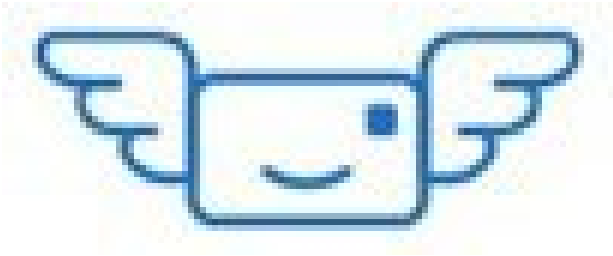

SYSTEM AND ORGANIZATION CONTROLS (SOC) 3 REPORT ON MANAGEMENT'S ASSERTION RELATED TO ITS

VPM Platform

Relevant to Security

For the period January 1, 2025 to December 31, 2025

TOGETHER WITH INDEPENDENT AUDITORS' REPORT

Prepared by:

Sensiba

Table of Contents

1. Independent Service Auditors' Report

To the Management of Virtual Post Solutions, Inc. (VPM)

Scope

We have examined VPM's accompanying assertion titled "Assertion of VPM Management" (assertion) that the controls within Virtual Post Solutions, Inc's VPM Platform (system) were effective throughout the period January 1, 2025 to December 31, 2025, to provide reasonable assurance that VPM's service commitments and system requirements were achieved based on the trust services criteria relevant to Security (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus — 2022)* in AICPA*, Trust Services Criteria.*

Service Organization's Responsibilities

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

Service Auditors' 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 attestation standards established by the AICPA. 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 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 VPM's 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 VPM's service commitments and system requirements based on the applicable trust services criteria.

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 engagement.

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 Virtual Post Solutions, Inc's VPM Platform were effective throughout the period January 1, 2025 to December 31, 2025, to provide reasonable assurance that VPM's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

San Jose, California
February 12, 2026

2. Assertion of VPM Management

We are responsible for designing, implementing, operating, and maintaining effective controls within the Virtual Post Solutions, Inc. (VPM) VPM Platform (system) throughout the period January 1, 2025 to December 31, 2025, to provide reasonable assurance that VPM's service commitments and system requirements relevant to Security were achieved. Our description of the boundaries of the system is presented in the section of this report titled, "Description of Virtual Post Solutions, Inc's VPM Platform ," (description) and identifies the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period January 1, 2025 to December 31, 2025, to provide reasonable assurance that VPM's service commitments and system requirements were achieved based on the trust services criteria relevant to Security (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus - 2022)* in AICPA*, Trust Services Criteria.*

VPM'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 the accompanying system description.

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 January 1, 2025 to December 31, 2025, to provide reasonable assurance that VPM's service commitments and system requirements were achieved based on the applicable trust services criteria.

Signed by Virtual Post Solutions, Inc. Management

February 12, 2026

3. Description of Virtual Post Solutions, Inc's VPM Platform

Company Background

Virtual Post Solutions, Inc. was founded in 2009 with the mission to allow people to access their postal mail remotely. Since then, VPM has expanded into 5 states – California, Nevada, Delaware, Florida, and Texas.

The mission has shifted since then to encompass a broader scope – to help individuals and businesses go 100% remote through a platform of services that allows customers to become location-independent.

Services Provided

VPM's primary core service is in offering different types of addresses for receiving mail, processing mail, scanning mail content, forwarding mail, and depositing check payments.

Additionally, VPM also provides registered agent service for corporate compliance.

VPM's platform is a multiuser software-as-a-service application that helps customers access and manage their postal mail online. Mail envelopes are scanned into the user's "online mailbox". The user can then decide to have the mail contents scanned, forwarded to another address, or trashed. If mail contains check payments, users can also request to have checks sent to their banks for deposit through the banks' mail-in deposit service.

Information is shared with users through email, secured support tools, and secured websites.

Principal Service Commitments and System Requirements

VPM designs its systems, procedures, and workflows to provide customers with service that meets the service commitments VPM makes to its customers, relevant laws and regulations that govern the provision of VPM services, and the financial, operational, and compliance requirements that VPM has established for the services. VPM operates in multiple States within the United States and is subject to the security and privacy requirements of both the U.S. and the States it operates in.

Security commitments to customers are documented and communicated in customer agreements as well as in the service descriptions provided on the VPM website. Security commitments are standardized and include, but not limited to:

All physical processing centers that store and process mail are secured using access control, security alarm, and 24/7 surveillance systems.

Use of encryption technologies to protect customer data both at rest and in transit.

All physical mail is shredded on-site using industrial mobile shredding services that provide document destruction certificates.

VPM establishes operational requirements that support the achievement of security commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in VPM's system policies and procedures, system design documentation, and contracts with customers. Information security policies define an organization-wide approach to how systems and data are protected. These include policies around how the service is designed and developed, how the system is operated, how the internal business systems and networks are managed and how employees are hired and trained.

In addition to these policies, standard operating procedures have been documented on how to carry out specific manual and automated processes required in the operation of the VPM platform.

Components of the System

Infrastructure

Primary Infrastructure		
Hardware	Type	Purpose
AWS	Config, WAF, GuardDuty	Network and web application firewall, threat detection, configuration change monitoring
AWS	Various services, including VPC, IAM, Lambda, CloudWatch, CloudFront	Primary infrastructure that manages application hosting, security, monitoring, notifications, and logging.
AWS	RDS and S3	Data storage
Google workspace	Google drive	Customer contracts, legal processing, temporary mail envelope image archiving

Software

Primary Software	
Software	Purpose
AWS	Cloud infrastructure hosting and security monitoring.
Google Workspace	Employee account management and organizational data.
HelpScout	Customer support
Endicia	Shipment labels
Asana	Issue reporting and tracking; task and project management
Slack	Internal communication
MongoDB	Database

People

VPM has a staff organized in the following functions areas:

- Corporate. Executives, senior operations staff, and company administrative support staff, such as legal, compliance, internal audit, training, contracting, accounting, finance, human resources. These individuals handle people related matters to ensure that people are performing at their best and with the utmost integrity through quality assurance monitoring, coaching, training, and other support to ensure the well-being of individuals.
- Operations - Manages day-to-day operations.
  - Operations staff handles mail processing, including mail induction, mail content scanning, shipping, check deposit processing, purging and destruction of mail, and other activities that require physical handling of mail.
  - Customer Support handles sales questions and customer issues and requests that cannot be handled through the platform.
  - Property managers manage the physical properties and maintain building security and safety for staff and customer mail. They also coordinate with address partners for proper mail delivery.
- IT
  - The help desk group provides technical assistance to users.
  - Systems admin typically has no direct use of the VPM platform. Rather, it supports VPM's IT infrastructure, which is used by the software. A systems admin will deploy releases of the VPM Platform and other software into the production environment.
  - The software development staff develops and maintains the software developed by VPM. This includes the VPM Platform, supporting utilities, and the external websites that interact with the VPM Platform. The staff includes software developers, database administration, software quality assurance.
  - The information security staff supports the VPM Platform indirectly by monitoring internal and external security threats and maintaining current antivirus software.
  - The information security staff maintains the inventory of IT assets.

Processes, Policies and Procedures

Formal IT policies and procedures exist that describe physical security, logical access, computer operations, change control, and data communication standards. All teams are expected to adhere to the VPM policies and procedures that define how services should be delivered. These are located on the Company's intranet and can be accessed by any VPM team member.

Physical Security

All systems are hosted by AWS. Physical and environmental security of the system is the responsibility of AWS. AWS does not allow Virtual Post Solutions staff on the data center floor.

All VPM processing centers are wholly operated by VPM to allow better management and control of security. Contractors are not granted access to VPM processing centers.

Upon an employee's termination of employment, HR generates an employee termination checklist of tasks to perform for removal of employee access. All tasks and subtasks are tracked for completion by HR.

Logical Access

VPM uses role-based and account-based security architecture to define user accounts and access to allowed resources. Users need to login before it can access any system resources. MFA is required on all accounts.
Separate AWS accounts are used for different environments. For example, development and productions reside in different AWS accounts. AWS IAM is then used to define who has access to specific accounts. Additionally, users must assume a role in any AWS account that allows specific access based on the assumed role.

All employee devices are managed through a Mobile Device Management system and can be controlled, updated, and disabled remotely.

Employees and approved vendor personnel sign on to cloud resources using Google Workspace for Single Sign-On (SSO). Users are also required to separately sign on to any systems or applications that do not implement Google SSO using passwords that conform to VPM's security policies.

Employee's Google Workspace account is created 1-2 days before the employee's start date. IT provides access to organizational level resources. Employee manager further defines any additional access required by the new hire.

All new hires must complete the security onboarding process within 10 working days.

Employee accounts are suspended and access to all applications and services revoked after termination as part of the off-boarding process.
User accounts and access rules are checked quarterly.

Computer Operations – Backups

All customer mail data files are stored on AWS S3 and versioned.

All customer data is backed up continuously through AWS RDS Aurora's point-in-time restore mechanism along with daily snapshots taken. Database and its associated backups are encrypted using KMS-managed encryption keys.

Computer Operations – Availability

Incident response policies and procedures are in place to guide personnel in reporting and responding to information technology incidents. Procedures exist to identify, report, and act upon system security breaches and other incidents. Incident response procedures are in place to identify and respond to incidents on the network.

AWS CloudWatch is used to monitor the production environment and send out automatic alerts and notifications as well as perform certain remediations automatically.

VPM monitors the capacity utilization of physical and computing infrastructure both internally such as database load, server cluster utilization, and data storage limits.

Reaching defined thresholds will automatically trigger scaling up/down resources, such as increasing the number of application instances to handle additional load.

VPM uses Systems Manager to perform automatic updates to servers. In addition, servers are normally replaced with new launched instances instead of patching an existing server to help ensure that all servers start from a clean slate.

Change Control

VPM maintains documented Systems Development Life Cycle (SDLC) policies and procedures to guide personnel in documenting and implementing application and infrastructure changes. Change control procedures include change request and initiation processes, documentation requirements, development practices, quality assurance testing requirements, and required approval procedures.

Applications are tracked via project management software and GitHub project repositories. All changes are tracked in Asana tasks, GitHub issues and GitHub pull requests.

A ticketing system is used to document the change control procedures for changes in the application and implementation of new changes. Unit tests are executed using Continuous Integration (CI) as part of the build process. Quality assurance testing and User Acceptance Testing (UAT) results are documented and maintained with the associated change request. Development and testing are performed in an environment that is logically separated from the production environment. Management approves changes prior to migration to the production environment and documents those approvals within the ticketing system.

Version control software is utilized to maintain source code versions and push source code through the development process to the production environment. The version control software maintains a history of code changes to track all code changes and support rollback capabilities.

Data Communications

Firewall systems are in place to filter unauthorized inbound network traffic from the Internet and deny any type of network connection that is not explicitly authorized. Network address translation (NAT) functionality is utilized to manage internal IP addresses. Administrative access to the firewall is restricted to authorized employees.

Penetration testing is conducted annually to measure the security posture of a target system or environment. The third-party vendor uses an accepted industry standard penetration testing methodology.

The third-party vendor’s approach begins with a vulnerability analysis of the target system to determine what vulnerabilities exist on the system that can be exploited via a penetration test, simulating a disgruntled/disaffected insider or an attacker that has obtained internal access to the network.

Once vulnerabilities are identified, the third-party vendor attempts to exploit the vulnerabilities to determine whether unauthorized access or other malicious activity is possible. Penetration testing includes network and application layer testing as well as testing of controls and processes around the networks and applications and occurs from outside the network.

Vulnerability scanning is performed by a third-party vendor on a quarterly basis in accordance with VPM policy. The third-party vendor uses industry standard scanning technologies and a formal methodology specified by VPM.

These technologies are customized to test the organization's infrastructure and software in an efficient manner while minimizing the potential risks associated with active scanning. Retests and on-demand scans are performed on an as needed basis.
Remote access is approved on a per-application basis for each user. Traffic is encrypted in transit and IP whitelisting is used to control access.

Boundaries of the System

The scope of this report includes the Services performed by Virtual Post Solutions. This report does not include the data center hosting services provided by AWS.

The applicable trust services criteria and the related controls:

The Trust Services Categories that are in scope for the purposes of 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 availability or confidentiality of information or systems and affect the entity's ability to meet its objectives.

Control Environment

Integrity and Ethical Values

Strong morals matter more than fancy rules. Even the best regulations can't work if the people in charge (making, using, and checking them) aren't honest and ethical. VPM's overall control system is built on this idea, meaning it's crucial for people to act with integrity. This comes from VPM's clear rules on right and wrong, how everyone learns about them, and how they're encouraged to follow them. This includes removing situations that might make people cheat or break the rules, and also clearly explaining VPM's values and expectations to everyone, both in writing and through how people act.

Specific control activities that the service organization has implemented in this area are described below:

- Formally, documented organizational policy statements and codes of conduct communicate entity values and behavioral standards to personnel.
- Policies and procedures require employees sign an acknowledgment form indicating they have been given access to the employee manual and understand their responsibility for adhering to the policies and procedures contained within the manual.
- A confidentiality statement agreeing not to disclose proprietary or confidential information, including client information, to unauthorized parties is a component of the employee handbook.
- Background checks are performed for employees as a component of the hiring process.

Commitment to Competence

VPM 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 consideration of the competence levels for particular jobs and how those levels translate into the requisite skills and knowledge.
Specific control activities that VPM has implemented in this area are described below:

- Management has considered the competence levels for particular jobs and translated required skills and knowledge levels into written position requirements.
- Training is provided to maintain the skill level of personnel in certain positions.
- Performance goals are set and measured for specific teams and individuals to achieve and maintain.

Management's Philosophy and Operating Style

VPM's management philosophy and operating style encompass a broad range of characteristics. Such characteristics include management's approach to taking and monitoring business risks, continuous improvement attitude, and management's attitudes toward information processing, accounting functions, and personnel.

Specific control activities that the service organization has implemented in this area are described below:

- Management meetings are held to discuss strategic initiatives, progress and challenges across all major teams that affect the business as a whole.
- Staff is encouraged to submit suggestions on how to improve the process and people's well-being through an online suggestion box system.
- Special task force team formed to educate, enforce, and reward people who are living the company values.

Organizational Structure and Assignment of Authority and Responsibility

VPM's organizational structure provides the framework within which its activities for achieving entity-wide objectives are planned, executed, controlled, and monitored. Management believes establishing a relevant organizational structure includes considering key areas of authority and responsibility. An organizational structure has been developed to suit its needs. This organizational structure is based, in part, on its size and the nature of its activities.

VPM's assignment of authority and responsibility activities include factors such as how authority and responsibility for operating activities are assigned and how reporting relationships and authorization hierarchies are established. It also includes policies relating to appropriate business practices, knowledge, and experience of key personnel, and resources provided for carrying out duties. In addition, it includes policies and communications directed at ensuring personnel understand the entity's objectives, know how their individual actions interrelate and contribute to those objectives, and recognize how and for what they will be held accountable.

Specific control activities that the service organization has implemented in this area are described below:

- Organizational charts are in place to communicate key areas of authority and responsibility.
- Organizational charts are available and communicated to employees and updated as needed.

Human Resource Policies and Practices

VPM's success is founded on sound business ethics, reinforced with a high level of efficiency, integrity, and ethical standards. The result of this success is evidenced by its proven track record for hiring and retaining top quality personnel who ensures the service organization is operating at maximum efficiency. VPM's human resources policies and practices relate to employee hiring, orientation, training, evaluation, counseling, promotion, compensation, and disciplinary activities.

Specific control activities that the service organization has implemented in this area are described below:

- New employees are required to sign acknowledgement forms for the employee handbook and a confidentiality agreement following new hire orientation on their first day of employment.
- Evaluations for each employee are performed on a quarterly or more frequent basis.
- Employee termination procedures are in place to guide the termination process and are documented in a termination checklist.

Risk Assessment Process

VPM's risk assessment process identifies and manages risks that could potentially affect VPM's ability to provide reliable services to user organizations. This ongoing process requires that management identify significant risks inherent in products or services as they oversee their areas of responsibility. VPM identifies the underlying sources of risk, measures the impact to organization, establishes acceptable risk tolerance levels, and implements appropriate measures to monitor and manage the risks.

This process has identified risks resulting from the nature of the services provided by VPM, and management has implemented various measures designed to manage these risks. Risks identified in this process include the following:

- Operational risk – changes in the environment, staff, or management personnel
- Strategic risk - new technologies, changing business models, and shifts within the industry
- Compliance – legal and regulatory changes

VPM has established an independent team that is responsible for identifying risks to the entity and monitoring the operation of the firm's internal controls. The approach is intended to align the entity's strategy more closely with its key stakeholders, assist the organizational units with managing uncertainty more effectively, minimize threats to the business, and maximize its opportunities in the rapidly changing market environment. VPM attempts to actively identify and mitigate significant risks through the implementation of various initiatives and continuous communication with other leadership committees and senior management.

Information and Communications Systems

Information and communication is an integral component of VPM internal control systems. It is the process of identifying, capturing, and exchanging information in the form and time frame necessary to conduct, manage, and control the entity's operations. This process encompasses the primary classes of transactions of the organization, including the dependence on, and complexity of, information technology. At VPM, information is identified, captured, processed, and reported by various information systems, as well as through conversations with customers and employees.

Various weekly meetings are held to discuss operational efficiencies within the applicable functional areas and to disseminate new policies, procedures, controls, and other strategic initiatives within the organization. Additionally, town hall meetings are held quarterly online and recorded to provide staff with updates on the firm and key issues affecting the organization and its employees. Senior executives and other team managers lead the town hall meetings with information gathered from formal automated information systems and informal databases, as well as conversations with various internal and external colleagues. General updates to entity-wide security policies and procedures are usually communicated to the appropriate VPM personnel via Asana.

Monitoring Controls

Management monitors controls to ensure that they are operating as intended and that controls are modified as conditions change. VPM's management performs monitoring activities to continuously assess the quality of internal control over time. Necessary corrective actions are taken as required to correct deviations from company policies and procedures. Employee activity and adherence to company policies and procedures is also monitored. This process is accomplished through ongoing monitoring activities, separate evaluations, or a combination of the two.

On-Going Monitoring

VPM's management conducts quality assurance monitoring on a regular basis and additional training is provided based upon results of monitoring procedures. Monitoring activities are used to initiate corrective action through department meetings, internal conference calls, and informal notifications. Management's close involvement in VPM's operations helps to identify significant variances from expectations regarding internal controls. Upper management evaluates the facts and circumstances related to any suspected control breakdown. A decision for addressing any control's weakness is made based on whether the incident was isolated or requires a change in the company's procedures or personnel. The goal of this process is to ensure legal compliance and to maximize the performance of VPM's personnel.

Reporting Deficiencies

An internal tracking tool is utilized to document and track the results of on-going monitoring procedures. Escalation procedures are maintained for responding and notifying management of any identified risks. Risks receiving a high rating are responded to immediately. Corrective actions, if necessary, are documented and tracked within the internal tracking tool. Annual risk meetings are held for management to review reported deficiencies and corrective actions.

Changes to the System in the Last 12 Months

No significant changes have occurred to the services provided to user entities in the 12 months preceding the end of the review date.

Incidents in the Last 12 Months

No significant incidents have occurred to the services provided to user entities in the 12 months preceding the end of the review date.

Criteria Not Applicable to the System

All relevant trust services criteria were applicable to Virtual Post Solutions, Inc's VPM Platform.

Subservice Organizations

VPM's services are designed with the assumption that certain controls will be implemented by subservice organizations. Such controls are called complementary subservice organization controls. It is not feasible for all of the trust services criteria related to VPM's services to be solely achieved by VPM's control procedures. Accordingly, subservice organizations, in conjunction with the services, should establish their own internal controls or procedures to complement those of VPM.

The following subservice organization controls should be implemented by AWS to provide additional assurance that the trust services criteria described within this report are met.

Security Category	
Criteria	Controls expected to be in place
CC6.1 - The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	AWS is responsible for implementing controls for the transmission, movement, and removal of the underlying storage devices for its cloud hosting services where the entity's system resides.
CC6.2 - Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	
CC6.3 - The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.	

Security Category	
Criteria	Controls expected to be in place
CC6.5 - The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.	
CC6.6 - The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	
CC6.7 - The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.	
CC6.4 - The entity restricts physical access to facilities and protected information assets (e.g., datacenter facilities, backup media storage and other sensitive locations) to authorized personnel to meet the entity's objectives.	AWS is responsible for restricting physical access to data center facilities, backup media, and other system components including firewalls, routers, and servers where the entity's system resides.

VPM management, along with the subservice organization, define the scope and responsibility of the controls necessary to meet all the relevant trust services criteria through written contracts, such as service level agreements. In addition, VPM performs monitoring of the subservice organization controls, including the following procedures:

- Holding periodic discussions with vendors and subservice organization
- Reviewing attestation reports over services provided by vendors and subservice organization
- Monitoring external communications, such as customer complaints relevant to the services by the subservice organization.

Complementary User Entity Controls

VPM's services are designed with the assumption that certain controls will be implemented by user entities. Such controls are called complementary user entity controls. It is not feasible for all the SOC 2 Criteria related to VPM's services to be solely achieved by VPM's control procedures. Accordingly, user entities, in conjunction with the services, should establish their own internal controls or procedures to complement those of VPM's.

The following complementary user entity controls should be implemented by user entities to provide additional assurance that the SOC 2 Criteria described within this report are met. As these items represent only a part of the control considerations that might be pertinent at the user entities' locations, user entities' auditors should exercise judgment in selecting and reviewing these complementary user entity controls.

1. User entities are responsible for understanding and complying with their contractual obligations to VPM.
2. User entities are responsible for notifying VPM of changes made to technical or administrative contact information.
3. User entities are responsible for maintaining their own system(s) of record.
4. User entities are responsible for ensuring the supervision, management, and control of the use of VPM services by their personnel.
5. User entities are responsible for developing their own disaster recovery and business continuity plans that address the inability to access or utilize VPM services.
6. User entities are responsible for providing VPM with a list of approvers for security and system configuration changes for data transmission.
7. User entities are responsible for immediately notifying VPM of any actual or suspected information security breaches, including compromised user accounts, including those used for integrations and secure file transfers.