

# **Report on Nutanix, Inc.'s Nutanix Cloud Clusters (NC2) on Google Cloud System Relevant to Security, Availability, and Confidentiality Throughout the Period December 9, 2025 to May 31, 2026**

SOC 3® - SOC for Service Organizations: Trust Services Criteria for General Use Report

# NUTANIX

## **Disclosure Statement:**

This document contains confidential and proprietary information of both Nutanix, Inc. and Coalfire Controls, LLC.

© 2026 Coalfire Controls, LLC. All rights reserved.

# Table of Contents

Section 1

Independent Service Auditor's Report ..... 3

Section 2

Assertion of Nutanix, Inc. Management..... 6

Attachment A

Nutanix, Inc.'s Description of the Boundaries of Its Nutanix Cloud Clusters (NC2) on Google Cloud System ..... 8

Attachment B

Principal Service Commitments and System Requirements ..... 17

# **Section 1**

## **Independent Service Auditor's Report**

## **Independent Service Auditor's Report**

To: Nutanix, Inc. ("Nutanix")

### **Scope**

We have examined Nutanix's accompanying assertion titled "Assertion of Nutanix, Inc. Management" (assertion) that the controls within the Nutanix Cloud Clusters (NC2) on Google Cloud System (system) were effective throughout the period December 9, 2025 to May 31, 2026, to provide reasonable assurance that Nutanix'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*.

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

Nutanix uses subservice organizations to provide Infrastructure-as-a-Service (IaaS), data transmission protection and sign-on services. The description of the boundaries of the system indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Nutanix, to achieve Nutanix's service commitments and system requirements based on the applicable trust services criteria. The description of the boundaries of the system presents the types of complementary subservice organization controls assumed in the design of Nutanix's controls. Our examination did not include the services provided by the subservice organizations, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

### **Service Organization's Responsibilities**

Nutanix 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 Nutanix's service commitments and system requirements were achieved. Nutanix has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, Nutanix 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 Nutanix'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 Nutanix'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 NC2 on Google Cloud System were effective throughout the period December 9, 2025 to May 31, 2026, to provide reasonable assurance that Nutanix's service commitments and system requirements were achieved based on the applicable trust services criteria if complementary subservice organization controls and complementary user entity controls assumed in the design of Nutanix's controls operated effectively throughout that period is fairly stated, in all material respects.

*Coalfire Controls LLC*

Louisville, Colorado  
August 31, 2026

## **Section 2**

# **Assertion of Nutanix, Inc. Management**

## Assertion of Nutanix, Inc. (“Nutanix”) Management

We are responsible for designing, implementing, operating and maintaining effective controls within the Nutanix Cloud Clusters (NC2) on Google Cloud System (system) throughout the period December 9, 2025 to May 31, 2026, to provide reasonable assurance that Nutanix’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 system is presented in attachment A and identifies the aspects of the system covered by our assertion.

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

Nutanix uses subservice organizations for Infrastructure-as-a-Service (IaaS), data transmission protection and sign-on services. The description of the boundaries of the system indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Nutanix, to achieve Nutanix’s service commitments and system requirements based on the applicable trust services criteria. The description of the boundaries of the system presents the types of complementary subservice organization controls assumed in the design of Nutanix’s controls. The description of the boundaries of the system does not disclose the actual controls at the subservice organizations.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period December 9, 2025 to May 31, 2026, to provide reasonable assurance that Nutanix’s service commitments and system requirements were achieved based on the applicable trust services criteria if complementary subservice organization controls and complementary user entity controls assumed in the design of Nutanix’s controls operated effectively throughout that period. Nutanix’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 December 9, 2025 to May 31, 2026, to provide reasonable assurance that Nutanix’s service commitments and system requirements were achieved based on the applicable trust services criteria.

Nutanix, Inc.

# **Attachment A**

## **Nutanix, Inc.'s Description of the Boundaries of Its Nutanix Cloud Clusters (NC2) on Google Cloud System**

# Type of Services Provided

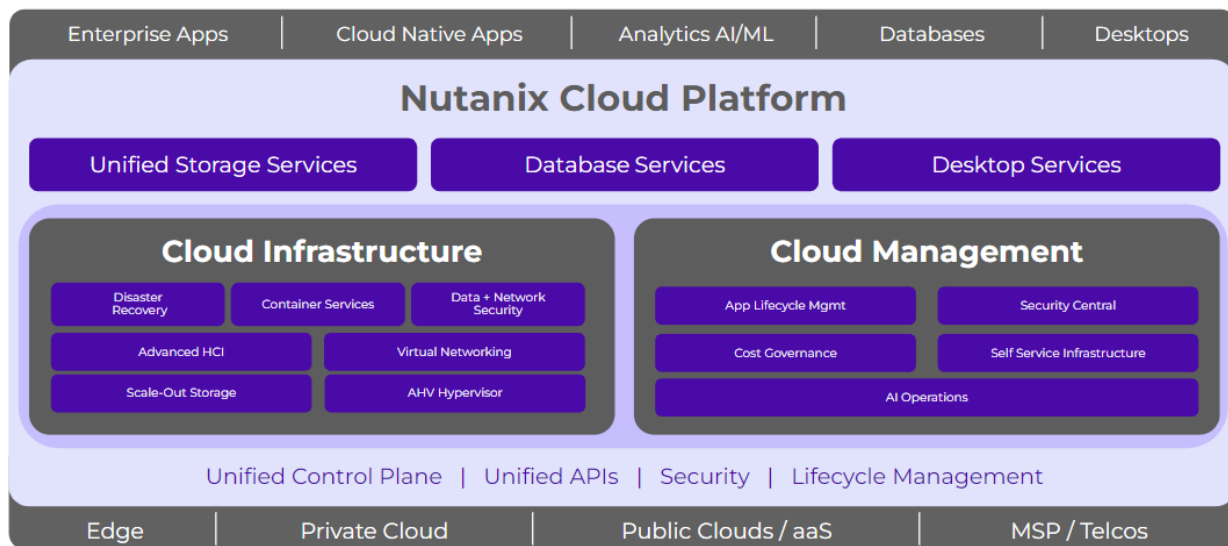
## Company Background

Nutanix, Inc. (“Nutanix” or “the Company”) provides a multi-cloud platform, called the Nutanix Cloud Platform™, that consists of software solutions and cloud services that power a customer’s IT infrastructure. Nutanix’s solutions are designed to deliver a consistent cloud operating model across edge, private-, hybrid-, and multi-cloud environments for applications and data. Nutanix’s solutions allow organizations to move their workloads, including enterprise applications, high-performance databases, container-based modern applications, and analytics applications, between on-premises and public clouds.

## Services Provided

### Nutanix Cloud Platform

Nutanix Cloud Platform provides management capabilities for scalable private, public, and distributed cloud operating environments.



### Nutanix Cloud Services

The Nutanix Cloud Services provide a native extension to the Nutanix Cloud Platform’s core infrastructure services, delivering integrated public cloud operations that can be quickly provisioned and automatically configured. The Nutanix Cloud Services include Nutanix Cloud Clusters (NC2)™ on Amazon Web Services (AWS), Nutanix Cloud Clusters (NC2)™ on Microsoft Azure (“Azure”), Nutanix Cloud Clusters (NC2)™ on Google Cloud™, Nutanix Insights™, Nutanix Data Lens™, NCM Cost Governance™, NCM Security Central™, and Nutanix Central™. The suite of Nutanix Cloud Services is summarized below.

- NC2 on AWS: NC2 on AWS is a hybrid multi-cloud platform with native networking integration to AWS public clouds to enable organizations to benefit from the flexibility, simplicity, and cost efficiency of running applications in private or public clouds.
- NC2 on Azure: NC2 on Azure is a hybrid multi-cloud platform with native networking integration to Azure public clouds to enable organizations to benefit from the flexibility, simplicity, and cost efficiency of running applications in private or public clouds.

- **NC2 on Google Cloud:** NC2 on Google Cloud is a hybrid multi-cloud platform with native networking integration to Google Cloud public clouds to enable organizations to benefit from the flexibility, simplicity, and cost efficiency of running applications in private or public clouds.
- **Nutanix Insights:** Nutanix Insights is a predictive health and automated support offering that enables support automation for the IT administrator, facilitating simplification of support ticket management.
- **Nutanix Data Lens:** Nutanix Data Lens provides a cloud-hosted analytics and monitoring service for Nutanix Files file servers. Nutanix Data Lens functions on a global level, in a cluster-neutral environment, without being tied to a single Nutanix cluster.
- **NCM Cost Governance:** NCM Cost Governance is a multi-cloud optimization service that provides organizations with deep visibility and rich analytics detailing cloud consumption patterns. NCM Cost Governance delivers one-click cost optimization across a cloud environment.
- **NCM Security Central:** NCM Security Central is a Nutanix multi-cloud governance service that provides organizations with visibility, optimization, and automated control needed to enforce cloud governance controls across the Nutanix Cloud Platform core infrastructure. NCM Security Central enables customers to directly enforce policies that improve cloud security from a single “pane of glass.”
- **Nutanix Central:** Nutanix Central gives customers a cloud operating model to unify their experience and view and manage their Nutanix Cloud Platform and Nutanix services deployed on-premises and in the public cloud via NC2.

The boundaries of the system in this section details the NC2 on Google Cloud System. Any other Company services including on-premises and hybrid-cloud services are not within the scope of this report.

## **The Boundaries of the System Used to Provide the Services**

The boundaries of the NC2 on Google Cloud System 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 NC2 on Google Cloud System.

The components that directly support the services provided to customers are described in the subsections below.

### **Infrastructure**

The NC2 on Google Cloud System runs on AWS and Google Cloud infrastructure. The Company leverages the experience, technical capabilities, and resources of AWS and Google Cloud to scale quickly and securely as necessary to meet current and future demand. However, the Company is responsible for designing and configuring the NC2 on Google Cloud System architecture within AWS and Google Cloud to help ensure the availability, security, and confidentiality requirements are met.

## Software

The NC2 on Google Cloud System places the Nutanix Hyperconverged Infrastructure (HCI) stack, including the Nutanix Acropolis Operating System (AOS) capabilities directly on a customer-managed bare metal instance. This bare metal instance allows a Controller Virtual Machine (CVM) with Nutanix Acropolis Hypervisor (AHV) to run as the hypervisor.

AHV runs an embedded distributed network controller that integrates user VM networking with Google Cloud networking. AHV assigns user VM internet protocols (IPs) to the bare metal instance where VMs are running. The NC2 on Google Cloud System uses Flow Virtual Networking to create an overlay network that provides communication between workloads running in the cluster.

AOS is used to help ensure that virtual machines running on the bare metal instance have the capability to maintain the availability and performance specified in the documentation as defined in the Nutanix License and Service Agreement.

To use the NC2 on Google Cloud System, customers must have a my.nutanix account and the appropriate license entitlement to use the NC2 on Google Cloud System.

Customers use their my.nutanix account and license entitlements to log in and use the NC2 on Google Cloud System console to deploy a cluster in a Google Cloud VPC. The NC2 on Google Cloud System is supported on the bare metal instances from the following GCE families:

- Z3 family
- C4 family

The NC2 on Google Cloud System is only supported using the Nutanix AHV hypervisor.

## Other Supporting Software and Tools

The list of software and ancillary software also used to build, support, secure, maintain, and monitor the NC2 on Google Cloud System includes the following business functions:

- Sign-on solution
- Source code repository
- Vulnerability scanning
- Secure code development scanner
- System logging and monitoring
- Automated alerting and on-call paging services
- Configuration management tool
- Ticketing/tracking system
- System logging
- System monitoring
- Intelligent threat prevention and detection
- Automation/deployment
- Infrastructure deployment
- Distributed denial-of-service (DDoS) and data transmission protection solution
- End-point threat detection and response

## People

The Company develops, manages, and helps secure the NC2 on Google Cloud System via separate departments. The responsibilities of these departments are defined in the following table:

| People                               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|--------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Group/Role Name                      | Function                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Engineering and Technical Operations | Members of the Engineering and Technical Operations team are organized around product components and are responsible for product development, bug fixes, and operations support. They are also responsible for supporting the running platform instances, customer support, monitoring and alerting systems, internal automation and tools, and information security.                                                                                                                                                                                                                                                                                                        |
| Security and Compliance              | Security and Compliance teams are groups within the engineering organization dedicated to the building and operation of leveraged security services. These services serve to constantly assess, prevent, detect, and respond to attacks on Nutanix cloud services. In addition, the teams are responsible for defining and driving the security development life cycle, developing engineering-specific security training, performing threat-model reviews, coordinating penetration tests, and implementing or building security tools. The Compliance team manages security, availability, and confidentiality compliance efforts for Nutanix products and cloud services. |
| Business Operations                  | Business Operations is responsible for corporate IT, human resources (HR), sales, and finance activities. These responsibilities include employee additions, moves and changes, overall corporate security oversight, and customer billing.                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Customer Support                     | Nutanix Customer Support ( <a href="https://www.nutanix.com/support-services">https://www.nutanix.com/support-services</a> ) is a team of global support professionals who support Nutanix products and services, provide consulting services, and provide training and certification.                                                                                                                                                                                                                                                                                                                                                                                       |
| Engineering and Technical Operations | Members of the Engineering and Technical Operations team are organized around product components and are responsible for product development, bug fixes, and operations support. They are also responsible for supporting the running platform instances, customer support, monitoring and alerting systems, internal automation and tools, and information security.                                                                                                                                                                                                                                                                                                        |

## Procedures

Procedures include the automated and manual procedures involved in the operation of the NC2 on Google Cloud System. Procedures are developed and documented by the respective teams for a variety of processes, including those relating to product management, engineering, technical operations, security, information technology (IT), and HR. These procedures are drafted in alignment with the overall information security policies and are updated and approved as necessary for changes in the business, but no less than annually.

The following table details the procedures as they relate to the operation of the NC2 on Google Cloud System:

| Procedures                                                                |                                                                                                                                                                                                                     |
|---------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Procedure                                                                 | Description                                                                                                                                                                                                         |
| Nutanix Acceptable Use Policy and Mobile Device Policy                    | Outlines the acceptable use of computing resources and is applicable to Nutanix employees.                                                                                                                          |
| Information Security Management and Privacy Information Management Manual | Outlines how Nutanix manages and mitigates security risks to safeguard the confidentiality and availability of Nutanix information and technological assets.                                                        |
| Security Incident Management Policy                                       | Facilitates a consistent and effective approach to the management of information security incidents including communication on security weaknesses and events.                                                      |
| Systems Operation Policy                                                  | Outlines system operations requirements for Nutanix's computing resources.                                                                                                                                          |
| Access Control Policy                                                     | Provides guidance to relevant Nutanix personnel in configuring and implementing appropriate access controls for systems and services within the NC2 on Google Cloud environments.                                   |
| Change Management Policy                                                  | Provides guidance and methodology for change management practices, including, but not limited to, configuration changes made to the production systems, infrastructure, and applications.                           |
| Cryptographic Policy                                                      | Defines the requirements regarding the use of cryptographic protections for the assets of Nutanix's computing resources.                                                                                            |
| Security Awareness and Training Policy                                    | Establishes methodologies and processes to provide security awareness and training that help the workforce understand and adhere to Nutanix security practices to allow the organization to achieve security goals. |
| Nutanix Product Security Patch and Assurance Policy                       | Establishes standards and guidelines for security patch management.                                                                                                                                                 |
| Information Classification Policy                                         | Outlines the levels of information classification at Nutanix to protect the employee and Nutanix from unauthorized disclosure of information due to improper handling.                                              |
| Secure Logging and Log Management Standard                                | Establishes standards and guidelines for audit logging and log management.                                                                                                                                          |
| Technology Vendor Management Policy                                       | Outlines vendor management requirements and monitoring procedures for all third party vendors.                                                                                                                      |
| Nutanix Password Standard                                                 | Establishes the standards and guidelines for passwords and password configurations.                                                                                                                                 |

## Data

Data refers to transaction streams, files, data stores, tables, and output used or processed by the NC2 on Google Cloud System. Through the application programming interface (API), the customer or end-user defines and controls the data they load into and store in the NC2 on Google Cloud System production network. Once stored in the environment, the data is accessed remotely from customer systems via the Internet.

The Company has deployed secure methods and protocols for the transmission or storage of confidential or sensitive information over public networks. Encryption is enabled for data stored at rest.

The following table details the types of data contained in the production application for the NC2 on Google Cloud System:

| Data                                |                                                                                                                                                                        |
|-------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Data Type                           | Description                                                                                                                                                            |
| Administration sensitive data       | Secure Sockets Layer (SSL) certificates with private keys, data-at-rest encryption keys, SSH keys to the NC2 on Google Cloud System infrastructure, and auditing data. |
| System metadata and operations data | Customer IDs, VM names, role names, the NC2 on Google Cloud System cluster metadata, service logs, and system IP addresses.                                            |

### Access and Processing of Data in the Customer Environment

Data that is within customer applications and VM's hosted and residing within the Customer's bare metal AWS instance is not processed or accessed by the NC2 on Google Cloud System. Protection of customer data remains the responsibility of the customer.

## Complementary User Entity Controls (CUECs)

The Company's controls related to the NC2 on Google Cloud System cover only a portion of overall internal control for each user entity of the NC2 on Google Cloud System. It is not feasible for the service commitments, system requirements, and applicable criteria related to the system to be achieved solely by the Company. Therefore, each user entity's internal control should be evaluated in conjunction with the Company's controls, taking into account the related CUECs identified for the specific criterion. In order for user entities to rely on the controls reported herein, each user entity must evaluate its own internal control to determine whether the identified CUECs have been implemented and are operating effectively.

Because the NC2 on Google Cloud System does not access data within the customer environments, and protection of customer data remains the responsibility of the customer, the following CUECs should be designed, implemented, and operated by the customer to help ensure the data managed and controlled by the customer is safeguarded appropriately. These controls require significant security, availability, and confidentiality measures, in addition to the specific controls listed below.

The CUECs presented should not be regarded as a comprehensive list of all controls that should be employed by user entities. Management of user entities is responsible for the following:

| Criteria | Complementary User Entity Controls                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|----------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CC2.1    | <ul style="list-style-type: none"><li>• User entities have policies and procedures to report any material changes to their overall control environment that may adversely affect services being performed by the Company according to contractually specified time frames.</li><li>• Controls to provide reasonable assurance that the Company is notified of changes in:<ul style="list-style-type: none"><li>– User entity vendor security requirements</li><li>– The authorized users list</li></ul></li></ul> |

| Criteria                        | Complementary User Entity Controls                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|---------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| CC2.3                           | <ul style="list-style-type: none"> <li>It is the responsibility of the user entity to have policies and procedures to: <ul style="list-style-type: none"> <li>Inform their employees and users that their information or data is being used and stored by the Company.</li> <li>Determine how to file inquiries, complaints, and disputes to be passed on to the Company.</li> </ul> </li> <li>User entities have policies and procedures for communicating support requests to the Company in a timely manner.</li> <li>User entities have policies and procedures for ensuring that system administrators and other relevant users are enrolled to receive updates through the Company's website.</li> </ul> |
| CC6.1                           | <ul style="list-style-type: none"> <li>Controls to provide reasonable assurance that policies and procedures are deployed over user IDs and passwords that are used to access services provided by the Company.</li> <li>Default application administrator passwords should be changed upon initial setup of the application.</li> <li>Segregation of duties between user entity employees is maintained, and the concept of least privilege is maintained.</li> </ul>                                                                                                                                                                                                                                         |
| CC6.1<br>CC6.2                  | <ul style="list-style-type: none"> <li>User entities grant access to the Company's system to authorized and trained personnel.</li> <li>Controls should be established to ensure that appropriate and authorized access has been granted and is revoked in a timely manner.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                         |
| CC6.2<br>CC6.3                  | <ul style="list-style-type: none"> <li>Controls should determine that authorized users and their associated access privileges are reviewed periodically.</li> <li>User entities should ensure timely removal of user accounts for any users that have been terminated and were previously involved in any material functions or activities.</li> </ul>                                                                                                                                                                                                                                                                                                                                                         |
| CC6.4<br>CC6.5<br>CC7.2<br>A1.2 | <ul style="list-style-type: none"> <li>User entities have adequate physical security and environmental controls for all devices and access points residing at their operational facilities, including remote employees or at-home agents for which the user entity allows connectivity.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                             |
| CC6.6<br>CC6.7                  | <ul style="list-style-type: none"> <li>User entities should encrypt all data transmitted to the NC2 on Google Cloud System.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| C1.2                            | <ul style="list-style-type: none"> <li>User entities have policies and procedures in place to delete data that they control from the NC2 on Google Cloud System, upon expiration or no longer needed.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |

## Subservice Organizations and Complementary Subservice Organization Controls (CSOCs)

The Company uses GCP, AWS, Akamai, and Okta as subservice organizations for Infrastructure as a Service (IaaS), data transmission protection, and sign-on services, respectively.

In some instances, a service organization's controls cannot provide reasonable assurance that its service commitments and system requirements are achieved without the subservice organizations performing certain activities in a defined manner. Such activities are referred to as complementary subservice organization controls (CSOCs). The following CSOCs are those controls that Nutanix's management assumed, in the design of the system, would be implemented by a subservice organization and are necessary, in combination with controls at Nutanix, to provide reasonable assurance that the service organization's service commitments and system requirements are achieved.

Company management receives and reviews the subservice organization's SOC 2 reports annually. In addition, through its operational activities, Company management monitors the services performed by AWS, Akamai, and Okta to determine whether operations and controls expected to be implemented are functioning effectively. Management also communicates with the subservice organizations to monitor compliance with the service agreement, stay informed of changes planned at the hosting facility, and relay any issues or concerns to GCP, AWS, Akamai, and Okta management.

It is not feasible for the service commitments, system requirements, and applicable criteria related to the Platform to be achieved solely by the Company. Therefore, each user entity's internal control must be evaluated in conjunction with the Company's controls, taking into account the related CSOCs expected to be implemented at GCP, AWS, Akamai, and Okta as described below.

| Criteria                                                                                           | Complementary Subservice Organization Controls                                                                                                                                                                                                                                                                                                                               |
|----------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Akamai Technologies, Inc., Amazon Web Services, Inc., Google Cloud Platform, and Okta, Inc.</b> |                                                                                                                                                                                                                                                                                                                                                                              |
| CC4.1<br>CC4.2<br>CC7.1<br>CC7.2<br>CC7.3                                                          | <ul style="list-style-type: none"> <li>Responsible for having controls in place to identify potential threats that would impair the system and communicate those to Nutanix immediately.</li> </ul>                                                                                                                                                                          |
| CC6.1<br>C1.1                                                                                      | <ul style="list-style-type: none"> <li>Responsible for encrypting databases in their control at rest.</li> </ul>                                                                                                                                                                                                                                                             |
| CC6.1<br>CC6.2<br>CC6.3                                                                            | <ul style="list-style-type: none"> <li>Responsible for having controls in place to limit and restrict access to system-designated resources to only authorized personnel.</li> </ul>                                                                                                                                                                                         |
| CC6.4<br>CC6.5<br>C1.2                                                                             | <ul style="list-style-type: none"> <li>Responsible for having controls in place to limit and restrict access to facilities and physical infrastructure housing the system to only authorized personnel.</li> </ul>                                                                                                                                                           |
| CC9.1<br>A1.2                                                                                      | <ul style="list-style-type: none"> <li>Responsible for having controls in place to automate the recovery of production hosts when necessary to maintain the availability of the system.</li> </ul>                                                                                                                                                                           |
| CC7.2<br>A1.2                                                                                      | <ul style="list-style-type: none"> <li>Responsible for having environmental protections in place that include, but are not limited to: <ul style="list-style-type: none"> <li>Cooling systems</li> <li>Battery and generator backup in the event of power failure</li> <li>Smoke detectors</li> <li>Fire suppression systems</li> <li>Water detection</li> </ul> </li> </ul> |
| <b>Akamai Technologies, Inc.</b>                                                                   |                                                                                                                                                                                                                                                                                                                                                                              |
| CC6.7                                                                                              | <ul style="list-style-type: none"> <li>Responsible for having controls in place to encrypt the NC2 on Google Cloud System data in transit.</li> </ul>                                                                                                                                                                                                                        |

## **Attachment B**

# **Principal Service Commitments and System Requirements**

# Principal Service Commitments and System Requirements

Nutanix designs its processes and procedures related to the NC2 on Google Cloud System to meet its business objectives. These objectives are based on the service commitments that Nutanix makes to customers and other relevant user entities, and the operational and compliance requirements that Nutanix has established for the System. Service commitments to customers and other relevant user entities are documented and communicated in master agreements and supplemental terms agreements, as well as in the description of the service offering provided on Nutanix's website, in its marketing materials, and within its customer-facing web portal.

Nutanix formalizes the security, availability, and confidentiality service commitments in the Nutanix License and Service Agreement (NLSA), found at: <https://www.nutanix.com/legal/eula>, which incorporates support and service level agreements for the NC2 on Google Cloud System:

The Company's principal service commitments communicated via the NLSA include, but are not limited to, the following:

- The Company will maintain administrative, physical, and technical safeguards to protect the security, confidentiality, and integrity of customer data.
- The Company will notify the customer in writing upon becoming aware of an unauthorized use or disclosure of confidential information.
- The Company will make the NC2 on Google Cloud System available 99.9% of the time.
- The Company will provide technical support on a 24/7/365 basis with response target objectives varying by criticality.
- The Company will protect confidential information from unauthorized use, access, or disclosure in the same manner as it protects its own confidential or proprietary information of a similar nature and, in any event, with at least a reasonable degree of care.
- Upon termination of the NC2 on Google Cloud System services, customer data in the application, metadata, and data stored in data backups are deleted in accordance with contractual agreements.

Nutanix establishes operational and compliance requirements that support the achievement of security, availability, and confidentiality commitments, compliance with relevant laws and regulations, and compliance with other System design requirements. Such requirements are communicated via Nutanix's System policies and procedures, System design documentation, and governing terms with customers. Information security policies define an organization-wide approach to how systems and data are protected. These include policies around how the NC2 on Google Cloud System 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 to carry out specific manual and automated processes required for the ongoing development and operation of the NC2 on Google Cloud System.