System and Organization Controls (SOC) 3

Report on Private Tech Inc. dba Cape's Mobile Carrier Platform Relevant to Security, Availability, Processing Integrity, Confidentiality, and Privacy Throughout the Period August 1, 2025, to October 31, 2025

Cape

INSIGHT ASSURANCE

+1 877.607.7727

www.InsightAssurance.com

TABLE OF CONTENTS

SECTION 1: INDEPENDENT SERVICE AUDITOR'S REPORT 1

INDEPENDENT SERVICE AUDITOR'S REPORT ON A SOC 3 EXAMINATION 2

SECTION 2: PRIVATE TECH INC. DBA CAPE'S MANAGEMENT ASSERTION 4

PRIVATE TECH INC. DBA CAPE'S MANAGEMENT ASSERTION 5

ATTACHMENT A: DESCRIPTION OF THE SYSTEM BOUNDARIES 6

PRIVATE TECH INC. DBA CAPE'S DESCRIPTION OF THE BOUNDARIES OF THE MOBILE CARRIER PLATFORM 7

ATTACHMENT B: PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS 18

PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS 19

SECTION 1:
INDEPENDENT SERVICE AUDITOR'S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT ON A SOC 3 EXAMINATION

To: Private Tech Inc. dba Cape

Scope

We have examined Private Tech Inc. dba Cape's ("Cape") accompanying assertion titled "Private Tech Inc. dba Cape's Management Assertion" (assertion) that the controls within the Mobile Carrier Platform (system) were effective throughout the period August 1, 2025, to October 31, 2025, to provide reasonable assurance that Cape's service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability, Processing Integrity, Confidentiality, and Privacy (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

Cape 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 Cape's service commitments and system requirements were achieved. Cape has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, Cape 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 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 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 believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

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

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 Cape'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 Cape'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.

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 the Mobile Carrier Platform were effective throughout the period August 1, 2025, to October 31, 2025, to provide reasonable assurance that Cape's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

Insight Compliance LLC

dba Insight Assurance
Tampa, Florida
January 27, 2026

SECTION 2:
PRIVATE TECH INC. DBA CAPE'S MANAGEMENT ASSERTION

Cape

PRIVATE TECH INC. DBA CAPE'S MANAGEMENT ASSERTION

We are responsible for designing, implementing, operating, and maintaining effective controls within Private Tech Inc. dba Cape's ("Cape") Mobile Carrier Platform throughout the period August 1, 2025, to October 31, 2025, to provide reasonable assurance that Cape's service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability, Processing Integrity, Confidentiality, and Privacy (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*. Our description of the boundaries of the system is presented in Attachment A 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 August 1, 2025, to October 31, 2025, to provide reasonable assurance that Private Tech Inc. dba Cape's service commitments and system requirements were achieved based on the applicable trust services criteria. Private Tech Inc. dba Cape'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 August 1, 2025, to October 31, 2025, to provide reasonable assurance that Private Tech Inc. dba Cape's service commitments and system requirements were achieved based on the applicable trust services criteria.

Private Tech Inc. dba Cape
January 27, 2026

ATTACHMENT A:
DESCRIPTION OF THE SYSTEM BOUNDARIES

ATTACHMENT A

PRIVATE TECH INC. DBA CAPE'S DESCRIPTION OF THE BOUNDARIES OF THE MOBILE CARRIER PLATFORM

Company Background

Cape ("the company") is a privately held company established in April 2022. Cape is an early-stage startup, heavy Mobile Virtual Network Operator ("MVNO"), serving as a more private and secure mobile carrier for privacy-conscious consumers. Cape is a C Corporation headquartered in Arlington, Virginia.

Description of Services Overview

Cape is a Federal Communications Commission (FCC)-registered telecommunications company ("telco") that provides domestic and international talk, text, and data services. There are four core elements of the "Cape Platform," referred to collectively for ease of reference:

- a subscription-based secure telecommunications service (the "Cape Service").
- a mobile application installed on end users' mobile devices (the "Cape App").
- a cloud-based back end (the "Cape Mobile Core").
- a pre-configured mobile Android device (the "Cape Phone").

Cape Platform

Cape offers users a private and secure cloud-based mobile carrier service that addresses privacy and security vulnerabilities at the cellular network level. Cape developed its network to safeguard users' sensitive and personal information by restoring individual users' control over their mobile identity. With privacy concerns at the forefront of its corporate mission, Cape developed a system to limit the ability of third parties to track individual users of the service by utilizing a combination of commercially available telecommunications and encryption software, along with secure data-handling protocols.

Cape Service

Cape provides its customers with subscription-based 4G and 5G-capable voice and data services, offering nationwide coverage. While the Cape Service is like a cellular plan offered by traditional cellular carriers, it provides users with minimal data collection and more built-in security and privacy features.

Cape App

To access the Cape Service, individual users must download and install Cape's mobile application, the Cape App. Among other functions, such as billing and account management, the Cape App provides users with the privacy features described in more detail below, which limit the ability of third parties, including advertisers and data brokers, to identify and track users. The Cape App is built from one codebase per OS, used by individual consumers and employees of

business enterprises and government agencies. Certain app features have limited availability (such as those on certain types of plans) or for certain types of customers.

Cape Mobile Core

Cape utilizes a cloud-based telecommunications back-end, the Cape Mobile Core. The 4G/5G-capable Cape Mobile Core enables Cape subscribers to make voice calls, exchange messages, and access the internet like any other phone plan, but with added safety and security.
The Cape Mobile Core is a system configured by Cape that consists of cloud-based telecommunications and encryption software produced by other companies.

Cape Phone

Cape's offering was designed and developed for use with any mobile handset; however, Cape also offers customers the Cape Phone, a pre-configured mobile Android device. Cape partners with Nothing Technology Limited ("Nothing"), a consumer electronics manufacturer, to modify the pre-installed device firmware and accommodate certain Cape privacy features and functionality, including IMEI switching, which is currently not possible on other devices due to the constraints of most other mobile phone firmware.

INFRASTRUCTURE

Cape utilizes AWS as a sub-service organization to host the Cape Platform, which is the central processing system supporting Cape's telecommunications services. By leveraging a leading Cloud Service Provider (CSP), Cape benefits from a highly reliable, secure, and scalable infrastructure that supports both current operational demands and anticipated future growth. The use of AWS enables Cape to focus on product development and service delivery, while relying on AWS's robust physical and environmental controls to maintain the security, availability, and confidentiality of customer data.

Cape's production environment is deployed across multiple Availability Zones (AZs) within geographically isolated AWS Regions to enhance fault tolerance and disaster recovery capabilities. Key components of the infrastructure—including compute instances, storage volumes, container orchestration, and network security controls—are managed through Infrastructure-as-Code (IaC) to ensure consistency, version control, and auditability.

SOFTWARE

The Company is responsible for managing the development and operation of the system. The software supporting the system consists of applications, programs, and other software components used to build, secure, maintain, and monitor the system

A description of software and tools supporting the Mobile Carrier Platform is shown in the table below:

Software Function
Threat Detection software
Vulnerability Management software
API monitoring software
Platform resources monitoring software
Password Manager software
International Roaming Aggregator software
Protocol Buffers software
CI/CD Pipeline Automation platform
Endpoint Detection & Response (EDR) software
Source code and version control software
Productivity and collaboration tool software
Biometric identification, cryptography and digital security tool
Integrated development environment software
Mobile Device Management (MDM) software
Cloud network and communications software
Mobile security and privacy testing software
Identity and Access management software
Incident reports and alert software
Voice, mobile, SMS/MMS number porting and trunking software
Lawful Intercept software
Payment Processing software
Virtual Private Network software
Application build and scale software

PEOPLE

The company employs dedicated team members to handle major product functions, including operations directly supporting the system. Cape's corporate structure includes the following roles and teams:

Chief Executive Officer (CEO) – Responsible for setting the company's vision, strategy, and long-term goals while driving overall business growth and success. They lead and inspire the executive team, make key decisions on funding, partnerships, and market positioning, and ensure the company adapts to changing market conditions. This role involves building a strong organizational culture, securing resources, and representing the company to investors, customers, and stakeholders. Additionally, the CEO is accountable for delivering results, balancing innovation with execution, and steering the startup toward profitability and scalability.

Chief of Staff – Serves as a strategic partner, helping the CEO manage priorities, execute key initiatives, and enhance organizational effectiveness. They facilitate communication across departments, prepare executive briefings, and ensure alignment between company goals and operations. This role often involves managing high-impact projects, streamlining decision-making processes, and providing data-driven insights to support strategic planning. Additionally, they act as a trusted advisor to the CEO, enabling them to focus on high-level vision and growth by handling day-to-day operational and strategic tasks.

Head of Internal Operations – Responsible for internal processes critical to tactical execution and company scaling. They oversee Finance, Recruiting, and Legal. They design and implement repeatable processes to enable speed and consistency at scale. This role involves interfacing with external advisory service experts and aligning them for maximum impact to the company. They focus on financial excellence and hiring, training, and growing the company. Additionally, they identify and address bottlenecks within the company through processes that drive sustainable growth.

Head of R&D – Responsible for driving innovation by leading the research and development of new products, technologies, or features that align with the company's strategic vision. They oversee R&D projects, manage teams of engineers and researchers, and ensure rapid experimentation, prototyping, and iteration. This role involves identifying emerging technologies, analyzing market trends, and collaborating with product and engineering teams to translate innovative ideas into viable solutions. Additionally, they play a key role in fostering a culture of creativity, continuous learning, and technological advancement to maintain Cape's competitive edge.

Head of Forward Deployed Engineering – Responsible for leading the development and delivery of the company's mobile applications, ensuring they are scalable, secure, and user-friendly. They manage the mobile engineering team, oversee architecture and technology decisions, and drive the implementation of best practices in development, testing, and deployment. This role involves collaborating closely with product, design, and other engineering teams to align mobile features with business goals and user needs. Additionally, they stay abreast of emerging mobile technologies and trends to continually innovate and enhance the mobile user experience.

Head of Network, Infrastructure Engineering – Responsible for designing, implementing, and maintaining the company's network infrastructure to ensure high availability, security, and performance. They oversee network architecture, including cloud and on-premises connectivity, and manage technologies such as firewalls, VPNs, and load balancers. This role involves monitoring network performance, troubleshooting issues, and mitigating security risks while ensuring compliance with industry standards and regulations. Additionally, they collaborate with engineering and IT teams to support scalable solutions, optimize network resources, and plan for future growth.

Head of Product – Responsible for defining and executing the product vision, strategy, and roadmap in alignment with business goals. They collaborate closely with cross-functional teams—comprising engineering, design, marketing, and sales—to prioritize features, address customer pain points, and drive product development. This role involves gathering and analyzing user

feedback, market trends, and data to inform decisions while ensuring rapid iterations to achieve product-market fit. Additionally, they act as a key product advocate, fostering a culture of innovation and ensuring the product delivers measurable business impact.

Head of Consumer Growth – Responsible for defining and executing the vision, strategy, and roadmap for the growth of the consumer business. Facilitate cross-functional collaboration between Product, Engineering, Design, Operations, and Marketing to optimize sales channels, gather user feedback, and analyze customer trends to realize growth in line with business goals.

Head of Federal Sales – Responsible for the company's strategy and execution across the Department of Defense, Intelligence Community, and federal law enforcement. This includes driving go-to-market efforts for Cape's secure mobile communications platform, enabling mission-critical connectivity in contested and surveillance-heavy environments. Builds strategic partnerships, captures priority programs, and aligns Cape's solutions with emerging federal requirements. Also oversees delivery and growth initiatives to ensure Cape scales as a trusted national security partner.

Head of Security – Responsible for developing and implementing a comprehensive security strategy to protect company assets, data, and operations. They oversee risk assessments, incident response, and the enforcement of security policies across all teams and technologies. This role involves staying ahead of emerging threats, ensuring compliance with security standards, and building a culture of security awareness. Additionally, they collaborate with engineering and product teams to embed security practices into the company's development and business processes.

Head of International Expansion – Responsible for leading Cape's global growth strategy by identifying, evaluating, and executing opportunities to expand into new international markets. This role oversees market entry planning, regulatory and compliance alignment, localization of product and operations, and the development of cross-functional go-to-market strategies. The Head of International Expansion ensures scalable, compliant, and customer-centric growth abroad while collaborating closely with product, legal, finance, and operations teams.

Head of Talent – Responsible for owning all aspects of the Cape's people operations. This includes talent acquisition, employee experience, performance management, compensation strategy, and organizational development to support scaling. Ensure compliance and implement processes that attract, retain, and develop top talent in alignment with business goals. Acting as a strategic partner to leadership to create a high-performance, engaged workforce that enables Cape's growth.

Head of Finance – Responsible for overseeing financial strategy, planning, operations, and compliance to ensure the company remains financially healthy and scalable. They manage budgeting, forecasting, treasury, accounting, and financial reporting while advising leadership on fundraising, investments, and risk management. This role involves optimizing resource allocation, ensuring compliance with regulatory requirements, and implementing financial controls. Additionally, they support key business decisions by providing data-driven insights and strategies to drive sustainable growth.

Head of SRE – Responsible for designing, building, and maintaining the company's technology infrastructure to support scalability, performance, and reliability. They oversee cloud services, networks, servers, and deployment pipelines, ensuring up time, security, and cost efficiency. This role involves collaborating with engineering teams to optimize infrastructure for development and operations, implementing automation, and managing infrastructure-as-code practices. Additionally, they monitor system performance, manage incidents, and lead efforts to adopt new technologies to support business growth and agility.

DATA

Customer data is managed, processed, and stored in accordance with the relevant data protection and other regulations, with specific requirements formally established in customer agreements.

All employees and contractors of the company are obligated to respect and, in all cases, to protect customer data. Additionally, the Company has policies and procedures in place for proper and

secure handling of customer data. These policies and procedures are reviewed on at least an annual basis.

Data is classified into the following major categories as outlined below.

Data		
Category	**Description**	**Examples**
Restricted	Sensitive information; baseline access limited to a subset of Cape FTEs	• Data requiring a business need, or "need-to-know" • Legal, contractual, or regulatory safeguarding obligations • Sensitive public-sector or government information (that is not classified or controlled) • Sensitive architecture or infrastructure details • Authentication information • Passwords • Shared secrets • Cryptographic private keys • Hash tables • Attributable quotes and sources (not approved for Internal or Public release) • Technical data • Code repositories and build artifacts • Vulnerability scan results • Penetration testing results • Test range credentials • SIM inventory information • Personally Identifiable Information (PII) • Social Security Numbers (SSN) • Driver's license numbers • Individual's expenses • Human Resources data • Compensation data • Financial Information • Account numbers + security or PIN codes • Revenue and Expense reports • Financial statements • Banking details • Credit card information • Tax Records • Capitalization Table

Data		
Category	**Description**	**Examples**
Internal	Non-sensitive information; baseline access includes Cape FTEs	• Proprietary information about ownership (patents, copyrights, or trademarks) • Business operation details • Team and project planning artifacts • Written artifacts • Meeting reports • Product roadmaps that have not been approved for Public Release • Supplier, Partner, and Vendor information, pricing, contracts • General ticketing / IT Service Management (ITSM) information
Public	Non-sensitive information; freely shareable	• Information that is freely shareable both internally and externally • Information already publicly available (e.g., information on the website)

PROCEDURES

Management has developed and communicated policies and procedures involved in the operation of the system. These procedures are developed in alignment with the information security policy and are reviewed, updated, and approved as necessary for changes in the business at least annually. Cape's employees are responsible for reading and acknowledging upon hire, annually thereafter, and when material changes are made.

Physical Security and Environmental Security

Cape's production servers are maintained by AWS. The physical and environmental security protections are the responsibility of AWS. Cape reviews the attestation reports and performs a risk analysis of AWS on at least an annual basis.

Logical Access

Cape provides employees and contractors with access to infrastructure via a role-based access control system, ensuring uniform, least privileged access for identified users and maintaining simple user provisioning and de-provisioning processes. Access to these systems is split into three levels: Administrator, User, and No Access. User access and roles are reviewed quarterly for critical applications and annually for non-critical applications to ensure the least privileged access is granted.

Initially, the Talent team is responsible for conducting reference checks and populating employee information into the Human Resources Information System (HRIS). The IT Team is then responsible for automatically provisioning access to other systems based on the employee's role. From there, the employee is responsible for reviewing and acknowledging Cape's policies in our Continuous Compliance Platform and completing the new-hire security training.

When an employee is terminated, the offboarding team is responsible for deprovisioning access to all in-scope systems on the same day as the employee's termination.

Change Management

Cape maintains documented policies and procedures to guide personnel in 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.

Jira is used to document the change control procedures for changes to the application and the implementation of new changes. Changes are tested in an environment that is logically separated from the production environment. The Change Control Board approves changes before migration to the production environment and documents those approvals within the ticketing system.

Patch Management

Software patches and updates are applied to systems as part of Cape's change and vulnerability management processes. The infrastructure supporting Cape's services is regularly maintained to help ensure systems remain protected against known security threats. Updates are subject to testing and validation procedures before deployment to minimize unintended disruptions.

Cape follows a risk-based approach to vulnerability remediation. Critical security patches are prioritized and typically applied within 30 days of identification, while non-critical patches are addressed during scheduled maintenance cycles, typically on a quarterly basis. This schedule may be expedited in cases where vulnerabilities pose a significant threat to the confidentiality, integrity, or availability of systems supporting the Cape telecommunications services system.

Backups and Recovery

Customer data is backed up nightly and monitored by Site Reliability Engineering (SRE) Team for completion and exceptions. If an exception occurs, the SRE team performs troubleshooting to identify the root cause and either rerun the backup or address the issue as part of the next scheduled backup job. Backup infrastructure is access-controlled and encrypted.

Computer Operations

Cape maintains an incident response plan to guide employees on reporting and responding to any information security or data privacy events or incidents. Procedures are in place for identifying, reporting, and acting upon breaches or other incidents.

Cape internally monitors all applications, including the web UI, databases, and cloud storage, to ensure that service delivery matches SLA requirements.

Cape utilizes vulnerability scanning software that checks source code for common security issues and vulnerabilities identified in open-source dependencies and maintains an internal Service Level Agreement (SLA) to respond to those issues.

Problem Management

Cape's methodology is based on the ITIL Framework, with alerts, warnings, and errors categorized as Events. Events cause Incidents, and the root cause of Incidents is defined as Problems. Cape maintains an Incident Response Plan that describes the process for identifying and addressing potential security and network incidents. The policy details exactly what must occur if an incident is suspected and covers both electronic and physical security incidents. The policy includes plans for detecting, responding to, and recovering from incidents, as well as defining post-incident activity requirements. To ensure that responsible employees are prepared to respond to incidents, the organization provides formal security breach training. The final stage of the Incident Response Plan involves conducting a root-cause analysis and providing lessons learned to the applicable teams.

Cape's public-facing Help Center and Live Chat Support provide customers with an avenue to report potential security breaches, as well as a Security email distribution list for the same purpose. Internal users are directed to escalate incidents to the Incident Response team or through an anonymous portal.

Data Communications

Cape has elected to use AWS to run its production infrastructure in part to avoid the complexity of network monitoring, configuration, and operations. AWS simplifies the company's logical network configuration by providing an effective firewall around Cape's application containers, with the only ingress from the network via HTTPS connections to designated web frontend endpoints.

AWS also automates the provisioning and de-provisioning of containers to match the desired configuration. If an application container fails, it will be automatically replaced, regardless of whether the failure occurs in the application or on the underlying hardware.

System Monitoring

The Data Protection Policy describes the organization's policies and procedures related to network logging and monitoring, while the Vulnerability Management Policy addressed vulnerability identification and remediation. The organization utilizes Okta for system access logging within the SSO environment, and it collects and reviews logs from the office router and firewall. Okta logs, the office router, and firewall logs document the source IP, destination IP, destination port, protocol type, and timestamp. The organization monitors system capacity using the Meraki bandwidth monitoring tool.

The vulnerability assessment process involves executing CIS testing, implementing antivirus software, and applying system patches. The organization utilizes CrowdStrike anti-malware and has configured the software to run daily updates and prohibit end-users from disabling or altering the software. Alerts are sent immediately when a potential virus is detected, and logs are generated and retained for at least one year, with at least three months readily available. AWS Inspector is used to identify newly emerging vulnerabilities, and the organization monitors vendors for patch updates to correct vulnerabilities.

Vendor Management

The organization maintains a Vendor Management Policy that outlines requirements for interacting with vendors and service providers. The policy includes requirements for performing due diligence measures prior to engaging with a new provider. Due diligence procedures include evaluating each material IT vendor's cost-effectiveness, functionality, services, risk, financial viability, compliance, and performance. The organization is required to define service levels when negotiating a new arrangement with a vendor or renegotiating an existing one, and all service levels must be agreed upon and documented clearly. The organization monitors its providers' service levels to ensure that each provider is delivering the agreed-upon services and is compliant with all relevant requirements. The organization executes non-disclosure agreements with third parties before sharing any information.

Boundaries of the System

The boundaries of the Cape Platform are the specific aspects of the Company's infrastructure, software, people, procedures, and data necessary to provide its services and that directly support the services provided to customers. Any infrastructure, software, people, procedures, and data that indirectly support the services provided to customers are not included within the boundaries of the Cape Platform.

This report does not include the Cloud Hosting Services provided by AWS at multiple facilities.

ATTACHMENT B: PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

ATTACHMENT B

PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

Cape designs its processes and procedures related to the system to meet its objectives. Those objectives are based on the service commitments that Cape makes to user entities, the laws, and regulations that govern the provision of the services, and the financial, operational, and compliance requirements. The system services are subject to Security, Availability, Processing Integrity, Confidentiality, and Privacy commitments established internally for its services. Commitments to user entities are documented and communicated in Service Level Agreements (SLAs) and other customer agreements, as well as in the description of the service offering that is provided online.

Security commitments include, but are not limited to, the following:

- System features and configuration settings designed to authorize user access while restricting unauthorized users from accessing information not needed for their role.
- Use of intrusion detection systems to prevent and identify potential security attacks from users outside the boundaries of the system.
- Regular vulnerability scans over the system and network, and penetration tests over the production environment.
- Operational procedures for managing security incidents and breaches, including notification procedures.
- Use of encryption technologies to protect customer data both at rest and in transit.
- Use of data retention and data disposal.

Availability commitments include, but are not limited to, the following:

- System performance and availability monitoring mechanisms to help ensure the consistent delivery of the system and its components.
- Responding to customer requests in a reasonably timely manner.
- Business continuity and disaster recovery plans that include detailed instructions, recovery point objectives (RPOs), recovery time objectives (RTOs), roles, and responsibilities.
- Operational procedures supporting the achievement of availability commitments to user entities.
- Uptime availability of production systems.

Processing Integrity commitments include, but are not limited to, the following:

- Controls exist to prevent or detect and correct processing errors to meet the entity's processing integrity commitments and system requirements.
- System inputs are measured and recorded completely, accurately, and timely to meet the entity's processing integrity commitments and system requirements.
- Data is processed completely, accurately, and timely as authorized to meet the entity's processing integrity commitments and system requirements.

- Data is stored and maintained completely, accurately, and promptly for its specified life span to meet the entity's processing integrity commitments and system requirements.
- System output is complete, accurate, and distributed to meet the entity's processing integrity commitments and system requirements.
- Modification of data, other than routine transaction processing, is authorized and processed to meet the entity's processing integrity commitments and system requirements.

Confidentiality commitments include, but are not limited to, the following:

- The use of encryption technologies to protect system data both at rest and in transit.
- Confidentiality and non-disclosure agreements with employees, contractors, and third parties.
- Confidential information must be used only for the purposes explicitly stated in agreements between Cape and user entities.

Privacy commitments include, but are not limited to, the following:

- The company defines documents, communicates, and assigns accountability for its privacy processes and procedures.
- The company provides notice about its privacy processes and procedures and identifies the purposes for which personal information is collected, used, retained, and disclosed.
- The company describes the choices available to the individual and obtains implicit or explicit consent concerning the collection, use, and disclosure of personal information.
- The company collects personal information only for the purposes identified in the notice.
- The company limits the use of personal information to the purposes identified in the notice and for which the individual has provided implicit or explicit consent.
- The company discloses personal information to third parties only for the purposes identified in the notice and with the implicit or explicit consent of the individual.
- The company protects personal information against unauthorized access (both physical and logical).
- The company maintains accurate, complete, and relevant personal information for the purposes identified in the notice.
- The company monitors compliance with its privacy policies and practices.