
***System and Organization Controls 3 (SOC 3) Report – SOC for Service Organizations: Trust Services Criteria for General Use Report***

***Report on Cockroach Labs, Inc.'s Description of its CockroachDB Dedicated and Serverless Platform Relevant to Security, Availability, and Confidentiality Throughout the February 1, 2024 to September 30, 2024***

Bonadio & Co., LLP
Accounting, Consulting & More

**REPORT ON COCKROACH LABS, INC.'S DESCRIPTION OF ITS COCKROACHDB DEDICATED AND SERVERLESS PLATFORM RELEVANT TO SECURITY, AVAILABILITY, AND CONFIDENTIALITY THROUGHOUT THE PERIOD FEBRUARY 1, 2024 TO SEPTEMBER 30, 2024**

**Table of Contents**

# SECTION ONE

## Independent Service Auditor's Report

Bonadio & Co., LLP
Accounting, Consulting & More

## INDEPENDENT SERVICE AUDITOR'S REPORT

To: Management of Cockroach Labs, Inc.

### Scope

We have examined Cockroach Labs, Inc.'s accompanying assertion, titled "Assertion of the Management of Cockroach Labs, Inc." (assertion), that controls within Cockroach Labs, Inc.'s CockroachDB Dedicated and Serverless Platform (the System) were effective throughout the period February 1, 2024 to September 30, 2024, to provide reasonable assurance that Cockroach Labs, Inc.'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, (With Revised Points of Focus—2022) in AICPA, *Trust Services Criteria* and included as Attachment A.

### Service Organization's Responsibilities

Cockroach Labs, Inc. 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 Cockroach Labs, Inc.'s service commitments and system requirements were achieved. Cockroach Labs, Inc. has also provided the accompanying assertion about the effectiveness of controls within the System. When preparing its assertion, Cockroach Labs, Inc. 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 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.

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

100 Corporate Parkway
Suite 200
Amherst, NY 14226
p (716) 250-6600
f (716) 250-6605

www.bonadio.com

**Service Auditor's Responsibilities (Continued)**

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 Cockroach Labs, Inc.'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 Cockroach Labs, Inc.'s service commitments and system requirements based the applicable trust services criteria.

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

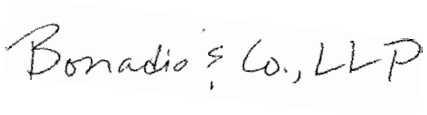
**Inherent Limitations**

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 Cockroach Labs, Inc.'s CockroachDB Dedicated and Serverless Platform were effective throughout the period February 1, 2024 to September 30, 2024, to provide reasonable assurance that Cockroach Labs, Inc.'s service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.




Amherst, New York
December 19, 2024

# SECTION TWO

## Assertion of the Management of Cockroach Labs, Inc.

CockroachDB

## ASSERTION OF THE MANAGEMENT OF COCKROACH LABS, INC.

December 19, 2024

We are responsible for designing, implementing, operating, and maintaining effective controls within Cockroach Labs, Inc.'s CockroachDB Dedicated and Serverless Platform throughout the period February 1, 2024 to September 30, 2024, to provide reasonable assurance that Cockroach Labs, Inc'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 (With Revised Points of Focus — 2022), in AICPA Trust Services Criteria*. Our description of the boundaries of the CockroachDB Dedicated and Serverless Platform is presented in Section 3 and identifies the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of the controls within the CockroachDB Dedicated and Serverless Platform throughout the period February 1, 2024 to September 30, 2024, to provide reasonable assurance that Cockroach Labs, Inc.'s service commitments and system requirements were achieved based on the applicable trust services criteria. Cockroach Labs, Inc.'s objectives for the CockroachDB Dedicated and Serverless Platform 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 CockroachDB Dedicated and Serverless Platform were effective throughout the period February 1, 2024 to September 30, 2024, to provide reasonable assurance that Cockroach Labs, Inc.'s service commitments and system requirements were achieved based on the applicable trust services criteria.

Mike Geehan
Head of Security and Compliance

# SECTION THREE

## Management's Description of Cockroach Labs, Inc.'s CockroachDB Dedicated and Serverless Platform Throughout the February 1, 2024 to September 30, 2024

## INTRODUCTION

### Company Overview

Cockroach Labs, Inc. (Cockroach Labs or the Company) is a computer software company that develops commercial database management systems. It is best known for CockroachDB, a distributed Structured Query Language (SQL) database. CockroachDB is a project that is designed to store copies of data in multiple locations in order to deliver speedy access.

Cockroach Labs has architected and built CockroachDB – a cloud-native, distributed SQL database that provides next-level consistency, ultra-resilience, data locality, and massive scale to modern cloud applications. Cockroach Labs licenses CockroachDB to customers as a self-hosted database and offers CockroachDB as a fully managed service via CockroachDB Dedicated and CockroachDB Serverless.

### System Description

In 2019, Cockroach Labs launched the CockroachCloud Platform, a fully managed Database-as-a-Service (DBaaS) offering for CockroachDB. In 2022, this platform was renamed to CockroachDB Dedicated and Serverless (the Platform). The Platform provides a self-service web interface that customers can use to create, manage, and monitor CockroachDB clusters. The Platform database clusters are deployed by Cockroach Labs on the customers' behalf in public cloud environments. Users can visit the cockroachlabs.cloud management console to create an account and provision (and deprovision) CockroachDB clusters running on either Google Cloud Platform (GCP), Amazon Web Services (AWS), or Microsoft Azure (Azure).

CockroachDB is deployed on commodity Linux servers in topologies ranging from one to hundreds of nodes. CockroachDB implements the wire protocol from PostgreSQL and much of PostgreSQL's SQL dialect for compatibility with existing client and driver software. CockroachDB also provides a web interface for cluster monitoring and troubleshooting. CockroachDB nodes communicate with each other via the Google Remote Procedure Call (gRPC) protocol, an open- source high performance remote procedure call framework.

Cockroach Labs provides the source code and official binaries of CockroachDB to the public free of charge. Use of CockroachDB is licensed through a dual-license model. CockroachDB's core feature set (including its distributed SQL functionality and its strongly consistent, highly available storage layer) is licensed free of charge for customers hosting CockroachDB for their own use. Enterprise features (such as data encryption at rest and distributed backup) can be enabled by purchasing an enterprise license from Cockroach Labs.

### System Boundaries

The scope of this report includes the Platform, and the supporting production systems, infrastructure, software, people, procedures, and data. Cockroach Labs offers both managed DBaaS and self-hosted solutions. This report is focused on the managed version of CockroachDB; elements of the Cockroach Labs self-hosted solution are in the scope of this report where the Platform is not specifically referenced.

### Subservice Organizations

Cockroach Labs uses AWS, GCP, and Azure to host the Platform. These subservice organizations are excluded from the scope of this report; the controls they are expected to provide are included in the subsequent section titled Complementary Subservice Organization Control Considerations.

## COMPONENTS OF THE PLATFORM USED TO PROVIDE THE SERVICES

### Infrastructure

*The collection of physical or virtual resources that supports an overall IT environment, including the physical environment and related structures, IT, and hardware (for example, facilities, servers, storage, environmental monitoring equipment, data storage devices and media, mobile devices, and internal networks and connected external telecommunications networks) that the service organization uses to provide the services.*

The Platform follows a multi-tier architecture comprising application and database layers, with load-balanced, redundant infrastructure included in each layer where possible and practical. The Platform is architected using network segmentation and security groups to create logical trust boundaries between Platform components. This architecture also restricts access to public-facing networks through a defined set of ports and protocols.

The Platform is exclusively built on public cloud infrastructure and services hosted on AWS, GCP, and Azure; Cockroach Labs does not have any physical hardware infrastructure devoted to the Platform. Cloud resources used to provide the services include:

- Virtual machines, provided via Google Compute Engine, Amazon Elastic Compute Cloud, and Azure Virtual Machines.
- Managed Kubernetes compute clusters, provided via Google Kubernetes Engine (GKE), Amazon Elastic Kubernetes Service (EKS), and Azure Kubernetes Service (AKS).
- Virtual network infrastructure, such as firewalls, application load balancers, and virtual private cloud (VPC) infrastructure.
- Object storage, via Google Cloud Storage (GCS), AWS Simple Storage Service (S3) and Azure Blob Storage (Blob).

Cloud resources are provisioned via infrastructure-as-code software that runs on the Pulumi platform, detailed in the Software section below.

### Software

*The application programs and IT system software that supports application programs (operating systems, middleware, and utilities), the types of databases used, the nature of external-facing web applications, and the nature of applications developed in-house, including details about whether the applications in use are mobile applications or desktop or laptop applications.*

The application layer for the Platform is deployed on Kubernetes. It is written in Go in the backend and Typescript for front-end interfaces. Primary software and tools used to provide the Platform include the following:

## COMPONENTS OF THE PLATFORM USED TO PROVIDE THE SERVICES (CONTINUED)

**Software (Continued)**

| Vendor Software | Operating System | Function |
|---|---|---|
| CockroachDB | Linux | Control Plane Database |
| CrowdStrike | SaaS | Endpoint Monitoring |
| Datadog | SaaS | Infrastructure monitoring |
| EKS | IaaS | Cloud-hosted Kubernetes in public cloud infrastructure |
| GCS | IaaS | Public cloud object storage |
| GKE | IaaS | Cloud-hosted Kubernetes in public cloud infrastructure |
| Google Security Command Center (GSCC) | SaaS | GCP intrusion detection system (IDS) |
| GuardDuty | SaaS | AWS IDS |
| GitHub | SaaS | Version control and issue tracking for engineering/development |
| TeamCity | Linux | Continuous integration and continuous delivery (CI/CD) |
| HashiCorp Vault | Linux | Vault is used to store secrets and manage security certificates |
| Jira | SaaS | Issue tracking system |
| Prometheus | Linux | Infrastructure and application monitoring |
| Pulumi | Linux | Infrastructure as code |
| S3 | SaaS | Public cloud object storage |
| Splunk | SaaS | Infrastructure logging |
| Panther | SaaS | Infrastructure logging, detection, and alerting |
| Stripe | SaaS | Credit card payment acceptance |
| Terraform | Linux | Infrastructure as code |
| Spacelift | Linux | Infrastructure as code |
| Qualys | SaaS | Vulnerability scanning |
| AKS | IaaS | Cloud-hosted Kubernetes in public cloud infrastructure |
| Blob | IaaS | Public cloud object storage |
| Microsoft Defender | SaaS | Azure IDS |
| Rootly | SaaS | Availability incident management |
| OpsGenie | SaaS | On-call paging system |

Architecturally, the Platform is composed of the following internal components:

- *Web UI* – The customer-facing web interface for customers to self-manage clusters, user accounts, and billing.
- *Control plane* – A set of services that is responsible for instantiating and managing the public cloud resources of which customer clusters are composed.
- *Dedicated customer clusters* – CockroachDB Dedicated customers' CockroachDB clusters are provisioned in a dedicated AWS, GCP, or Azure VPC.
- *Serverless customer clusters* – CockroachDB Serverless customers' CockroachDB clusters are provisioned in a shared Kubernetes (K8s) instance of CockroachDB and customer K8s tenant pods manage logical isolation.

## COMPONENTS OF THE PLATFORM USED TO PROVIDE THE SERVICES (CONTINUED)

### People

*The personnel involved in the governance, management, operation, security, and use of a system (business unit personnel, developers, operators, user entity personnel, vendor personnel, and managers).*

The personnel primarily involved in the security governance, operation, and management of the client include the following:

- *Engineering* – The Engineering team is responsible for the ideation, construction, and development of Cockroach Labs' products. Engineering is divided into many product teams according to logical areas of CockroachDB and the Platform, such as Storage, SQL Execution, and the Platform and includes the following teams:
    - *Cloud Console* – Responsible for front-end development, on-call front-end support, and User Experience and User Interface (UX/UI) components.
    - *Cloud Platform (CP)* – Responsible for the automations and tooling required to acquire and stand up the cloud infrastructure.
    - *Corporate Engineering* – Responsible for Cockroach Labs' internal information technology (IT) operations and infrastructure.
    - *Engineering On-Call* – Level 2 and Level 3 support engineers responsible for triaging, driving, and resolving customer issues in a timely manner.
    - *Engineering Productivity and Developer Infrastructure* – Responsible for maintaining internal development tools, continuous integration, and release engineering.
    - *Engineering Operations* – Responsible for Engineering team operations.
    - Site Reliability Engineering (SRE) – Responsible for the Platform production operations.
    - *Information Security* – Responsible for operational security of the Platform (working with SRE), information security compliance, and secure development of the Platform and CockroachDB.
    - *Technical Support Engineering (TSE)* – Expert support for any database related issues and questions. This team diagnoses, reproduces, and fixes issues.
    - *Compliance* - Responsible for ensuring that an organization adheres to industry regulations, standards, and laws related to information security and data privacy.
- *Finance* – Responsible for accounts receivable, accounts payable, insurance, budgeting and forecasting, the annual planning process, income tax, sales tax, treasury and cash management, general ledger accounting, technical accounting, revenue recognition, regulatory compliance, and financial reporting. Finance also partners with other departments for investor relations and equity raises, payroll, commissions and customer deal reviews.
- *Compliance, Security, and Corporate Engineering (CSC) Team* - Cross functional team that implements and manages the day-to-day security, risk, and compliance functions of the organization.
- *Information Security Management System (ISMS) Committee* – Cross-functional committee responsible for the security, risk, and compliance efforts of the Company.
- *Marketing* – Responsible for bringing CockroachDB to the world, building a community of open-source and enterprise users. Entails content marketing, creative design, demand generation, and product marketing functional areas.
- *Legal* – In-house general counsel of the Company.

## COMPONENTS OF THE PLATFORM USED TO PROVIDE THE SERVICES (CONTINUED)

### People (Continued)

- *People Operations* – Responsible for finding, growing and retaining talent to embody the Company's values and support the Company culture and mission.
    - *Human Resources (HR) and Office Experience* – The HR and Office Experience team is responsible for employee development and retention at Cockroach Labs.
    - *Recruiting* – The Recruiting team is responsible for finding talent for Cockroach Labs.
- *Product* – Responsible for the research, prioritization, and delivery of Cockroach Labs' products.
    - *Education* – The Education team is composed of Documentation and Training teams, with a mission to make it easy to learn CockroachDB.
    - *Product Design* – The Product Design team at Cockroach Labs is responsible for creating a scalable consumer-grade user experience that makes data easy for all users of CockroachDB.
    - *Product Management* – The Product Management team is responsible for guiding CockroachDB to product-market fit through problem discovery, customer-centric execution, and differentiated go-to-market.
- *Revenue* – Runs sales, service, sales operations, technical support, and sales enablement for Cockroach Labs' customers; entails business development (partner engagement), customer success, sales account executives, sales development representatives, sales engineering, and sales operations.
- *Technology* – Includes the ideation, construction, execution of the development of Cockroach Labs' products and the ongoing support of its customers.

### Data

*The types of data used by the system, such as transaction streams, files, databases, tables, and other output used or processed by the Platform.*

The data stored and processed by the Platform service consists of:

- Data stored and managed by customers within their clusters
- Backups of customer data
- Management console user and account information
- Cluster and cloud infrastructure metadata
- Monitoring and logging data

### Processes and Procedures

*The automated and manual procedures related to the services provided, including, as appropriate, procedures by which service activities are initiated, authorized, performed, and delivered, and reports and other information are prepared.*

Formal policies and procedures codify the principles and requirements to help ensure security, availability, and confidentiality of the Platform. The Company maintains the following policies and procedures:

- *Acceptable Encryption Policy* – provides guidance on proper use of encryption.
- *Cockroach Labs GitHub User Access Policy* – outlines administrative access responsibilities for GitHub.

## COMPONENTS OF THE PLATFORM USED TO PROVIDE THE SERVICES (CONTINUED)

### Processes and Procedures (Continued)

- *Business Continuity Plan* – provides direction and guidance for the continued fulfillment of Cockroach Labs' service contracts and the ongoing continuity of Cockroach Labs' business operations when an event or series of events impacts the primary Cockroach Labs facility.
- *CockroachDB Cloud Backup Policy* – specifies scope and frequency of backups for the Platform production infrastructure.
- *CockroachDB Cloud Capacity Management Policy* – outlines process to help ensure the Platform maintains sufficient capacity to meet customer demand.
- *CockroachDB Cloud Disaster Recovery Test Plan* – provides direction and guidance for simulating a disaster event, recovery steps, and post recovery tests to recover from a disaster event.
- *CockroachDB Cloud Production System Access Policies* – set of policies that outlines processes to govern access control to the Platform production environment.
- *CockroachDB Cloud Staging System Access Policy* – outlines processes to govern access control to the Platform production environment.
- *Cockroach Labs Information Security Policy* – describes general company security policies and procedures. Specifically, it includes a defined set of information security standards and policies that are under the direction and ownership of the ISMS Committee. The Security Policy includes content related to risk and control assessment, security awareness, secure development, and system monitoring. These standards and policies address the management and implementation of security controls of the logical security and the data element layer. The information security policies and standards are designed to provide information to employees, contractors, and vendors that are aligned with their job or functional responsibilities, while also contemplating segregation of functions that may otherwise create a segregation of duties conflict.
- *Employee Handbook* – sets forth the commitments to integrity and ethics, standards of conduct, and employee expectations designed to maintain a healthy, fun, and supportive environment.
- *Data Classification Policy* – this policy classifies company data to help personnel determine what information can be disclosed to fellow employees, contractors, or customers as well as the relative sensitivity of information that should not be disclosed outside of Cockroach Labs without proper authorization.
- *Password Policy* – establishes guidance for how passwords should be managed in Cockroach Labs information systems.
- *Privacy Policy* – establishes policies and procedures regarding the privacy of user data and the confidentiality thereof. Additionally, Cockroach Labs' Terms of Service are published and require agreement from users before they utilize the Cockroach Labs services.
- *Secure Software Development and Testing Policy* – outlines the processes for developing production code, submitting code changes for review, code unit and security testing, and merging code into the master branch.
- *Security Incident Management Process* – outlines the specific processes in place for managing security-related events at Cockroach Labs, including the specific steps required to track, resolve, and mitigate incidents.
- *Vendor Management Policy* – defines policy and procedures for procurement, security approval, and risk classification of third party vendors.

# ATTACHMENT A

## AICPA Trust Services Categories and Criteria

## AICPA TRUST SERVICES CATEGORIES AND CRITERIA

This attachment includes the Trust Services Criteria (TSC) included in the scope of the engagement relevant to the security, availability, and confidentiality categories set forth in *TSP 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus—2022)* in AICPA*, Trust Services Criteria*.

| | |
|---|---|
| **CC1.0 – Common Criteria Related to Control Environment** | |
| **CC1.1** | COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values. |
| **CC1.2** | COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control. |
| **CC1.3** | COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives. |
| **CC1.4** | COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives. |
| **CC1.5** | COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives. |
| **CC2.0 – Common Criteria Related to Communication and Information** | |
| **CC2.1** | COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control. |
| **CC2.2** | COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control. |
| **CC2.3** | COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control. |
| **CC3.0 – Common Criteria Related to Risk Assessment** | |
| **CC3.1** | COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives. |
| **CC3.2** | COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed. |
| **CC3.3** | COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives. |
| **CC3.4** | COSO Principle 9: The entity identifies and assesses changes that could significantly impact the System of internal control. |
| **CC4.0 – Common Criteria Related to Monitoring Activities** | |
| **CC4.1** | COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning. |
| **CC4.2** | COSO Principle 17: The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate. |
| **CC5.0 – Common Criteria Related to Control Activities** | |
| **CC5.1** | COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels. |
| **CC5.2** | COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives. |

## AICPA TRUST SERVICES CATEGORIES AND CRITERIA (CONTINUED)

| CC5.0 – Common Criteria Related to Control Activities (Continued) | |
|---|---|
| **CC5.3** | COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action. |
| **CC6.0 – Common Criteria Related to Logical and Physical Access Controls** | |
| **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. |
| **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. |
| **CC6.4** | The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives. |
| **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. |
| **CC6.8** | The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives. |
| **CC7.0 – Common Criteria Related to System Operations** | |
| **CC7.1** | To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities. |
| **CC7.2** | The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events. |
| **CC7.3** | The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures. |
| **CC7.4** | The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate. |
| **CC7.5** | The entity identifies, develops, and implements activities to recover from identified security incidents. |
| **CC8.0 – Common Criteria Related to Change Management** | |
| **CC8.1** | The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives. |

## AICPA TRUST SERVICES CATEGORIES AND CRITERIA (CONTINUED)

| | |
|---|---|
| **CC9.0 – Common Criteria Related to Risk Mitigation** | |
| **CC9.1** | The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions. |
| **CC9.2** | The entity assesses and manages risks associated with vendors and business partners. |
| **Additional Criteria for Availability** | |
| **A1.1** | The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives. |
| **A1.2** | The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives. |
| **A1.3** | The entity tests recovery plan procedures supporting system recovery to meet its objectives. |
| **Additional Criteria for Confidentiality** | |
| **C1.1** | The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality. |
| **C1.2** | The entity disposes of confidential information to meet the entity's objectives related to confidentiality. |

# ATTACHMENT B

## Principal Service Commitments and System Requirements

## PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

The Company makes service commitments to its customers through agreements such as the Company's Terms of Service, included in customer contracts, and in the description of the service offering provided online. Some of these commitments are principal to the performance of the Platform and relate to the applicable Trust Services Criteria (TSC).

The Company is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the Platform to provide reasonable assurance that the service commitments and system requirements are achieved. The Company has compiled a set of policies and procedures to help ensure security, availability, and confidentiality commitments can be met. These commitments include the following:

- Data encryption over Transport Layer Security (TLS) connections.
- Production cloud infrastructure hosted within multiple availability zones.
- Regular security audits and penetration testing of the Platform.
- Implement industry-standard business continuity and disaster recovery plans.
- Disaster recovery plans are maintained and reviewed at least annually.