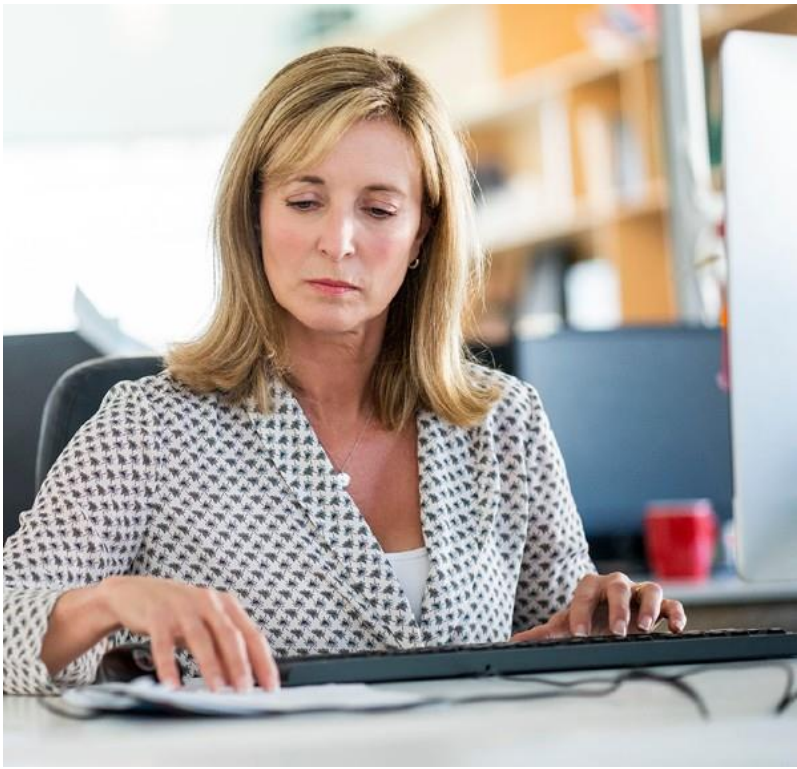
## Logical Access Controls

Logical access controls are designed so that only authorized users are permitted access to systems and applications. Formal processes and procedures guide system access requests for additions, changes, and removals.

## Audit and Monitoring

Proactive and detective monitoring of system audit logs and alerts is performed to ensure the use of Paychex systems is in accordance with published policies.

System audit logs are collected and monitored to help detect unauthorized activity and invalid changes to key data elements. Security activity is monitored, and security violations are reported to management.



## Employee System Termination Procedures

Paychex uses formal procedures to revoke physical, computer, network, and data access privileges upon termination of employment.

# System Development and Maintenance

## Change and Release Management

A formal change management process governs all changes to the production application infrastructure. This process covers the review and approval of project-size initiatives as well as minor changes such as enhancements, infrastructure changes, bug fixes, and regulatory changes. All significant modifications to the application infrastructure are managed within a project using a defined project life cycle.

All releases to the production environment are tested, approved, and promoted only by authorized individuals with the required rights.

## Enterprise Business Solutions

Enterprise Development designs, develops, and tests software applications that support Paychex business units. A defined software development process (SDP), based upon industry best practices for a systems development life cycle (SDLC), is used. The SDP includes guidelines for creating and testing program changes and allows for customization based on project requirements. Quality is ensured throughout the Paychex software development life cycle. The code is thoroughly tested. It is also scanned for vulnerabilities and appropriate actions performed prior to deployment into production.

## Quality Assurance (QA)

The purpose of quality assurance is to verify that all new functionality is working as documented and that design defects are identified and addressed.

# Data Backup/Business Continuity/ Disaster Recovery

## Business Continuity Management (BCM)

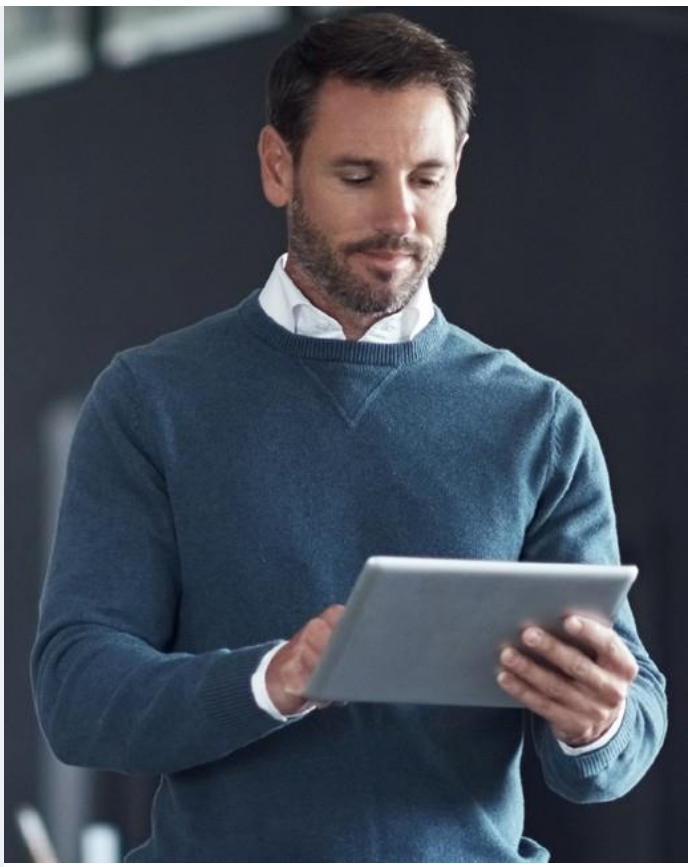
Paychex has adopted a business continuity strategy designed to ensure the continuation of business-critical functions in the event of a significant business disruption at any of our branches or corporate offices, including technical failures affecting our applications, data centers, networks, and the buildings we occupy. Paychex business continuity plan also includes measures designed to deal with severe weather, localized and regional disasters, and workforce-impacting events such as pandemics. The documented and tested recovery strategies are designed to mitigate the impact of events to our clients from any business disruption.

Our process for developing business resumption strategies and plans involves analysis, planning, implementation, maintenance, testing, and awareness. The program is initiated by conducting a Business Impact Analysis (BIA) with each business unit. The BIA identifies requirements for essential personnel, applications, and services necessary to support critical business functions during a disruptive event.

Business recovery strategies vary to make appropriate use of both internal and external capabilities and resources. They include external recovery vendor solutions, office relocation, branch workload redirection, and remote access to critical systems.

Through extensive testing, we verify the resources and requirements identified during the BIA process that are necessary for the recovery of all critical business functions operate in accordance with recovery specifications. The company continually updates the IT Disaster Recovery (IT DR) plans to minimize the time required to recover from a disruption.

Paychex has developed and maintains BIAs and IT DR plans on a secure site available to key personnel from any location and on many different types of mobile devices. These plans include relocation procedures, an emergency notification system initiation procedure, call trees, and other pertinent information for business resumption as well as plans for crisis management and executive management personnel to ensure proper coordination of command-and-control activities in the event of an emergency.



## Business Continuity

Our business resilience strategy is a component of our business continuity program, where the focus is on Paychex people, processes, and facilities. Our workforce, facilities, vendors, and business continuity plans, including defined Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs), are outlined in the business impact analysis.

The Paychex Business Continuity Plan (BCP) includes corporate- and business unit-specific components. Reviewed, updated, and tested annually, at a minimum, the BCP includes, but is not limited to:

- Automated notification/communication pathways and call lists
- Alternate worksite planning
- Critical vendor/third-party information
- Recovery activation procedures
- Workforce recovery plan
- Pandemic planning
- Crisis communications
- Infrastructure readiness checklist
- Recovery command team

Changes to the Paychex BCP impacting clients, vendors, and/or partners are communicated through normal business unit/vendor communication channels. Essential personnel are identified, documented, and trained on the BCP plan. These personnel are also included in the Paychex testing strategy. In addition, Paychex has implemented a regional workforce recovery strategy that is tested periodically.

## Disaster Recovery

This aspect of our business continuity management strategy focuses on data centers, servers, technology, application recovery strategies, data replication, data synchronization, and incorporation of other leading technologies. These technologies and entities are tested and audited using the latest tools. They are aligned with industry best practices and through our rigorous architecture validation testing. Furthermore, Paychex employs the latest configuration management and DR assurance tools available to ensure our RTOs, RPOs, and SLAs are met.

The corporate data centers have appropriate geographic separation for local and regional disasters. They are equipped with heat and smoke detection, fire suppression systems, redundant uninterruptible power supplies (UPS), redundant generator-provided power, and monitoring by a 24/7/365-staffed IT operations center. In addition, branch offices are equipped with heat, smoke, and fire detection systems. Certain branch offices have a UPS and a generator to protect computers, phones, and alarm systems from power surges and failures. Each year, Paychex performs power failure exercises in each corporate data center and branch office. Paychex maintains documented recovery strategies for all critical resources, including services, systems, buildings, and its workforce.

## Business Impact Analysis (BIA)

The purpose of the business impact analysis (BIA) is to identify which business units/departments and processes are essential to the survival of the business. The BIA will identify how quickly essential business units and/or processes must return to full operation following a disaster situation. The BIA will also identify the resources required to resume business operations.

**The outcomes of the BIA include the following:**

- Endorsement or modification of the organization's BCM scope
- Identification of legal, regulatory, and contractual requirements (obligations) and their effect on business continuity requirements
- Evaluation of impacts on the organization over time, which serves as the justification for business continuity requirements (time and capability)
- Identification of legal confirmation of product/service delivery requirements following a disruptive incident, which then sets the prioritized timeframes for activities and resources
- Identification and establishment of the relationships between products/services, processes, activities, and resources
- Determination of the resources needed to perform prioritized activities (e.g., facilities, people, equipment, information, communication and technology assets, supplies, and financing)
- Understanding of the dependencies on other activities, supply chains, partners, and other interested parties
- Determination of how up-to-date the information needs to be

[Source: ISO/TS 22317:2015(E)]

## Data Backups

Paychex has developed a combination of technological solutions and comprehensive, industry-leading recovery planning strategies for a rapid response to events. These include:

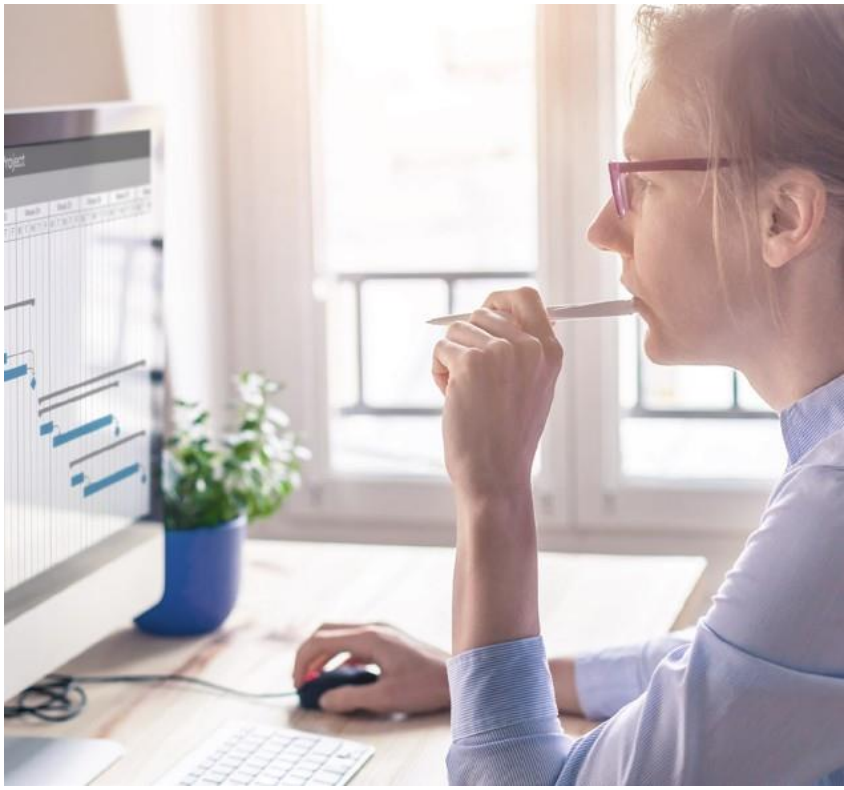
- Redundant backups of client and client employee information at multiple regional data centers
- Ongoing backups of payroll transactions daily
- Electronic transmission of business-centric application transactions throughout each processing day

### Proper destruction of disposed media

Backups are protected from unauthorized access and tampering. Controls have been created to keep customer data highly secure from outside tampering and to guide the proper and secure disposal of media at the end of its required life.

### Testing of archived data

Paychex infrastructure support personnel practice recovery techniques every month within a test environment. The test measures the thoroughness of Paychex strategies and minimizes problems before they occur in a real situation. Testing not only addresses data integrity but also keeps personnel current with recovery procedures.



# Vulnerability/ Intrusion Detection

## General Network Security and Intrusion Detection Information

### Patch management

Patches are applied to systems and applications at Paychex to address security issues. Patch deployment timeframes are based on the risk of exploitation and are aligned with industry best practices. Patches are staged in nonproduction environments to evaluate stability and performance impact on the target assets.

### Levels of network security testing

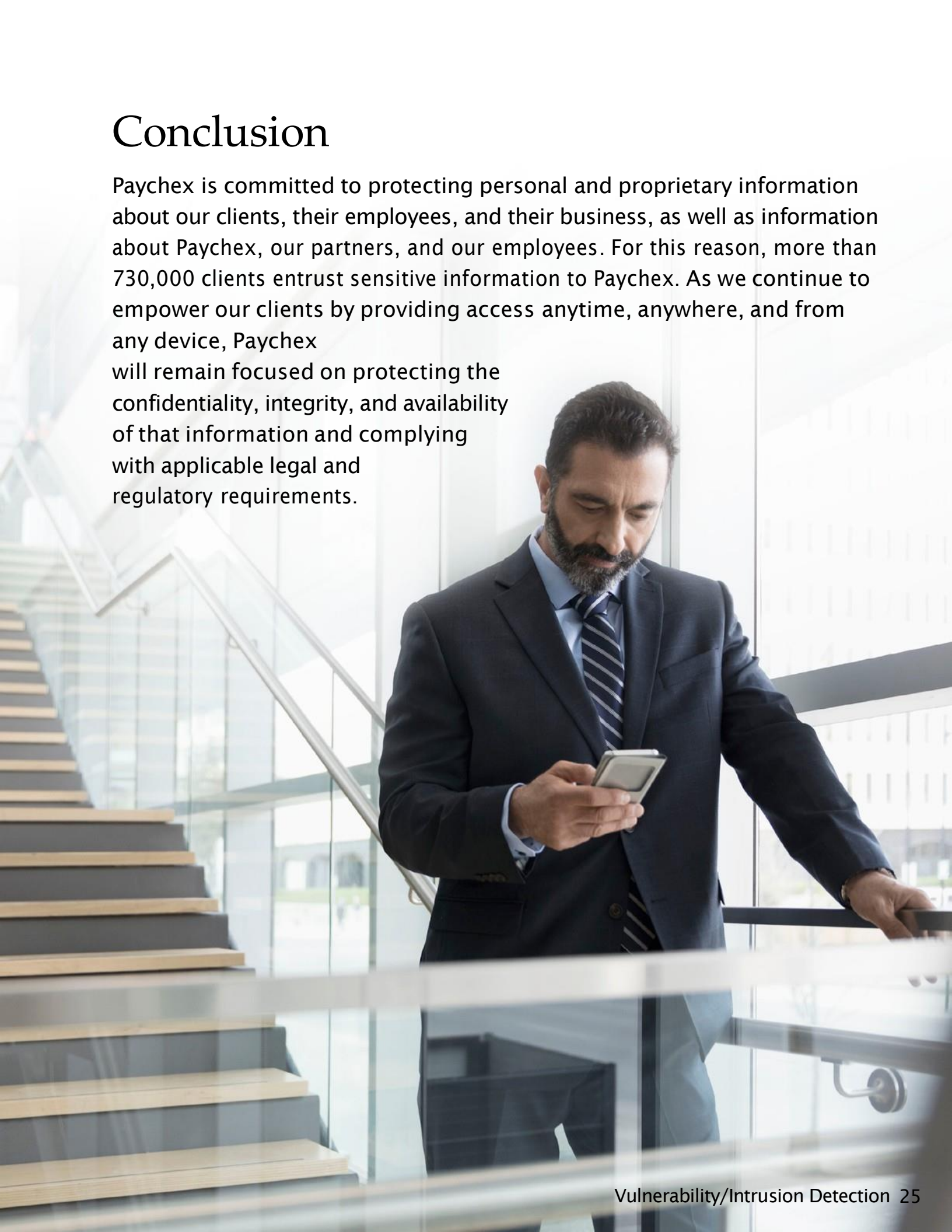
Vulnerability scanning — To validate that Paychex is using and applying the best possible technical configuration, ongoing network vulnerability and configuration baseline scans as well as source code scans are performed. The results are shared with the appropriate IT teams inside Paychex to identify the best mitigation strategy. These reviews are critical in measuring progress against desired patch levels and code quality metrics. When applicable and possible, the hardware and software of external vendors are scanned for vulnerabilities.

Penetration testing — Ongoing internal and external penetration testing is performed against our infrastructure and our applications. After management reviews these reports, remediation is performed if necessary.

Bug Bounty — Paychex Flex® and other Paychex applications are part of a private, invitation-only bug bounty program that rewards security researchers for the identification of complex and critical vulnerabilities within our web applications.

# Conclusion

Paychex is committed to protecting personal and proprietary information about our clients, their employees, and their business, as well as information about Paychex, our partners, and our employees. For this reason, more than 730,000 clients entrust sensitive information to Paychex. As we continue to empower our clients by providing access anytime, anywhere, and from any device, Paychex will remain focused on protecting the confidentiality, integrity, and availability of that information and complying with applicable legal and regulatory requirements.



# About Paychex

Paychex, Inc. (NASDAQ:PAYX) is a leading provider of integrated human capital management solutions for payroll, benefits, human resources, and insurance services. By combining its innovative software-as-a-service technology and mobility platform with dedicated, personal service, Paychex empowers small and medium sized business owners to focus on the growth and management of their business. Backed by 50 years of industry expertise, Paychex serves more than 730,000 payroll clients as of May 31, 2023, across more than 100 locations in the U.S. and Europe and pays one out of every 12 American private sector employees. Learn more about Paychex by visiting paychex.com and staying connected on Twitter and LinkedIn.

PAYCHEX®

HR | Payroll | Benefits | Insurance

The Power of Simplicity®

© 2021 Paychex, Inc. All Rights Reserved. | Rev. 07/01/2023