ePS Packaging US, LLC

SYSTEM AND ORGANIZATION CONTROLS
SOC 3 REPORT

MANAGEMENT'S REPORT OF ITS ASSERTIONS ON THE EFFECTIVENESS OF ITS CONTROLS OVER THE ePS PACKAGING SYSTEM BASED ON THE TRUST SERVICES CRITERIA FOR SECURITY, AVAILABILITY, AND CONFIDENTIALITY

November 6, 2025 to May 25, 2026

TABLE OF CONTENTS

SECTION I: INDEPENDENT SERVICE AUDITOR'S REPORT.....03
SECTION II: MANAGEMENT ASSERTION OF EPS.....07
SECTION III: DESCRIPTION OF EPS SYSTEM.....09
SECTION IV: APPENDIX.....32

SECTION : I

INDEPENDENT SERVICE AUDITOR'S REPORT

Precision Assurance
CPA LLC

Independent Service Auditor's Report

To: **EPS Packaging US, LLC**

Scope

We have examined EPS Packaging US (also referred to as "ePS" or "service organization") accompanying assertion titled "Assertion of ePS Management" (assertion) that the controls within ePS Packaging Platform (the "system") were effective throughout the period November 6, 2025 to May 25, 2026 to provide reasonable assurance that ePS service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, and confidentiality (applicable trust services criteria) set forth in TSP section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria)

ePS utilizes data center colocation services provided by ASK4 and Expedient and cloud hosting services provided by Amazon Web Services (AWS). The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with the controls at ePS, to achieve ePS service commitments and system requirements based on the applicable trust services criteria. Our examination did not extend to the controls implemented by subservice organizations.

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

The description indicates that certain applicable trust services criteria specified in the description can be achieved only if complementary user-entity controls contemplated in the design of EPS Packaging's controls are suitably designed and operating effectively, along with related controls at the service organization. Our examination did not extend to 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

ePS 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 ePS service commitments and system requirements were achieved. ePS has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, ePS is responsible for selecting, and identifying in its assertion, the applicable trust services criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system.

Service Auditor's Responsibilities

Our responsibility is to express an opinion, based on our examination, on whether management's assertion that controls within the system were effective throughout the period to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria.

Our examination was conducted in accordance with the attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects.

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the engagement. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Our examination included:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements.
- Assessing the risks that controls were not effective to achieve ePS service commitments and system requirements based on the applicable trust services criteria.
- Performing procedures to obtain evidence about whether controls within the system were effective to achieve ePS service commitments and system requirements based on the applicable trust services criteria.
- Performing such other procedures as we considered necessary in the circumstances.

Inherent Limitations

There are inherent limitations in the effectiveness of 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 were achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the 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, management's assertion that the controls within ePS Packaging Platform were effective throughout the period November 6, 2025 to May 25, 2026, to provide reasonable assurance that ePS service commitments and system requirements were achieved based on the applicable trust services criteria for security, availability, and confidentiality, is fairly stated, in all material respects, if subservice organization controls assumed in the design of ePS controls operated effectively throughout the period November 6, 2025 to May 25, 2026.

Precision Assurance CPA LLC

Certified Public Accountants
CPA Firm License No: CF-0010917
Dover, Delaware

Date : 20th July, 2026

SECTION : II

MANAGEMENT ASSERTION OF EPS

ASSERTION OF EPS PACKAGING US, LLC MANAGEMENT

We are responsible for designing, implementing, operating, and maintaining effective controls within eProductivity Software's ("ePS" or the "Company") ePS Packaging Platform (the "System") throughout the period November 6, 2025 to May 25, 2026, to provide reasonable assurance that ePS's service commitments and system requirements relevant to security, availability, and confidentiality were achieved. Our description of the boundaries of the System is presented in attachment A and identifies aspects of the System covered by our assertion.

The ePS Packaging Platform encompasses the Packaging Suite, Corrugated Suite, Metrics, and Paxis services, including supporting production environments, hosted cloud infrastructure, code repositories, and the people, processes, and technology controlled by the company. Cloud services are primarily hosted on Amazon Web Services (AWS). The company also utilizes data center colocation services provided by ASK4 and Expedient.

The description in attachment A indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at ePS, to achieve ePS's service commitments and system requirements based on the applicable trust services criteria. The description presents ePS's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of ePS's controls. The description presented in attachment A does not extend to or disclose the actual controls at the subservice organizations. The subservice organizations are carved out from the scope of the examination.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period November 6, 2025 to May 25, 2026, to provide reasonable assurance that ePS's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, and confidentiality (applicable trust services criteria) set forth in TSP section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA Trust Services Criteria). ePS's objectives for the System in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in attachment B.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of these inherent limitations, a service organization may achieve reasonable, but not absolute, assurance that its service commitments and system requirements are achieved.

We assert that the controls within the system were effective throughout the period November 6, 2025 to May 25, 2026, to provide reasonable assurance that ePS's service commitments and system requirements were achieved based on the applicable trust services criteria relevant to Security, Availability, and Confidentiality set forth in the AICPA's TSP section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy, if subservice organizations applied the complementary subservice organization controls assumed in the design of ePS's controls throughout the period November 6, 2025 to May 25, 2026.

Signed by:
Scott Brown
D0DA326E439C466...

ePS

Management of EPS Packaging US, LLC

Date 16 July 2026

SECTION : III

DESCRIPTION OF EPS SYSTEM

OVERVIEW OF OPERATIONS

Company Background

eProductivity Software ("ePS" or the "Company") is a global provider of transformative technology solutions for the packaging and corrugated industries. The ePS delivers software, cloud-hosted platforms, managed services, and professional services that help organizations optimize business operations, production workflows, manufacturing processes, and customer engagement across the packaging lifecycle.

The ePS solutions include Packaging Suite, Corrugated Suite, Paxis, and Metrics services, providing capabilities across estimating, order management, production planning, workflow automation, analytics, reporting, and plant floor operations. These solutions are designed to support packaging manufacturers, converters, and enterprise customers in improving operational efficiency, visibility, scalability, and digital transformation initiatives.

The ePS supports customers globally through cloud and on-premises deployments, with cloud services primarily hosted on Amazon Web Services (AWS). The ePS integrates security, availability, monitoring, backup, and operational governance controls into its service delivery model to support reliable and secure customer operations. The ePS serves customers across multiple regions worldwide, delivering industry-focused technology solutions and managed services tailored to the packaging and corrugated manufacturing sectors.

Types of Services Provided

The ePS Packaging Platform (the "Platform") provides a suite of enterprise resource planning (ERP) and manufacturing execution system (MES) solutions designed specifically for the packaging industry. The table below outlines the services comprising the Platform:

Platform Service / Pillar	Description
Packaging Suite *(Legacy Platform Service)*	A comprehensive ERP and MES solution supporting folding carton, tag and label, and flexible packaging operations. It provides intelligent estimating, production planning, scheduling, inventory, and shop-floor data management to optimize manufacturing efficiency.
Corrugated Suite *(Legacy Platform Service)*	An industry-specific ERP and MES solution designed for corrugated packaging manufacturers. It integrates production planning, inventory, quality management, and business intelligence tools to enhance visibility, productivity, and operational control.
Metrics *(Legacy Platform Service)*	An ERP solution tailored for the Latin American print and packaging market, providing end-to-end functionality for estimating, production, inventory, and financial management across multilingual, multi-currency environments.

Paxis *(Legacy Platform Service)*	A cloud-based ERP solution designed for small and growing label converters. It offers pre-configured, packaging-specific estimating, order management, and production tools within a secure, scalable, and rapidly deployable cloud architecture.
CommandCore ERP Foundation *(CommandCore Pillar)*	**Run the business on one source of truth.** It handles estimating, quoting, order and production management, inventory control, and job costing. By eliminating duplicate entry and manual handoffs, it protects margins and accelerates order cycles from quote to cash.
CommandCore MES *(CommandCore Pillar)*	**Turn plans into perfect execution.** It connects planning directly to the shop floor to deliver real-time tracking, trimming and conversion optimization, and resource management. This provides instant visibility across orders and machines so teams can fix variance without stopping the line.
CommandCore Control Systems *(CommandCore Pillar)*	**Lock in best-practice machine performance.** It captures live machine data to make closed-loop, real-time adjustments and output optimizations. This takes operator guesswork out of production, ensuring repeatable quality and higher throughput regardless of the shift.
CommandCore Operational Excellence *(CommandCore Pillar)*	**Standardise, measure, improve.** It standardizes how work gets done across multi-site operations utilizing automated workflow design, scenario planning, and built-in audit trails.
CommandCore Smart Scheduling *(CommandCore Pillar)*	**Build the plan you can actually run.** It utilizes capacity constraint management and KPI reporting to generate realistic, optimized plans. It allows planners to run rapid "what-if" scenarios to quickly adapt when priorities or materials change.
CommandCore Quality & Compliance *(CommandCore Pillar)*	**Build quality in and prove it fast.** It standardizes Non-Conformance Report (NCR) management and Corrective/Preventive Actions (CAPA). By linking quality actions directly to real production events, it provides end-to-end traceability and always-ready documentation for audits.
CommandCore Sustainability *(CommandCore Pillar)*	**Carbon insight you can act on.** It turns raw operational data into credible carbon accounting and transparency reporting. This allows manufacturers to quickly handle regulatory disclosures and prioritize the right carbon reductions.
CommandCore Smart Supply Agility	**Order and supply, without friction.** It connects B2B customer portals, supplier management, and procurement

(CommandCore Pillar)	into a digital ordering workflow. This reduces manual administrative drag, aligns forecasting with safety stock, and delivers higher service levels.

The Company is responsible for the development, maintenance, and support of the **CommandCore™ platform** comprising its eight unified, packaging-native operational pillars. Built on a secure, cloud-native technology foundation, the platform supports both cloud and hybrid deployment models. Customers may choose to deploy these solutions within customer-controlled on-premises or private cloud environments, or as Company-managed hosted Cloud Services operated on Amazon Web Services (AWS). Depending on the deployment model selected by the customer, the Company may process and store customer data within Company-managed cloud environments.

EPS also offers eMAS (ePS Managed Application Services), a managed service offering that provides operational support, monitoring, maintenance, upgrade coordination, and technical assistance for customer-managed on-premises environments. Customer-managed environments supported through eMAS are not within the scope of this report.

Principal Service Commitments and System Requirements

ePS Packaging Platform was prepared to describe the procedures and controls ePS implemented to manage the risks that threaten the achievement of the service organization's service commitments and system requirements. The disclosure of the principal service commitments and system requirements enables report users to understand the critical objectives that drive the system's operation.

Service Commitments

Service commitments include those made to user entities and others to the extent those commitments relate to the trust services categories addressed by the description. Security objectives and commitments are made available to customers through information shared on ePS website. The following summarizes ePS principal service commitments:

- EPS uses commercially reasonable physical, managerial, and technical safeguards designed to secure data from accidental loss and unauthorized access.
- EPS provides logical tenant separation, encryption in transit (TLS 1.2 or greater), and encryption at rest utilizing AES-256.
- EPS employs routine vulnerability scanning, code review, and other security best practices to manage risks to an ePS Platform installation.
- EPS leverages a mobile device management solution to monitor, manage, update, and secure personnel laptops and workstations.
- EPS continuously monitors access to its infrastructure.
- The Platform provides a 99.9% uptime service level agreement (SLA).
- Access to critical resources and sensitive information requires multi-factor authentication and is provided based on the principle of least privilege.

System Requirements

EPS system requirements are communicated in system policies and procedures, system design documentation, and customer agreements. Information security policies define an organization-wide approach to protecting systems and data and include descriptions and expectations for the system's design, development, and operation. In addition to these policies, standard operating procedures have been prepared to describe specific manual and automated processes required to operate and develop services provided.

Components of the System

A system is designed, implemented, and operated to achieve specific business objectives according to management-specified requirements. The boundaries of the system described in this description include the system components related to the service life cycle. The components of the Platform can be classified into the following five categories: Infrastructure, Software, People, Data, and Procedures.

Infrastructure

EPS infrastructure supporting the Packaging Suite, Corrugated Suite, Metrics, and Paxis services is hosted through a combination of third-party colocation providers and cloud hosting providers, including ASK4, Expedient, and Amazon Web Services (AWS) (collectively, the "Infrastructure Providers"). EPS-managed hosted cloud environments for the Packaging Suite, Corrugated Suite, and Paxis services are operated on AWS. These Infrastructure Providers are responsible for the operation of the underlying physical and environmental security controls supporting the hosted infrastructure.

EPS is responsible for designing, configuring, securing, and managing the application, platform, and supporting cloud architecture within these environments to ensure security, availability, and resiliency requirements are met. This includes the implementation of logical access controls, network security configurations, monitoring, backup management, and system hardening controls across Company-managed environments.

EPS also operates a set of centralized shared services within its AWS environment that provide common, integrated capabilities consumed across the Platform's products. These shared services include AI Translation (automated translation), Central eFlow (license provisioning and inter-product message brokering across cloud and hybrid deployments), and Genie (an AI-powered chatbot for in-product assistance).

The specific infrastructure services utilized to support the Platform include the following:

Service / Component	Description
Palo Alto Global Protect	Virtual private network (VPN) solution
Check Point	Firewall platform
Amazon EC2	Compute infrastructure supporting hosted workloads
Amazon RDS SQL Server	Relational database server
Amazon ECS / EKS	Managed container and Kubernetes services
Amazon ECR	Managed container registry
Amazon Route 53	Domain name system (DNS) service
AWS IAM / AWS SSO	Identity, access management, and federated authentication with MFA
Amazon CloudWatch	Infrastructure, application monitoring, logging, metrics, and alerting
AWS KMS	Cryptographic key management

Service / Component	Description
Amazon RDS / DynamoDB	Managed relational and NoSQL database services
AWS S3	Object storage service
AWS VPC	Logically isolated virtual network with public, private, and database subnets
AWS ALB / NLB	HTTP/HTTPS and TCP/UDP traffic distribution and load balancing
AWS Auto Scaling	Automatic scaling of compute resources based on demand
AWS Certificate Manager	SSL/TLS certificate management
AWS WAFv2	Web application firewall with centralized logging

AWS Secrets Manager	Secure credential and secrets storage
AWS CloudTrail	Centralized AWS API activity logging, audit trail monitoring
Amazon GuardDuty	Threat detection and security monitoring
AWS Organizations SCPs	Organization-wide governance controls for AWS accounts
Amazon Inspector	Automated internal and external vulnerability scanning
AWS Backup	Centralized backup management for AWS resources
AWS Systems Manager	Patch management, automation, and operational tooling
AWS Lambda	Serverless compute service
AWS Step Functions / Batch	Workflow orchestration and batch job processing

Software

Software consists of the programs and applications that support the Platform. The list of software and ancillary software used to build, support, secure, maintain, and monitor the Platform includes the following:

Application	Purpose
Microsoft 365	Email, file sharing, messaging, and collaboration tools
GitHub / GitHub Actions	Source code repository, CI/CD, and automated workflow management
GitHub Dependabot	Automated dependency scanning for vulnerable packages
HCP Packer	Automated build configurations and image management
Atlassian (Jira/Confluence)	Project management, issue tracking, and centralized notifications
Jenkins	Continuous integration and deployment automation
Mosyle	Apple mobile device management (MDM)
Application	**Purpose**
Qualys Patch Management	Patch management and vulnerability scanning
Sophos Advanced Endpoint Protection	Virus, malware, ransomware, and exploit protection for endpoints
Microsoft Defender	Threat detection and email security for Microsoft 365 environment
Zabbix	Infrastructure monitoring and alerting
Security Onion	Log management and security monitoring
OpenSearch / Grafana / Prometheus	Log analytics, monitoring dashboards, and metrics collection

Dashlane	Enterprise password manager
CloudKeeper (CK Prism)	AI-driven cloud cost optimization and governance for AWS
ConnectWise ScreenConnect	Remote access platform for customer environment support
Salesforce / HubSpot	Customer relationship management (CRM)
Selenium	Automated testing platform
WalkMe	Paxis user guidance platform
VMware / vCenter	Infrastructure virtualization and centralized VM management
OpenAI	Third-party AI service for Genie in-product assistant (data not used for training)
Google Cloud Translation	Third-party AI translation for AI Translation service (data not used for training)
ePS Infra Pilot	Internal AI-driven SRE agent for log analysis and incident support
AI Translation	Company-developed automated translation service integrated across Platform products
Central eFlow	Company-developed license provisioning and message brokering service
Genie	Company-developed AI-powered chatbot providing in-product assistance
GitHub Copilot	AI coding assistant
Anthropic Claude Code	AI coding assistant

People

EPS organizational structure provides the framework for the management, operation, and security of the Platform. The table below summarizes the key roles and functional responsibilities of ePS. Due to ePS size, one individual may serve multiple roles.

Role	Function
Executive Management	Responsible for oversight, implementation, and continual improvement of the Information Security Program; includes the CIO and leaders from Legal, Security, and PeopleOps.
CEO	Responsible for oversight of the development and performance of internal controls and the direction of company-wide activities.
CIO	Provides strategic leadership and oversight for information technology and security functions. The information security program operates under the CIO's direction, ensuring alignment with corporate objectives.

Information Technology (IT)	Responsible for managing and maintaining the organization's technology infrastructure, systems, and applications that support business operations and security objectives.
Security Team	Cross-functional team responsible for oversight, implementation, and continual improvement of the information security program.
Engineering	Responsible for the development, testing, deployment, and maintenance of the Platform and for maintaining security throughout the SDLC.
Human Resources	Responsible for managing the employee lifecycle, including recruitment, onboarding, training, performance management, and offboarding.
Business Operations	Manages internal business needs such as customer success and other administrative functions.
Legal	Responsible for compliance and legal functions of ePS, including external attorneys providing services under management supervision.

EPS leverages a remote workforce for the Platform's management, operation, and security with individuals worldwide. Certain individuals within ePS core team may be hired legally as independent contractors but are subject to identical controls as employees within the context of this system description; thus, both classes are defined as "personnel" throughout the report.

Procedures

Procedures are the specific actions undertaken to implement a process. EPS has adopted the following defined set of information security standards and policies (described as the information security program throughout the report). These policies are reviewed annually and approved by the CIO prior to publication. Policies include, but are not limited to:

- Access Control Policy
- AI Policy
- Antivirus & Endpoint Protection Policy
- Asset Management Policy
- Backup & Recovery Policy
- Bring Your Own Device (BYOD) Policy
- Business Continuity Policy & Plan
- Change Management Policy
- Clean Desk & Clear Screen Policy
- Data Classification Policy
- Code of Conduct
- Environmental, Social, and Governance Policy
- Data Deletion Policy
- Data Handling & Retention Policy
- Data Protection Policy
- Security Incident Response Plan (SIRP)
- Disaster Recovery Policy & Plan
- Encryption Policy
- Executive Management Charter
- Information Security & Privacy Risk Assessment Policy
- Information Security Awareness & Training Policy
- Information Security Policy
- Information Storage & Collaboration Policy
- ICT Acceptable Use Policy
- IT Account Management Policy
- Logging & Monitoring Policy
- Open-Source Software (OSS) Policy
- Password Policy
- Patch Management Policy
- Remote Access Software Policy
- Physical Security Policy
- Responsible Disclosure Policy
- Remote Access Policy
- Single Sign-On (SSO) Policy
- Remote Work Policy
- Third-Party Management Policy
- Risk Assessment & Risk Register Policy
- Vulnerability Management Policy
- Software Development Lifecycle Policy

- Endpoint Management & Security Policy

Data

Data refers to the transaction streams, files, databases, tables, and output processed, transmitted, or stored by ePS services. The following table summarizes the types of data used by the System:

Type	Description	Storage and Processing
Account data	PII and administrative data from personnel, customers, and third parties	AWS and third-party managed applications
Type	**Description**	**Storage and Processing**
Customer application data	Operational and manufacturing data processed across estimating, quoting, order and production management, inventory, scheduling, and analytics	AWS (Company-managed hosted); customer-controlled environments (self-hosted)
Secrets	Access credentials, tokens, certificates, API keys, and other secrets	AWS KMS, AWS Secrets Manager
Internal log information	Metadata and audit information relevant to services	OpenSearch, AWS CloudTrail, Amazon CloudWatch
AI-processed content	Content submitted to AI-enabled features for translation and in-product assistance	Processed via third-party AI services (OpenAI for Genie; Google Cloud Translation). Data is not used to train providers' models.

System Incidents

There were no identified significant system incidents that

a) Were the result of controls that were not suitably designed or operating effectively to achieve one or more of the service commitments and system requirements or
b) Otherwise, it resulted in a significant failure in the achievement of one or more of those service commitments and system requirements for the period November 6, 2025 to May 25, 2026.

Applicable Trust Services Criteria and Related Controls

The trust services criteria are classified into five categories: security, availability, processing integrity, confidentiality, and privacy. The trust services categories in scope for this report are as follows:

- ***Security:*** Information and systems are protected against unauthorized access, unauthorized disclosure of information, and damage to systems that could compromise the confidentiality of information or systems and affect the entity's ability to meet its objectives.
- ***Availability:*** Information and systems are available for operation and use to meet the entity's objectives.

- **Confidentiality:** Information designated as confidential is protected to meet the entity's objectives.

ePS has determined that the processing integrity and privacy trust services categories are not applicable to the system based on the nature of the services provided and the customer-controlled deployment models supported by ePS.

The common criteria are organized as follows: Control Environment; Communication and Information; Risk Assessment; Monitoring Activities; Control Activities; Logical and Physical Access Controls; System Operations; Change Management; and Risk Mitigation.

Control Environment

EPS control environment describes a set of standards, processes, and structures that provide the basis for carrying out internal control across the organization.

Integrity and Ethical Values

Integrity and ethical behavior are the products of ePS ethical and behavioral standards, communicated, monitored, and enforced in its business activities. EPS maintains a formal code of business conduct and ethics that is distributed to all personnel and acknowledged upon hire and annually thereafter. EPS standards of conduct outline its commitments to integrity and ethical values and include management's actions to remove or reduce incentives, pressures, and opportunities that might prompt personnel to engage in dishonest, illegal, or unethical acts. A whistleblower policy and confidential reporting hotline are maintained to allow personnel to report concerns without fear of retaliation.

Oversight Responsibility

EPS executive management team, operating under the leadership of the CIO who reports directly to the CEO, includes leaders from IT, Security, Legal, and Human Resources. This team provides oversight of organizational operations and internal controls to ensure effective governance, accountability, and alignment with ePS strategic objectives. Each quarter, the CIO meets with executive management to discuss the strategic direction of the organization and key initiatives to align the security program with business objectives. Quarterly compliance and security oversight meetings are documented and retained as evidence of governance.

Organizational Structure, Authority, and Responsibility

A formal organizational chart is maintained and made available to personnel to communicate key areas of authority, responsibility, and applicable lines of reporting. Management established the operating structure based on its size and the nature of its control environment, with reporting lines designed to establish key areas of authority and the proper flow of information. Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in the information security program. Job requirements and responsibilities are documented and communicated in formal job descriptions for all positions.

.

Commitment to Competence

Management demonstrates its commitment to competence through established policies and practices that attract, develop, and retain sufficient and competent individuals to support the achievement of objectives. EPS has implemented a security training program using KnowBe4, which is required to be completed for all personnel upon hire and renewed annually. The primary objective of the security training program is to educate personnel on their responsibility to protect the confidentiality, availability, and integrity of ePS information and includes periodic security updates, procedures for protection from malicious software, and password management. Background verification checks on personnel are performed prior to onboarding in accordance with relevant laws and regulations.

Accountability

EPS expects individuals to be held accountable for their internal control responsibilities in pursuing objectives. Individual performance is evaluated annually through a documented, formal performance review process. EPS has established a formal disciplinary process that describes disciplinary action to be applied against individuals who fail to comply with the security policies and procedures.

External Individuals

EPS commitment to integrity and ethical values extends to its use of contractors and vendors. Service providers who may impact the security of the production environment or have access to customer data are required to execute a non-disclosure agreement. EPS leverages the services of vendors generally accepted in the industry and reviews their public security commitments for consistency with ePS policies. EPS has a formal vendor management program that includes third-party risk assessments, review of vendor SOC 2 Type 2 reports where available, and written agreements including confidentiality and privacy commitments.

Communication and Information

EPS has established processes to identify information requirements and ensure appropriate internal and external sources of information are properly captured to support the functioning of other internal control components. Network architecture diagrams have been prepared and are shared with authorized individuals to communicate information about system operation and boundaries.

Internal Communication

EPS has a defined information security program that describes policies and procedures to guide personnel in achieving ePS security commitments and associated system requirements. Personnel are required to review and acknowledge the information security program and standards of conduct upon hire and re-certify annually. Management reinforces the information security program in meetings, internal communication, and during annual security training and awareness programs. Various weekly calls are held to discuss operational efficiencies and to disseminate new policies, procedures, controls, and strategic initiatives. All-hands meetings are held frequently to provide staff with updates on the firm and key issues. EPS makes available to personnel the processes for reporting system failures, incidents, concerns, and other complaints to appropriate personnel.

External Communication

EPS has prioritized maintaining open communication channels with external parties. Agreements are established with critical vendors and business partners that clearly define terms, conditions, and responsibilities. Security objectives and commitments are made available to customers through a dedicated security page and other information shared on ePS website (epssw.com). Customers are provided access to product documentation, certified release builds, and customer communication updates through the ePS community portal. Customers are also provided information on how to report systems failures, incidents, concerns, and other complaints to appropriate personnel. Product updates that impact user functionality or security are communicated to users directly via email or other methods.

Risk Assessment

EPS has a defined risk management program that includes guidance on the identification of potential threats, rating the significance of the risks associated with the threats, and mitigation strategies for those risks. EPS risk assessments are performed at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) to assets and service commitments are identified, and the risks are formally assessed using a qualitative risk assessment methodology that evaluates likelihood and impact.

EPS fraud risk assessment considers incentives, opportunities, and attitudes of management and other personnel to override controls and result in fraud or general misconduct and the specific fraud risks that arise from IT and access to information. Risk management discussions include a consideration of how changes in the environment impact risk, such as revisions to ePS business model, personnel turnover, and the implementation of new systems and technology. The security team meets monthly to prioritize and monitor mitigation strategies so the team can react to emerging risks.

Monitoring Activities

EPS selects, develops, and performs ongoing and, if necessary, separate evaluations to ascertain whether the components of internal control are present and functioning. The following describes the primary methods currently utilized by management:

- ***Penetration Testing:*** EPS engages third parties to conduct penetration tests of the production environment at least annually. Penetration tests are performed by a certified penetration tester to identify specific technical threats and vulnerabilities and to benchmark the environment against leading cybersecurity practices. Management reviews the results, and high-priority findings are tracked to resolution. During the review period, ePS completed penetration tests for the Packaging Suite, Corrugated Suite, and Paxis applications.
- ***Vulnerability Scanning:*** EPS performs routine vulnerability scanning of its production environment and managed workloads using Qualys to identify software vulnerabilities and unintended exposure. Findings are regularly reviewed by management and prioritized for remediation based on assessed risk.
- ***Code Security Scanning:*** EPS integrates security review throughout the development lifecycle. AI-automated code review is performed on every pull request, supplemented by mandatory peer review. As part of release certification, ePS performs static application security testing (SAST) and dynamic application security testing (DAST) to identify potential security flaws prior to deployment.
- ***Dependency Scanning:*** GitHub Dependabot is enabled to continuously scan for vulnerable dependencies. Updates identified are scored for compatibility, categorized by risk, and pull requests are automatically created for review.
- ***Patch Management:*** Qualys patch management continuously scans managed systems to identify missing security patches and software updates across ePS environment. The tool automates patch deployment for supported operating systems and applications, and patch compliance status is monitored through centralized dashboards.
- ***Endpoint Monitoring:*** Sophos advanced endpoint protection continuously monitors managed endpoints to detect, prevent, and respond to security threats such as malware, ransomware, and exploits. Security events and detections are visible through centralized dashboards, and alerts are generated for critical incidents.
- ***Threat Detection:*** Microsoft Defender and Amazon GuardDuty continuously assess managed endpoints and cloud infrastructure, providing real-time security alerts and recommendations. AWS CloudTrail logs are retained and monitored centrally for indicators of compromise.
- ***Access Logs:*** EPS maintains user access logs for privileged access and for access to user data, which are periodically reviewed by the CIO. Logical access to audit logs is restricted to authorized personnel, and system administrators are not permitted to erase or deactivate logs of their own activities.
- ***Internal Audit:*** EPS performs internal security and compliance reviews using Jira to track findings. Security and compliance activities are tracked in a dedicated Jira project (PACKSEC) monitored throughout the year.
- ***Third-Party Attestation:*** EPS conducts an annual third-party security and compliance review of key vendors. Results are reviewed by management and tracked for remediation where required.

Control Activities

Control activities are the actions established through policies and procedures that help ensure management's directives to mitigate risks to achieve objectives are carried out. As part of its annual risk assessment, management selects and develops control activities, including general control activities over technology, that contribute to the mitigation of risks to the achievement of objectives to acceptable levels. The information security program is reviewed by management annually and formally approved.

Logical and Physical Access Controls

EPS has established policies and procedures that define the access control requirements for requesting and provisioning user access to the system. Duties and access to sensitive resources are established based on the principle of least privilege. Logical access to systems is restricted through access control software and rule sets and is controlled by limited administrative users. Individuals require a unique username and are identified and authenticated before accessing information assets. Access to critical tools and resources requires multi-factor authentication (MFA).

EPS has established a formal onboarding and termination process. Appropriate management approval is obtained before granting access to critical tools and resources. New hire access provisioning requests are documented and tracked via Jira and email-based request workflows. System access reviews are performed monthly. Accounts for personnel who have been terminated or no longer require access are disabled within one business day.

Privileged access to critical tools and resources is highly restricted. Users with multiple access levels (e.g., administrators) are given separate accounts for normal system use and administrative functions. EPS systems can only be accessed by authorized personnel via an approved encrypted connection. Access to the production environment requires connection to a VPN (Palo Alto Global Protect), and access to servers is controlled through AWS systems manager session manager, which provides auditable, end-to-end encrypted sessions with logs retained in AWS S3.

EPS has implemented measures to secure personnel workstations, including session lock after a period of inactivity. Full-disk encryption is implemented for all personnel workstations and laptops. Personnel accessing critical tools and resources utilize laptops with the most recent operating system security updates and configured with antivirus software. Mobile device management is enforced using Mosyle for apple devices.

Management maintains a detailed inventory of all information systems, including AWS infrastructure components across multiple AWS accounts (Packaging Production, Corrugated Production, Paxis Production, and Central Shared Services). Information and data assets are subject to ePS policies and procedures for data protection, classification, and retention. For company-managed hosted environments, customer data is logically separated and not accessible to other tenants to prevent unauthorized access.

Secure data transmission protocols are used to encrypt confidential and sensitive data when transmitted over public networks utilizing TLS v1.2 or better. Encryption is used to protect data at rest utilizing 256-bit Advanced Encryption Standard (AES-256). SSL/TLS certificates are managed through AWS Certificate Manager, with Route 53 used for DNS management. AWS KMS is used for cryptographic key management.

EPS uses AWS WAFv2 configured to protect applications and APIs against common web exploits, including those identified in the OWASP Top 10. Security rules are periodically reviewed and updated as new threats emerge. Firewall rules are reviewed on an annual basis. Physical security of ePS India office is enforced through an access control system, CCTV surveillance, visitor registration, fire extinguishers with regular inspection, and UPS/generator backup systems with active maintenance contracts.

System Operations

EPS has established baseline configuration standards and uses tools to detect and restore configuration deviations from the standards. Production workloads are built from hardened, baseline-configured images managed in a controlled registry, and container images are subject to vulnerability scanning prior to deployment. Production instances are monitored for viruses, malware, and other threats using Amazon GuardDuty. Identified security deficiencies are tracked and prioritized through internal tools according to their severity.

Applicable security patches are applied immediately or during a scheduled release to the environment based on the severity of the vulnerability. Formal procedures are defined for security event detection and management. EPS uses a system that collects and stores logs in a central location (OpenSearch and AWS CloudTrail). Activity logs and other data sources are analyzed by continuous monitoring tools to identify unusual system activities and filter, summarize, and analyze anomalies to identify security events.

EPS has established plans for incident response that outline management responsibilities and procedures to respond to information security incidents. Security events are quantified, monitored, and tracked by an identified incident response team. Post-mortem meetings are conducted for security incidents to discuss root causes, remediation steps, and lessons learned. During the review period, ePS responded to security-related incidents including a supply chain security alert involving an npm package (Axios), and a security scorecard rating review requested by a client.

EPS has established defined availability and recovery commitments for its company-managed hosted environments, including a minimum availability SLA of 99.9%, a Recovery Point Objective (RPO) of four hours, and a Recovery Time Objective (RTO) of eight hours. Database backups are configured to run automatically and are retained on a rolling 30-day basis, executed in alignment with the four-hour RPO. AWS RDS and Aurora automated backup configurations are in place across all production accounts. Backup integrity is validated periodically through automated restoration tests using AWS Lambda functions. Processing capacity and usage are monitored on an automated, real-time basis. Load balancers are used to distribute incoming application traffic across compute resources, and scaling is configured to adjust capacity based on demand.

Business and system recovery plans are documented, providing the roles, responsibilities, and detailed procedures for the recovery of systems. EPS plans for business continuity, disaster recovery, and incident response are reviewed, tested, and updated on an annual basis. A BCP/DR tabletop exercise was conducted during the review period to validate recovery procedures and identify areas for improvement.

Change Management

EPS has established policies and procedures for secure software development to ensure information security is designed and implemented within the development lifecycle for applications and information systems. The change management processes and procedures have been established to plan, schedule, apply, distribute, and track changes to the production environment to minimize risk and client impact.

EPS uses GitHub as its version control system to manage source code, documentation, release labeling, and other change management tasks. Software developers are expected to adhere to ePS coding standards throughout the development cycle, including standards for quality, commenting, and security. Releases are tested throughout the development process and validated prior to deployment. Testing is performed in an isolated environment that is separate from production workloads.

Code changes include a formal code review process. AI-automated code review is performed on every pull request, supplemented by mandatory peer review requiring approval from one or two qualified engineers depending on the nature and risk of the change. Branch protection rules are enforced in GitHub to prevent unauthorized merges to protected branches. Only experienced engineers with experience in code review techniques and secure coding practices can approve a code change. As part of release certification, static application security testing (SAST) and dynamic application security testing (DAST) are performed prior to deployment. Access to deploy changes to production is restricted to authorized individuals with a business need. Changes are tracked through Jira with documented workflows.

Risk Mitigation

EPS implements risk mitigation strategies to prioritize, evaluate, and implement the appropriate risk-reducing controls. Strategies for risk mitigation activities are based on an assessment of risk and a formal business impact analysis used to evaluate the criticality of each application, service, and data set to drive business continuity requirements. Management has identified potential business disruptions as a critical risk to meeting its objectives and has established plans for business continuity, disaster recovery, and incident response to respond to, mitigate, and recover from events that could disrupt business operations. Cybersecurity insurance is maintained to mitigate the financial impact of business disruptions.

As part of its risk mitigation strategies, management assesses and manages risks associated with vendors and business partners. Periodically, generally annually, management assesses the risks that vendors and business partners represent to the achievement of ePS objectives. The vendor management process includes maintaining an inventory of third-party vendors, categorization of vendor risks based on access levels and criticality to services provided, and a review of vendor security requirements. Based on the risk assessment, management obtains due diligence and compliance information, such as SOC 2 Type 2 reports, during the vendor acceptance and re-review process. EPS has written agreements in place with vendors and business partners that include confidentiality and privacy commitments consistent with the commitments and requirements of ePS.

User Entity Controls and Responsibilities

EPS services are designed utilizing a shared responsibility model where maintaining the security of a customer's information is dependent upon the customer implementing controls that are outside ePS control. CUECs are not required or significant to achieve the service commitments and system requirements based on the applicable trust services criteria. User entity responsibilities that should be implemented to allow the customer to benefit from the

use of the Platform include the following:

- Ensuring the confidentiality of user accounts and passwords.
- Notifying ePS promptly when changes are made to technical, billing, or administrative contact information.
- Developing internal disaster recovery and business continuity plans that address the inability to access or utilize ePS services.
- Notifying ePS and providing accurate information regarding new, terminated, and changes necessary to user accounts.
- Informing ePS of any regulatory issues that may affect the services provided.
- Understanding and complying with contractual obligations to ePS.
- Immediately notifying ePS of any actual or suspected information security breaches involving the Platform, including compromised user accounts.
- Granting access only to authorized and trained personnel.
- Deploying physical security and environmental controls for all devices and access points used to access ePS services.

Subservice Organization Controls

When controls at a vendor are necessary in combination with ePS controls to provide reasonable assurance that ePS service commitments and system requirements are achieved, the vendor is considered a subservice organization. Management has identified the below subservice organizations and has elected to use the carve-out method for the purposes of this report:

Subservice Organization	Description
ASK4 and Expedient	Data center colocation services
Amazon Web Services (AWS)	Cloud hosting services

EPS has implemented procedures for the oversight and monitoring of the services provided by the subservice organizations, which are outlined in the vendor management policies and procedures. EPS evaluates risks related to the Infrastructure Providers and reviews current SOC 2 Type 2 reports or other procedures as deemed necessary.

The following are the applicable trust services criteria and controls that are necessary to be in place at the subservice organizations to provide reasonable assurance that ePS service commitments and system requirements were achieved:

Trust Services Criteria	Complementary Subservice Organization Control
Logical and Physical Access	Procedures are implemented to authenticate authorized users, restrict physical and logical access, and detect unauthorized access attempts. Procedures are implemented to decommission and physically destroy production assets securely. Security measures are implemented to provision and deprovision user access to systems and applications based on appropriate authorization, and encryption has been implemented, by default or as configured by

	ePS, to secure the transmission and storage of information.

Trust Services Criteria	Complementary Subservice Organization Control
System Operations	Vulnerability scans and penetration testing are performed periodically to identify system vulnerabilities, and environmental protection, monitoring, and procedures for regular maintenance are implemented at the data center facilities. Incident response procedures are established and implemented to identify, analyze, and remediate events and incidents.
Change Management	Procedures are established and implemented to ensure system changes are authorized, designed, developed, configured, documented, tested, and approved before production deployment.
Availability	Monitoring tools are implemented to monitor and manage the capacity and availability of hosting infrastructure. Environmental protections, data backup processes, and recovery mechanisms have been implemented and appropriately tested to adequately address availability requirements.

Significant Changes to the System

Other than as described below, there have been no changes that are likely to affect report users' understanding of how the Platform is used to provide services for the period November 6, 2025 to May 25, 2026. During the period, ePS expanded its company-managed hosted cloud offering on AWS for the Packaging Suite, Corrugated Suite, and Paxis services, and introduced centralized shared services hosted within ePS AWS environment that provide common, integrated capabilities across the Platform's products (AI Translation, Central eFlow, and Genie).

Trust Services Criteria Relevance

All security, availability, and confidentiality trust services criteria as set forth in TSP 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy were relevant to the Platform as presented in this report.

Use of Report

The description does not omit or distort information relevant to the Platform while acknowledging that the description is prepared to meet the common needs of a broad range of users and may not, therefore, include every aspect of the system that each user may consider important to their own particular needs.

PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

Overview

ePS makes service commitments to its customers and has established system requirements as part of the ePS Packaging Platform. ePS 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 ePS service commitments and system requirements are achieved.

The principal service commitments are communicated via customer contracts, service level agreements, description of service offerings provided on ePS website, and the information security program. ePS has made commitments to customers with respect to service level objectives, security of customer data, and system availability. These commitments are addressed through measures including encryption, multi-factor authentication, physical security, vulnerability management, continuous monitoring, and other relevant security controls.

Service Commitments

Category	Commitment	How Addressed
Security	Commercially reasonable safeguards to secure data from accidental loss and unauthorized access	Information security program, MFA, encryption, access controls, endpoint protection, and continuous monitoring
Security	Logical tenant separation for hosted environments	AWS VPC isolation, logical access controls, and customer data segregation in hosted environments
Security	Encryption in transit using TLS 1.2 or greater	AWS certificate manager, ALB SSL/TLS termination, and Route 53 DNS management
Security	Encryption at rest using AES-256	AWS KMS key management and RDS/S3 encryption at rest
Security	Multi-factor authentication for critical resources	AWS SSO / IAM identity center with MFA enforcement, Palo Alto GlobalProtect VPN with MFA
Security	Annual vulnerability scanning and penetration testing	Qualys vulnerability scanning, annual third-party penetration testing of Packaging Suite, Corrugated Suite, and Paxis
Availability	99.9% uptime SLA for Company-managed hosted environments	AWS high-availability architecture, load balancing, auto-scaling, and CloudWatch monitoring
Availability	RPO of four hours and RTO of eight hours	Automated AWS RDS database backups on 30-day retention, Lambda-based restore testing

Category	Commitment	How Addressed
Availability	Continuous monitoring from internal and external points	Zabbix, Grafana, Prometheus, CloudWatch, and GuardDuty monitoring
Confidentiality	Data classification and protection policies	Data Classification Policy, Data Handling & Retention Policy, and Data Deletion Policy
Confidentiality	Access restricted to authorized personnel on need-to-know basis	Role-based access controls, monthly access reviews, and privileged access management via AWS SSM

System Requirements

ePS management establishes operational requirements that support the achievement of service commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated through ePS system policies and procedures, system design documentation, and contracts with customers. The information security program defines an organization-wide approach to protecting systems and data, including descriptions and expectations for the system's design, development, and operation.

EPS system requirements include:

- Maintaining and enforcing policies and procedures that govern the operation, security, and availability of the Platform.
- Implementing and maintaining access controls consistent with the principle of least privilege and role-based access management.
- Performing risk assessments at least annually to identify, assess, and mitigate information security risks.
- Ensuring the availability of the Platform at a minimum availability SLA of 99.9% and meeting RPO and RTO commitments for hosted environments.
- Maintaining encryption of customer data in transit (TLS 1.2+) and at rest (AES-256) for hosted environments.
- Performing background verification checks for all personnel prior to granting access to the Platform.
- Ensuring security training is completed by all personnel upon hire and annually thereafter.
- Reviewing and updating the information security program at least annually with CIO approval.
- Performing annual penetration testing and routine vulnerability scanning of the production environment.
- Maintaining a formal incident response process and documented business continuity and disaster recovery plans.
- Monitoring and managing third-party vendor risks on an annual basis or more frequently as changes occur.

System Description

eProductivity Software LLC ("ePS") provides the ePS Packaging Platform, a suite of Enterprise Resource Planning (ERP) and Manufacturing Execution System (MES) solutions purpose-built for the packaging and corrugated industries, comprising the Packaging Suite, Corrugated Suite, Metrics, and Paxis services and serving label, folding carton, flexible packaging, and commercial print manufacturers.

The platform supports multi-company, multi-plant, multi-currency, and multi-language deployments, enabling enterprise-wide operations across geographically distributed facilities.

Radius encompasses modules for estimating, job management, production planning, shop floor data collection, inventory and warehouse management, purchasing, financial accounting, and reporting. ePS maintains a comprehensive, versioned documentation library covering system setup, user administration, operational procedures, and upgrade processes, accessible to authorized personnel through ePS's documentation portal.

Security

- ***Logical Access Controls:*** ePS has designed the Platform with application-level logical access controls that restrict user access based on assigned roles and responsibilities. User accounts are individually provisioned, and access to system functions is limited to those relevant to each user's role. Controls are in place to manage access for personnel whose job functions involve shop floor operations, separating those accounts from administrative and financial functions within the system.
- ***Segregation of Duties:*** The Platform incorporates workflow-based authorization controls that route transactions, including purchasing and production activities, to appropriate personnel for review and approval, supporting segregation between transaction initiators and approvers.
- ***Audit Trail***: The Platform includes a database auditing capability that provides logging of data changes, supporting detection and investigation of unauthorized modifications.

Availability

ePS designs the Platform to support deployment in multi-site, multi-company environments with configurable time zone support, enabling continuous operations across distributed facilities. ePS publishes formal upgrade and patch management documentation to guide customers in applying software updates in a controlled manner, reducing the risk of unplanned downtime associated with software maintenance activities.

Confidentiality

Access to sensitive data, including financial information, pricing, and procurement terms, is restricted through the Platform's role-based access controls. Multi-company deployments maintain logical separation between organizational entities, ensuring that users authorized for one entity cannot access data belonging to another. ePS's documented procedures and access control framework support the protection of confidential customer and operational information within the system.

SECTION : IV

APPENDIX

APPENDIX A

GLOSSARY

Applicable Trust Services Criteria

The criteria codified in TSP section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA Trust Services Criteria), used to evaluate controls relevant to the trust services categories included within the scope of a particular examination.

Authentication

The process of verifying the identity or other attributes claimed by or assumed of an entity (user, process, or device), or to verify the source and integrity of data.

Authorization

The process of granting access privileges to a user, program, or process by a person who has the authority to grant such access.

Boundaries of the System

The specific aspects of a service organization's infrastructure, software, people, procedures, and data are necessary to provide its services. Systems for multiple services may share aspects, but the boundaries of each system will differ.

Carve-Out Method

Method of addressing the services provided by a subservice organization in which the components of the subservice organization's system are excluded from the description of the service organization's system and from the scope of the examination.

Complementary Subservice Organization Controls (CSOCs)

Controls that service organization management assumed, in the design of the service organization's system, would be implemented by the subservice organization and that are necessary, in combination with controls at the service organization, to provide reasonable assurance that the service commitments and system requirements are achieved.

Commitments

Declarations made by management to customers regarding the performance of one or more systems that provide services or products. Commitments can be communicated in written individualized agreements, standardized contracts, service level agreements, or published statements.

Criteria

The benchmarks are used to measure or evaluate subject matter.

Encryption
The process of transforming data into an unreadable format using a cryptographic algorithm and key, to protect the confidentiality and integrity of information.

Internal Control
A process, effected by an entity's board of directors, management, and other personnel, designed to provide reasonable assurance regarding the achievement of objectives relating to operations, reporting, and compliance.

Multi-Factor Authentication (MFA)
An authentication method in which a user is granted access only after successfully presenting two or more pieces of evidence (factors) to an authentication mechanism.

Personal Information
Information that is or can be about or related to an identifiable individual.

Policies
Management or board member statements of what should be done to effect control. Such statements may be documented, explicitly stated in communications, or implied through actions and decisions. Policies serve as the basis for procedures.

Recovery Point Objective (RPO)
The maximum acceptable amount of data loss measured in time, defining how far back in time data can be recovered in the event of a system failure or disaster.

Recovery Time Objective (RTO)
The maximum acceptable length of time that a system can be offline following a failure or disaster before the business is significantly impacted.

Risk
The possibility that an event will occur adversely affect the achievement of objectives.

Security Incident
A security event that requires action on the part of an entity in order to protect information assets and resources.

SOC 3 Engagement
An examination engagement to report on management's assertion about whether controls within the system were effective to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the trust services criteria relevant to one or more of the trust services categories.

Subservice Organization
A vendor used by a service organization that performs controls that are necessary, in combination with controls at the service organization, to provide reasonable assurance that the service organization's service commitments and system requirements were achieved.

System
The infrastructure, software, people, processes, and data that are designed, implemented, and operated to work together to achieve one or more specific business objectives in accordance with management-specified requirements.

System Components
The individual elements of a system, classified into the following five categories: infrastructure, software, people, processes, and data.

System Requirements
Specifications about how the system should function to (a) meet the service organization's service commitments to user entities; (b) meet commitments to vendors and business partners; (c) comply with relevant laws and regulations; and (d) achieve other objectives relevant to the trust services categories addressed by the description.

Unauthorized Access
Access to information or system components that (a) has not been approved by a person designated to do so by management and (b) compromises segregation of duties, confidentiality commitments, or otherwise increases risks beyond levels approved by management.

User Entity
An entity that uses the services provided by a service organization.

Vendor
An individual or business engaged to provide services to the service organization. Depending on the services provided, a vendor might also be a subservice organization.

APPENDIX B

ABBREVIATIONS

Abbreviation	Expanded Form
AES	Advanced Encryption Standard
AICPA	American Institute of Certified Public Accountants
ALB	Application Load Balancer
API	Application Programming Interface
AWS	Amazon Web Services
BCP	Business Continuity Plan
CEO	Chief Executive Officer
CIO	Chief Information Officer
CI/CD	Continuous Integration / Continuous Deployment
CPA	Certified Public Accountant
CRM	Customer Relationship Management
CSOC	Complementary Subservice Organization Control
CUEC	Complementary User Entity Control
DAST	Dynamic Application Security Testing
DNS	Domain Name System
DR	Disaster Recovery
EC2	Elastic Compute Cloud (AWS)
ECS	Elastic Container Service (AWS)
ECR	Elastic Container Registry (AWS)
EKS	Elastic Kubernetes Service (AWS)
eMAS	ePS Managed Application Services
ePS	eProductivity Software
ERP	Enterprise Resource Planning
IAM	Identity and Access Management
IT	Information Technology

Abbreviation	Expanded Form
KMS	Key Management Service (AWS)
LLC	Limited Liability Company
MDM	Mobile Device Management
MES	Manufacturing Execution System
MFA	Multi-Factor Authentication
NDA	Non-Disclosure Agreement
NLB	Network Load Balancer
OWASP	Open Web Application Security Project
RDS	Relational Database Service (AWS)
RPO	Recovery Point Objective
RTO	Recovery Time Objective
S3	Simple Storage Service (AWS)
SAST	Static Application Security Testing
SDLC	Secure Software Development Lifecycle
SIRP	Security Incident Response Plan
SLA	Service Level Agreement
SNS	Simple Notification Service (AWS)
SOC	System and Organization Controls
SOC 2	System and Organization Controls 2 (detailed report with tests)
SOC 3	System and Organization Controls 3 (public general use report)
SQS	Simple Queue Service (AWS)
SRE	Site Reliability Engineering
SSL	Secure Sockets Layer
SSM	Systems Manager (AWS)
SSO	Single Sign-On
TLS	Transport Layer Security
TSP	Trust Services Principles
VPC	Virtual Private Cloud (AWS)
VPN	Virtual Private Network
WAF	Web Application Firewall

------End of the Report------