

# SOC 3 Report

Manson Western, LLC  
(WPS - Western Psychological Services)

April 16, 2022 to April 15, 2023  
Next Report Issue Date: May 5, 2024

An Independent Service Auditor's Report on Controls Relevant to Security,  
Confidentiality, Availability



**AUDIT AND ATTESTATION BY**



## Table of Contents

<b>Management's Assertion</b>	<b>5</b>
<b>Independent Service Auditor's Report</b>	<b>8</b>
Background	8
Scope	8
Service Organization's Responsibilities	9
Service Auditor's Responsibilities	9
Inherent Limitations	10
Opinion	10
Restricted Use	11
<b>System Description</b>	<b>12</b>
Company Overview and Types of Products and Services Provided	13
The Components of the System Used to Provide the Services	14
People	14
Processes and Procedures	17
System Boundaries	18
The Applicable Trust Services Criteria and the Related Controls Designed to Provide Reasonable Assurance that the Service Organization's Service Commitments and System Requirements were Achieved	19
Integrity and Ethical Values	19
Commitment to Competence	19
Management's Philosophy and Operating Style	19
Organizational Structure and Assignment of Authority and Responsibility	20
Human Resource Policies and Practices	20
Security Management	21
Security Policies	21
Personnel Security Procedures	22
Change Management	22
System Monitoring	23
Incident Management	24
System Account Management	25
Integration with Risk Assessment	25
Information and Communications Systems	26
Access to Production Code Base	26
Complementary Subservice Organization Controls (CSOCs)	27
Any Specific Criterion of the Applicable Trust Services Criteria that is Not Relevant to the System and the Reasons it is Not Relevant	28
Disclosures of Significant Changes In Last 1 Year	29



# SECTION 1

Management's Assertion



## Management's Assertion


We have prepared the accompanying description of Manson Western, LLC's (WPS - Western Psychological Services) system throughout the period April 16, 2022, to April 15, 2023, based on the criteria for a description of a service organization's system set forth in DC 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 3 ® Report. The description is intended to provide report users with information about WPS's system that may be useful when assessing the risks arising from interactions with WPS's system, particularly information about system controls that WPS has designed, implemented and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Confidentiality and Availability set forth in *TSP 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*.

WPS uses a subservice organization for cloud hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at WPS, to achieve WPS's service commitments and system requirements based on the applicable trust services criteria. The description presents WPS's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of WPS's controls. The description does not disclose the actual controls at the subservice organization.

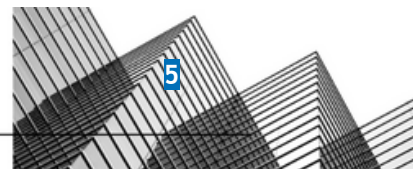
The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at WPS, to achieve WPS's service commitments and system requirements based on the applicable trust services criteria. The description presents WPS's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of WPS's controls.

We confirm, to the best of our knowledge and belief, that:

- a. The description presents WPS's system that was designed and implemented throughout the period April 16, 2022, to April 15, 2023, in accordance with the description criteria.
- b. The controls stated in the description were suitably designed throughout the period April 16, 2022, to April 15, 2023, to provide reasonable assurance that WPS's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout the period, and if the subservice organization and user entities applied the complementary controls assumed in the design of WPS's controls during that period.
- c. The controls stated in the description operated effectively throughout the period April 16, 2022, to April 15, 2023, to provide reasonable assurance that WPS's service commitments and system requirements were achieved based on the applicable trust services criteria, if the complementary subservice organization and complementary user entity controls assumed in the design of WPS's controls operated effectively throughout the period.

DocuSigned by:  
  
-----F86671931F5748C-----

Rocco Cretacci  
Director of Infrastructure, Security Officer  
Manson Western, LLC





# SECTION 2

Independent Service Auditor's Report

**PRESCIENT**  
**ASSURANCE**

## Independent Service Auditor's Report

To: Manson Western, LLC

### Background

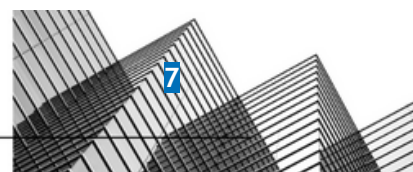
Prescient Assurance, LLC is a licensed CPA Firm which provides audits and examinations for SOC2 attestations, Cloud Security Alliance STAR attestations, HIPAA, GDPR, CCPA, and FISMA compliance. Prescient Assurance is a leader in security certifications for B@B SAAS companies worldwide. We are a global Top 10 cloud security auditor certified by the Cloud Security Alliance STAR program.

### Scope

We have examined WPS's ("WPS") accompanying description of its Online Evaluation System found in Section 3, titled WPS System Description throughout the period April 16, 2022, to April 15, 2023, based on the criteria for a description of a service organization's system set forth in DC 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2 ® Report, and the suitability of the design and operating effectiveness of controls stated in the description throughout the period April 16, 2022, to April 15, 2023, to provide reasonable assurance that WPS's service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Confidentiality and Availability set forth in *TSP 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*.

WPS uses a subservice organization for cloud hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at WPS, to achieve its service commitments and system requirements based on the applicable trust services criteria. The description presents WPS's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of WPS's controls. The description does not disclose the actual controls at the subservice organization. Our examination did not include the services provided by the subservice organization, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

The description indicates that certain complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at WPS, to achieve WPS's service commitments and system requirements based on the applicable trust services criteria. The description presents WPS's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of WPS's controls. Our examination did not include such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls.



## Service Organization's Responsibilities

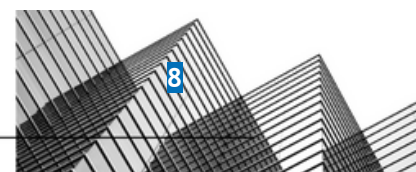
WPS is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that WPS's service commitments and system requirements were achieved. In Section 1, WPS has provided the accompanying assertion titled "Management's Assertion of WPS" (assertion) about the description and the suitability of the design and operating effectiveness of controls stated therein. WPS is also responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; selecting the applicable trust services criteria and stating the related controls in the description; and identifying the risks that threaten the achievement of the service organization's service commitments and system requirements.

## Service Auditor's Responsibilities

Our responsibility is to express an opinion on the description and on the suitability of design and operating effectiveness of controls stated in the description based on our examination. Our examination was conducted in accordance with attestation standards established by the AICPA. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the description is presented in accordance with the description criteria and the controls stated therein were suitably designed and operating effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

An examination of the description of a service organization's system and the suitability of the design and operating effectiveness of controls involves:

1. Obtaining an understanding of the system and the service organization's service commitments and system requirements.
2. Assessing the risks that the description is not presented in accordance with the description criteria and that controls were not suitably designed or did not operate effectively.
3. Performing procedures to obtain evidence about whether the description is presented in accordance with the description criteria.
4. Performing procedures to obtain evidence about whether controls stated in the description were suitably designed to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria.
5. Testing the operating effectiveness of controls stated in the description to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria.





6. Evaluating the overall presentation of the description.

Our examination also included performing such other procedures as we considered necessary in the circumstances.

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the examination engagement.

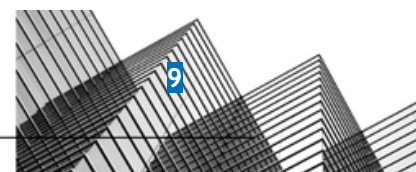
## Inherent Limitations

The description is prepared to meet the common needs of a broad range of report users and may not, therefore, include every aspect of the system that individual report users may consider important to meet their informational needs. There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements are achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the suitability of the design or operating effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

## Opinion

In our opinion, in all material respects:

- a. The description presents WPS's system that was designed and implemented throughout the period April 16, 2022, to April 15, 2023, in accordance with the description criteria.
- b. The controls stated in the description were suitably designed throughout the period April 16, 2022, to April 15, 2023, to provide reasonable assurance that WPS's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout the period and if the subservice organization and user entities applied the complementary controls assumed in the design of WPS's controls throughout the period.
- c. The controls stated in the description operated effectively throughout the period April 16, 2022, to April 15, 2023, to provide reasonable assurance that WPS's service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls assumed in the design of WPS's controls operated effectively throughout the period.



## Restricted Use

This report is intended solely for the information and use of WPS, user entities of WPS's system during some or all of the period April 16, 2022 to April 15, 2023, business partners of WPS subject to risks arising from interactions with the system, practitioners providing services to such user entities and business partners, prospective user entities and business partners, and regulators who have sufficient knowledge and understanding of the following:

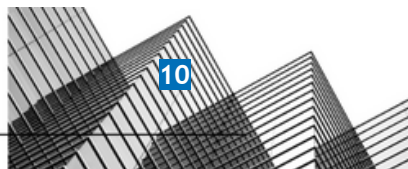
1. The nature of the service provided by the service organization.
2. How the service organization's system interacts with user entities, business partners, subservice organizations, and other parties.
3. Internal control and its limitations.
4. Complementary subservice organization controls and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements.
5. User entity responsibilities and how they may affect the user entity's ability to effectively use the service organization's services.
6. The applicable trust services criteria.
7. The risks that may threaten the achievement of the service organization's service commitments and system requirements and how controls address those risks.

This report is not intended to be, and should not be, used by anyone other than these specified parties.

Prescient Assurance LLC

DocuSigned by:  
*John D Wallace*  
F5ADFAS569EA450.....

John D. Wallace, CPA  
Chattanooga, TN  
May 10, 2023





# SECTION 3

System Description





## Company Overview and Types of Products and Services Provided

WPS is a leading independent publisher of educational and psychological assessments and related intervention resources. With more than 70 years of experience, we've built a global reputation as assessment experts in the areas of autism, speech and language, school and clinical psychology, and occupational therapy. We develop tests that improve clinical evaluation, inform diagnosis, and guide therapy. In doing so, we foster personal connections between authors and clinicians, educators, and researchers who use their tests. When we develop a new test, we bring an author's idea to life, answer a researcher's question, meet a clinician's need, and, ideally, change an individual's life for the better.

WPS is a profitable, dynamic, and growing company engaged in work that makes a difference in people's lives. We offer the stability of a third-generation family business combined with the entrepreneurial spirit of a startup. We recognize that the world is changing fast, and that equally applies to our field and industry. For years, we've been investing in digital transformation and new ways of working. This has only accelerated in a post-covid world. Our mission is "unlocking potential." Inspired by our customers, who dedicate themselves to helping others in need, we hope to better understand the impact of our products and services on their lives. We are equally dedicated to applying the same to ourselves; as we continue to invest in a company culture that encourages growth, innovation, creativity, transparency, and collaboration.

## The Principal Service Commitments and System Requirements

WPS will use commercially reasonable efforts to make Service available with an uptime percentage of at least 99.99%. WPS knows that providing the best possible support to our customers is critical to making our customers successful. Email, phone, and chat support is available from 6 am - 4 pm PST (M-F)

WPS would provide ongoing support to customers using the approved service support channel and knowledge base resources. When a request or transaction is submitted, WPS will authenticate the customer to verify their identity in proportion to the risk of the request or transaction.

The WPS Online Evaluation System is an Internet-based platform for administering and scoring assessments. It improves clinical efficiency by allowing you to administer and score WPS assessments electronically. This industry-leading digital solution streamlines assessment delivery, allowing you more time for helping your clients. The WPS Online Evaluation System provides access to a variety of assessments mostly for children and adolescents.

Internet access is required along with one of the following compatible web browsers:

1. Mozilla Firefox version 54 and later (recommended)
2. Google Chrome version 58 and later
3. Microsoft Internet Explorer version 10 and later
4. Apple Safari version 10.0 and later

## The Components of the System Used to Provide the Services

### People

People	
Role	Responsibilities
Management	Responsible for enabling other employees to perform their jobs effectively and for maintaining security and compliance across the environment.
Product Management	Helps WPS define product requirements that meet customer needs by collecting customer insights and market research data to identify product viability, new product opportunities, and business scalability to meet larger company objectives across both paper and digital products, including our digital platform.
IT Infrastructure & Support	Responsible for ongoing procurement, support, maintenance and management of the servers, networking, data storage, computers, applications and other systems used to support WPS services. Also, responsible for providing timely resolution of employees' technical issues and problems.
IT Applications	Designs and implements new functionality, assesses and remediates any issues or bugs found in the WPS Platform, and architects and deploys the underlying cloud infrastructure on which the platform runs. Develops and enforces coding standards and best practices including performance, security, monitoring policies, and procedures.
Customer Service	Responsible for providing internal and external customer support via phone, email, and live engagement. Additional responsibilities consist of order management, quote processing, general inquiries, and product returns.
Accounting & Finance	The Accounting and Finance department is responsible for the recording and reporting of all financial transactions within the business including the preparation of customer bills, payment of bills and payroll, maintenance of general ledger, and preparation of financial statements. Additionally, the department is responsible for tax and business compliance as well as analyzing financial data and preparing departmental and company budgets and forecasts.

People	
Role	Responsibilities
Marketing	Responsible for ongoing communication, strategic vision, and execution of all marketing programs, plans, and promotions including but not limited to paid advertising, email, conference exhibit, eCommerce site, social media, and content development. Also responsible for internal support of the WPS Sales and Training Departments and for any WPS customer facing channel used for promotion or advertising of products.
Project Management	Responsible for project planning and execution of all projects across the company through cross-collaboration and communication.
Art & Production	Executes design and copyediting work on WPS assessment products, marketing and sales collateral, and training presentations. Maintains, upholds, and evolves WPS brand style. Interfaces with WPS Procurement department and external vendors to ensure timely delivery and high-quality standards across printed products.
Facilities	Responsible for the maintenance and upkeep of the WPS facility in Torrance.
Fulfillment	Responsible for the receipt, storing, inventory control/management, assembly, picking, and shipping of WPS goods and services.
Professional Development & Training	Responsible for delivering high-quality professional training experiences to our customers, including continuing education for independent study products, webinars, and in-person courses. Includes responsibility for all related order processing and activating and delivering courses through the WPS Learning Management System (WPS LMS).
People	The People Department is responsible for the various traditionally Human Resource responsibilities of compliance, employee life cycle processing, engagement, benefits administration, and coaching. Our department is also responsible for payroll processing and the positive reinforcement of culture, policy, and practices.
Procurement	Responsible for ongoing procurement, purchasing requests are filled - both goods and services are purchased by purchasers and delivered by suppliers. Strategic activities, like demand planning, responsible for finding new suppliers, running various sourcing activities, and negotiation terms and conditions. Take part in new savings initiatives, KPIs, and on-time, on-quality, and on-cost deliveries. Communication and teamwork, maintaining information about existing suppliers, giving operational



People	
Role	Responsibilities
	visibility, and keeping track of daily task, and automating routine processes.
Research & Development	Responsible for developing WPS assessments by working with authors to develop and refine item content for ratings scales and performance measures, collecting nationally representative data and clinical samples, analyzing data and developing norms, and producing manuals and content for forms, easels, and record forms. Also, responsible for developing and delivering training and intervention products and providing customer support across all products.
Rights & Permissions	Responsible for asserting intellectual property rights over WPS proprietary content, managing WPS's publishing agreements, approving and issuing licensing and permissions arrangements, processing licensing revenue, collecting royalty recipients' contact and tax ID information for provision to WPS Accounting, assisting authors or their estates in the transfer of rights as appropriate, and approving and issuing WPS Research Discounts. Also assists other departments with consultant agreements and other contracts related to outside contributions to WPS-owned content.
Sales	Responsible for supporting our customers in their assessment needs and purchases. We focus on providing solutions; be that training on products through site visits, webinars, or convention attendance, providing quotes, assisting with vendor registrations, or processing orders.
IT Security & Compliance	Responsible for providing ongoing information security to WPS's assets (people, application, infrastructure, and data). Also responsible for supporting and maintaining ongoing regulatory compliance initiatives.
Operations	Responsible for trade compliance, strategic and operational objectives, budgets, quality control, facility upkeep, the safety of staff, and finding ways to increase the quality of customer service.
IT DevOps	Responsible for deployment governance including CICD, SecOps-integration of SAST and DAST Tools and Source Code and Release Management with tagging and Branching Merging. Ensuring highly available solutions including replication, clustering, etc. Design, implement, and document Disaster Recovery strategies for critical business servers for OES. Communicate and coordinate with other IT teams to successfully resolve support and maintenance issues.

People	
Role	Responsibilities
IT Database Engineering	Responsible for implementing database solutions. Develops and enforces database standards and best practices including performance, security, monitoring policies, and procedures.

## Processes and Procedures

Processes and Procedures	
Procedure/Process	Description
Security Policy	The Company's policies concerning various security, availability, and confidentiality matters are reviewed at least annually by the Security Team.
Risk Assessment	At least annually the COO, Privacy Officer, VP of Engineering, and the Cyber Security Officer collaborate on an overall risk assessment for WPS and the Online Evaluation System.
Communication	WPS opportunistically and continually uses a mixture of intranet services, email, and in-person meeting opportunities for the communication of security policies and procedures. Regular confirmation of this communication is captured in annual attestations from each team member that they have read general internal policies.
Logical Access	All team members must have unique credentials as well as established authorization to access WPS's information assets. Access to systems and information is restricted based on the responsibilities of the individual and their role.
Change Management	WPS has a Secure Development Policy. The policy covers the planning, assignment, development, design, code review, impact considerations, infrastructure assignments, quality assurance, security testing, implementation, and maintenance of both the System software and infrastructure.

#### Third Party Access

Third Party Access	
Name of Third Party/ Vendor	Type of Access and Connectivity to data
AWS	AWS provides infrastructure and database components.

#### System Boundaries

System Boundaries	
Name of the System	Purpose
None	None

## The Applicable Trust Services Criteria and the Related Controls Designed to Provide Reasonable Assurance that the Service Organization's Service Commitments and System Requirements were Achieved

### Integrity and Ethical Values

WPS is committed to protecting employees, customers, partners, vendors, and the company from illegal or damaging actions by individuals, either knowingly or unknowingly. Our Corporate Ethics Policy establishes behavioral and ethical standards for WPS employees, vendors, and the company and serves to guide business behavior to ensure ethical conduct.

WPS employees will maintain the highest ethical standards in the conduct of company business. The intent is that each associate will conduct WPS's business with integrity and comply with all applicable laws in a manner that excludes considerations of personal advantage or gain.

### Commitment to Competence

WPS's management defines competence as the knowledge and skills necessary to accomplish tasks that define employees' roles and responsibilities. Management's commitment to competence includes management's careful consideration and review of detailed job descriptions for roles. These job descriptions outline accountabilities, skills necessary to do the work, and behavioral competencies. These job descriptions are updated each time a role needs to be filled, a promotion is outlined, or if the role's requirements are changed. Employees are asked to review these new job descriptions upon entry into their new role.



Training is provided to current staff on an as-needed basis to maintain the skill level of personnel. This training is one on one and based on the individuals' needs at the time.

## Management's Philosophy and Operating Style

WPS is a stable, successful company engaged in work that makes a difference in people's lives. We have the stability of a third-generation family business combined with the entrepreneurial drive of a startup. WPS is a place where people come to build careers. Many of our 120+ employees have been with us for 10, 20, or even 30 years or more.

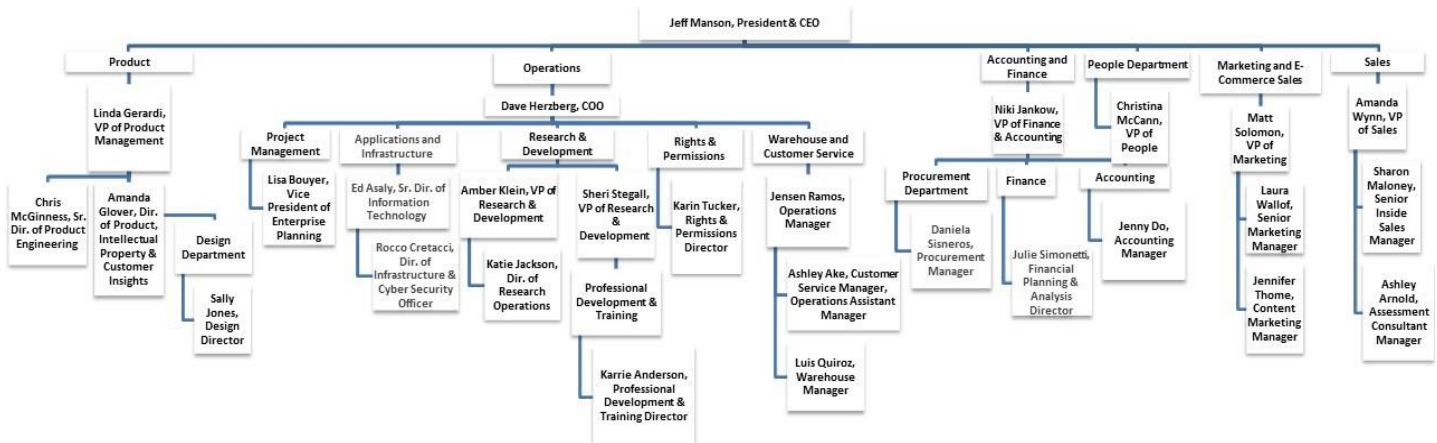
WPS's management team is committed to creating a productive and encouraging work environment as well as providing a secure product to our customers and users. To accomplish this WPS has instituted a number of processes:

- Quarterly "all hands" meetings for employees to voice their blocks, successes, and concerns
- A rigorous QA program ensuring that software development meets industry security standards
- Meetings are held between managers on a monthly basis to prioritize objectives and tasks
- Employees are encouraged to engage in a process of collaborative problem-solving in dealing with any challenging or unexpected situation.

## Organizational Structure and Assignment of Authority and Responsibility

WPS has a simple organizational structure. Employees report directly to the Department Heads, Managers, or Supervisors, who ultimately provide direction. WPS has clearly defined job descriptions and as the organization grows, we have in place, roles and responsibilities which will allow for the dissemination of managerial responsibilities as necessary. WPS has taken the following steps to achieve this goal:

- Regularly updated organization chart fully accessible by employees
- Responsibilities of roles are clearly defined in policies and job descriptions.



## Human Resource Policies and Practices

Our People Department Mission Statement:

In support of our company's principles, values, vision, and mission, it is the charge of the People Department to help WPS thrive by helping our People Thrive.

It is our mission to:

- Build trust: our organization succeeds and grows on a foundation of trust.
- Create an atmosphere that fosters belonging, creativity, collaboration, and career growth.
- Commit to doing and to acting openly, equitably, and consistently.
- Promote ethical and legal conduct in personal and business practices.
- Communicate in a candid and fair manner.
- Foster diversity and inclusion in our workforce.

Some of the transactional practices that support this mission include the ongoing process improvement and documentation of processes to deliver a transparent and expected outcome for each step. Hiring and retaining competent and qualified talent is key and is accomplished through the rigorous hiring practices of the organization. This includes not only a technical skill review, a cross-functional interview, and a culture fit interview so the right people are determining the most qualified candidate for the role.

Our culture is one that involves collaboration and individualized care based on the specific situation surrounding an issue. Each issue is resolved with the mission, labor law, and values of the organization in mind.

As a matter of standard practice, WPS routinely conducts the following for all staff:

- Annual performance reviews
- Regular feedback and team collaboration on projects
- Monthly employee cyber security training and annual safety training
- New employees are required to sign a confidentiality agreement upon hire
- WPS recognizes that policies and procedures often need to change to serve the needs of the organization. To accomplish this, all security procedures are regularly reviewed and updated based on need.

## Security Management

The WPS Information Security team is composed of an internal Director of Infrastructure, a Cyber Security Officer, and a Systems Engineer. They are responsible for enforcing the information security policies, configuring, monitoring, and maintaining preventative, corrective, and detective controls within the WPS environment, and ensuring user awareness training is conducted. WPS also employs a 3rd party Managed DetectionResponse team that provides 24/7 security monitoring, threat hunting, threat containment, and security advisory services.

## Security Policies

WPS has adopted the following Security Policies:

- Acceptable Use
- Access Control
- Asset Management
- Backup and Restoration
- Business Associate Agreement
- Business Continuity and Disaster Recovery
- Change Management
- Clean Desk and Clear Screen
- Confidentiality and Non-Disclosure Agreement
- Confidential Communication
- Corporate Ethics
- Customer Support and SLA
- Data Integrity
- Data Retention and Disposal
- Guidelines on Uses and Disclosure of Protected Health Information (PHI)
- HIPAA Breach Notification Policy
- HIPAA Internal Privacy Policy
- Incident Management
- Internal Audit
- Information Classification
- Information Security
- Key Management and Cryptography
- Limited Data Set Policy
- Logging and Monitoring
- Network Security
- Patch Management Policy
- Personnel Security
- PHI De-identification Policy and Procedure
- PHI Retention and Disposal
- Physical and Environmental Security
- Privacy Policy for Websites
- Progressive Disciplinary Policy
- Risk Assessment
- Server Security
- Social Media Policy
- Software Development
- Standards of Conduct
- System Maintenance Policy
- Technology Equipment Handling and Disposal
- Vendor Management
- Vulnerability and Penetration Testing Management
- Workstation and Mobile Device



## Personnel Security Procedures

WPS has several personnel security procedures in place specifically during the onboarding process. These include:

- Background checks for new employees.
- Employees must read and agree to all security policies.
- Roles within the organization have been clearly defined and are reflected in the organizational chart.
- Employees are granted access/authorization based on their role and in accordance with the principle of least privilege.
- Upon hire and monthly thereafter, security awareness training is completed by all WPS employees.
- Employees are directed to report any potential security incidents to the Cyber Security Officer.
- Violations of WPS security policies have clearly defined repercussions.

## Change Management

WPS's change management procedures are detailed in the Change Management Policy. There are six key requirements for all changes to the organization, business processes, information processing facilities, and systems that affect information security in WPS's production environment. They are as follows:

- All change requests must be entered into the ticketing system of record and all approvals, scheduling, comments, and implementation details will be recorded as part of the entered ticket.
- Changes to the information system shall be authorized, documented, and controlled using a formal change control procedure.
- All changes are tested and reviewed before deployment to production.
- Development/test environments are separate from production environments with access control in place to enforce separation.
- Production data shall not be used for testing or development.
- A rollback process must be used for unsuccessful deployments.

## System Monitoring

System Monitoring	
Service	Description
AWS Cloudwatch	Used for monitoring of network usage, availability, and overall performance and health of network resources. Also logs metrics for fine-tuning alarms and alerts as usage data is received. Amazon CloudWatch Logs are used in conjunction with AWS CloudTrail to monitor for failed and successful authorization attempts.

System Monitoring	
Service	Description
Vulnerability Management Platform	Compliance Automation Platform allows us to monitor multiple aspects of your attack surface including employee devices, monitoring AWS resources for potential configuration vulnerabilities, and tracking necessary patches/updates.
AWS CloudTrail	Used to log actions taken by users and services within our AWS account.
WAF	Provide metrics regarding attempted and successful requests to the application.
3rd Party Penetration Testing	Validate WPS systems in an attempt to identify weaknesses and/or security gaps in all areas of an organization, from the web or mobile applications to supporting network landscapes.
Endpoint Security	Securing endpoints or entry points of end-user devices such as desktops, laptops, and mobile devices from being exploited by malicious actors and campaigns. Endpoint security systems protect these endpoints on a network or in the cloud from cybersecurity threats.
Intrusion Prevention System	Continuously monitor the network for malicious activity and take action to prevent it, including reporting, blocking, or dropping it, when it does occur.
Security Assurance Platform	Used to manage and monitor our InfoSec and Compliance program as well as security posture vulnerabilities with some of our systems.
Managed Detection & Response - MDR	MDR is designed to identify and remove cyber threats from a company's environment with the help of an expert offsite security operation center and a dedicated security team. This is a 24/7 operation that's also proactive. Security analysts can step into the customer's environment to look for adversarial behavior rather than rely on a tool that reactively detects that something is going on.

System Monitoring	
Service	Description
AWS GuardDuty	Amazon GuardDuty is a continuous security monitoring service that analyzes and processes the following Data sources: VPC Flow Logs, AWS CloudTrail management event logs, CloudTrail S3 data event logs, and DNS logs. It uses threat intelligence feeds, such as lists of malicious IP addresses and domains, and machine learning to identify unexpected and potentially unauthorized and malicious activity within your AWS environment. This can include issues like escalations of privileges, uses of exposed credentials, or communication with malicious IP addresses, or domains.
Datadog, SumoLogic	Application metrics such as response and request times, distributed tracing, complete serverless monitoring

## Incident Management

WPS's incident response procedures are detailed in its Incident Response Plan. Our primary goals will be to investigate, contain any exploitations, eradicate any threats, recover WPS systems, and remediate any vulnerabilities. Throughout this process, thorough documentation will be required as well as a post-mortem report.

Specific steps that WPS will take are:

- The Security Officer will manage the incident response effort
- A recurring Incident Response Meeting will be held at regular intervals until the incident is resolved.
- WPS will inform all necessary parties of the incident without undue delay
- Should the breach involve the release or loss of control of PHI, WPS will refer to its HIPAA Addendum to the Incident Response Plan. The addendum lays out specific definitions as well as a comprehensive plan for remediation.

## Data Backup and Recovery

This Backup and Restoration Policy includes:

- Backup data shall be protected with the same level of security as the production data.
- The frequency, extent and retention of backups shall be in accordance with the importance of the information and the acceptable risk as determined by the data owner.
- Backup data shall not be stored in the same location as the production data.
- Backup jobs shall be monitored to check for and correct errors.
- Backups shall be periodically tested to ensure that they are recoverable and verify data integrity.





- Records demonstrating the review of logs and test restores should be kept to demonstrate compliance with this policy for auditing purposes.
- All backup data shall be stored encrypted using strong encryption mechanisms or the same access controls as the data in production.
- Access to backup data shall be reviewed at least annually.

## System Account Management

WPS's access management procedures are documented in its Access Control Policy. WPS uses Role-based authorization to control access to its network infrastructure. WPS uses the principle of least privilege to determine the type and level of access to grant users. A number of standards are in place that WPS uses when granting access to its systems:

- Valid access authorization from the immediate supervisor or system owner,
- The principle of least privilege, which allows only authorized access to users, including privilege users based on their job functions and intended system usage,
- Considering the separation of duties between individuals, to prevent malicious activity without collusion, and,
- Other attributes as required by the WPS or business function.
- Restrict user accounts from installing software on devices.
- Administrator, system, and generic accounts shall be strictly controlled and given access based on an authorization from designated personnel. WPS shall authorize and monitor the use of guest/anonymous and temporary accounts.
- Temporary and inactive accounts that are no longer required and accounts of terminated or transferred users shall be deactivated promptly. Account access privileges shall be reviewed periodically.
- Access Approval: WPS shall follow a documented formal access approval process for granting or changing access privileges.

## Risk Management Program Activities

On a practical level, WPS's Risk Management process shall focus on the following five types of activities: Identification of Strategic Objectives, Identification of Risks, Analysis of Risks, Mitigation Planning, and Tracking and Controlling Risks. Examples of categories used are technical, reputational, contractual, financial, regulatory, and fraud risks.

The risk assessment focuses on the likelihood and potential impact of risks to WPS. Likelihood can be assessed as not likely, somewhat likely, or very likely. Impact can be assessed as not impactful, somewhat impactful, and very impactful. These factors together will give an overall risk ranking. WPS's stance towards any given risk is based on the assessment described above. Where WPS chooses a risk response other than "Accept," it shall develop a Risk Treatment Plan. WPS's stance will fall into one of the following categories:

- Mitigate: WPS may take actions or employ strategies to reduce the risk
- Accept: WPS may decide to accept and monitor the risk at the present time. This may be necessary for some risks that arise from external events.

- Transfer: WPS may decide to pass the risk on to another party. For example, contractual terms may be agreed to ensure that the risk is not borne by WPS, or insurance may be appropriate for protection against financial loss.
- Eliminate: The risk may be such that WPS could decide to cease the activity or to change it in such a way as to end the risk.

## Risk Assessment

WPS's Risk Assessment process takes into account a number of factors each of which contributes to both the likelihood and potential impact of a given risk. These include:

- The criticality of potentially impacted business processes.
  - Whether a risk could potentially impact the confidentiality, availability, integrity, or privacy of customer data, PII, or PHI.
  - Potential monetary loss.
  - The ability of the risk to impact WPS's business objectives.
  - Potential impact to WPS customers or vendors
- WPS uses Risk Treatment Plans for any response to risks other than "Accept".

## Integration with Risk Assessment

WPS is committed to handling and remediating risks inherent in any commitments, agreements, or responsibilities it may enter into or take on during the operation of the company. Due to the nature of these risks, it may be necessary for WPS to develop specialized controls. WPS takes into account all relevant factors; contractual, legal, and regulatory when designing these controls. In general, WPS's Risk Assessment procedure is still applicable to risks inherent in WPS's commitments and contractual responsibilities and should be applied to determining the severity of risks.

## Access to Production Code Base

WPS uses a fully encrypted VPN solution as well as HTTPS and TLS 1.2 to communicate with and access its network. Furthermore, MFA is required to access any production code base and SSO is used wherever possible.

Access Control to the production code base is limited via the following controls:

- VPN credentials must be used to access any part of WPS's codebase
- The production code branch is protected, requiring a merge request and approval before any changes can be made. This also protects the branch from being deleted.
- RBAC approach is used for accessing the application code repository.

## Internal Monitoring

WPS has various internal infrastructure, security, and physical environmental monitoring solutions in place that will alert on many factors such as hardware failures, security incidents and breaches, capacity monitoring, and environmental issues.

WPS has a highly interconnected business process allowing for visibility and insight by management into the operations of each department. Corrective action is initiated through various mediums. Within departments, process reviews and quality assurance help ensure internal controls are being followed and implemented.

## Complementary Subservice Organization Controls (CSOCs)

Although the subservice organization has been “carved out” for the purposes of this report, certain Trust Services Criteria are intended to be met by controls at the subservice organization.

Complementary Subservice Organization Controls (CSOCs)	
Criteria	Complementary Subservice Organization Controls
CC6.4	AWS is responsible for restricting data center access to authorized personnel.
CC6.4	AWS is responsible for the 24/7 monitoring of data centers by closed circuit cameras and security personnel.
CC7.2, A1.2	AWS is responsible for the installation of fire suppression and detection, and environmental monitoring systems at the data centers.
CC7.2, A1.2	AWS is responsible for protecting data centers against disruption in power supply to the processing environment by an uninterruptible power supply.
CC7.2, A1.2	AWS is responsible for overseeing the regular maintenance of environmental protections at data centers.

## Any Specific Criterion of the Applicable Trust Services Criteria that is Not Relevant to the System and the Reasons it is Not Relevant

Trust Service Categories in Scope		
Category	Definition	Applicable



Security	Information and systems are protected against unauthorized access, unauthorized disclosure of information and damage to systems that could compromise the availability, integrity, confidentiality and privacy of information or systems and affect the entity's ability to meet its objectives.	Yes
Availability	Information and systems are available for operation and use to meet the entity's objectives	Yes
Confidentiality	Information designated as confidential is protected to meet the entity's objectives	Yes
HIPAA	The HIPAA Security Rule Standards and Implementation Specifications has four major sections, created to identify relevant security safeguards that help achieve compliance: 1) Physical; 2) Administrative; 3) Technical, and 4) Policies, Procedures, and Documentation Requirements.	Yes

## Disclosures of Significant Changes In Last 1 Year

No significant changes in the last 12 months.