Report on Nutanix, Inc.’s Nutanix Cloud Manager (NCM) Security Central System Relevant to Security, Availability, and Confidentiality Throughout the Period November 1, 2024 to May 31, 2025

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

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 Manager (NCM) Security Central 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 Manager (NCM) Security Central System were effective throughout the period November 1, 2024 to May 31, 2025, 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*.

Nutanix uses subservice organizations to provide infrastructure-as-a-service, 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 Nutanix Cloud Manager (NCM) Security Central System were effective throughout the period November 1, 2024 to May 31, 2025, 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 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
October 3, 2025

Section 2

Assertion of Nutanix, Inc. Management

NUTANIX

Assertion of Nutanix, Inc. ("Nutanix") Management

We are responsible for designing, implementing, operating and maintaining effective controls within the Nutanix Cloud Manager (NCM) Security Central System throughout the period November 1, 2024 to May 31, 2025, 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.

Nutanix uses subservice organizations for infrastructure-as-a-service, 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 November 1, 2024 to May 31, 2025, 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 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 November 1, 2024 to May 31, 2025, 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 Manager (NCM) Security Central System

Type of Services Provided

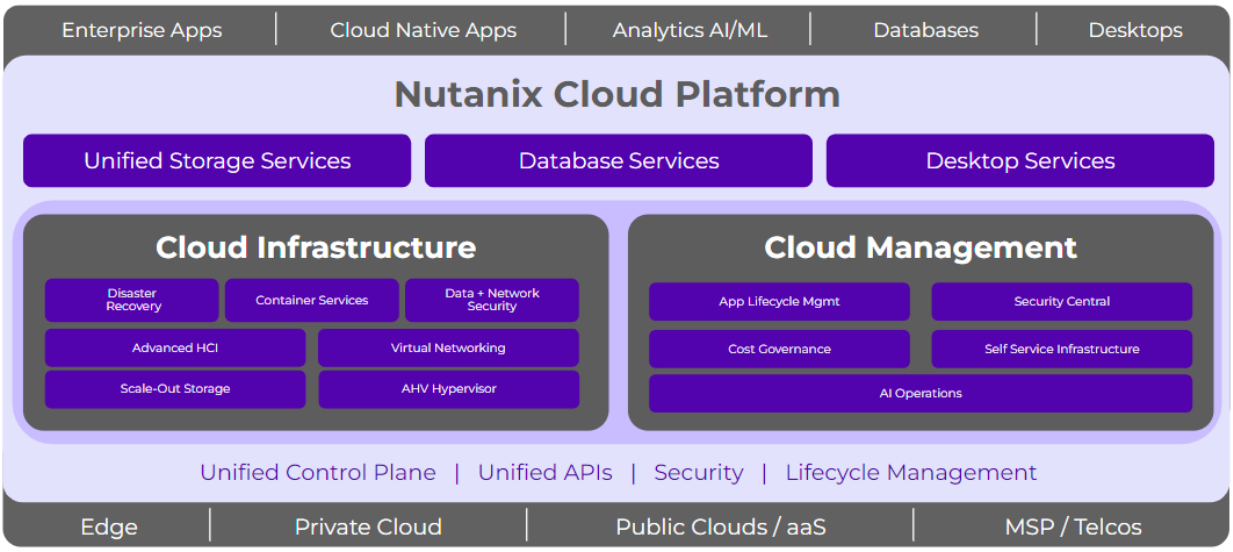
Company Background

Nutanix, Inc. (“Nutanix” or “the Company”) provides a 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 Enterprise Cloud combines private, public, and distributed cloud operating environments and provides a single point of control to manage IT infrastructure and applications at any scale.



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 Insights™, Nutanix Cloud Manager (NCM) Self-Service™, Nutanix Data Lens™, NCM Cost Governance™, NCM Security Central™(“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.

- 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.
- NCM Self-Service (formerly Calm): NCM Self-Service is a hosted application orchestration service that delivers infrastructure and application management for the IT administrator to manage the internal end user, providing the ability for the IT administrator to start, stop, and scale an application based on business requirements and internal end-roles.
- 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 (formerly Flow 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, AWS, and Azure. 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 NCM Security Central 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 NCM Security Central 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 NCM Security Central System.

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

Infrastructure

The NCM Security Central System production environment is deployed on AWS infrastructure in its own virtual private cloud (VPC), with access controls for network and application-level security, and is protected using a web application firewall service. The NCM Security Central System’s back-end services, such as databases and logs, are isolated into separate private networks for enhanced protection. Data sent to and from the NCM Security Central System is transmitted securely using Transport Layer Security (TLS) and Hypertext Transfer Protocol Secure (HTTPS). The NCM Security Central System customers are not required to open any custom ports from their network or cloud. The NCM Security Central System is secured with authentication, authorization, and tampering protection.

Software

Software consists of the programs and software that support the NCM Security Central System (operating systems [OSs], middleware, and utilities). The list of software and ancillary software used to build, support, secure, maintain, and monitor the NCM Security Central System includes the following business functions:

- In the NCM Security Central System, the engineers do not have persistent access to sensitive data or persistent access to perform high-risk operations. Teleport is the service that facilitates management's approval for requests of temporary privileged access.
- Among other purposes, the my.nutanix.com portal provides the NCM Security Central System customers with identity services, billing and payment services, and support infrastructure.
- A secrets (e.g., passwords, application programming interface (API) keys, certificates) management tool used to store sensitive credentials as well as to generate dynamic, short-lived credentials for entities such as AWS, Postgres, or public key infrastructure certificates. The sealing and unsealing mechanism is offloaded to the AWS Key Management Service (KMS). Communication among servers is over TLS requiring a vault token.
- An open-source agent that collects metrics across various domains and dimensions.
- Platforms that scan for security vulnerabilities in devices, applications, operating systems, cloud services, and other network resources. After every scan, they provide a report of vulnerabilities found and a summary on how to remediate or mitigate them.
- A threat prevention and detection service that continuously monitors for malicious activity and unauthorized behavior to protect AWS accounts and workloads.
- A threat prevention and detection service
- An internal, single pane that consume communications-platform-as-a-service (CPaaS) for management and access of Nutanix engineering teams. It provides modules with full-fledged Kubernetes support through which teams can manage their applications and workloads. It provides insights, auditing, alerting, and role-based access control (RBAC) for engineering teams and their resources. It also offers a software development kit (SDK), which is used to integrate Clutch with continuous integration/continuous delivery (CI/CD) pipelines and other use cases involving management of workloads. Besides Kubernetes, Clutch has modules for secrets management, scoped infrastructure access, approval systems for business processes, and export/import of resources across different setups.
- Sign-on solution
- Configuration management tool
- Container scheduling and orchestration
- Secure networking solution
- Microservices deployment
- Infrastructure deployment
- Long-term report storage
- Automated alerting service
- Ticketing/tracking system
- Asset management system
- Distributed denial-of-service (DDoS) and data transmission protection solution

- Automated alerting services
- Alerting service
- GitOps continuous delivery tool
- Kubernetes infra operations management
- Column-oriented, open-source, distributed data store
- All-in-one messaging and streaming platform
- Elasticsearch index management, backup, and restoration
- Manages pod restarts for changes in ConfigMap and secrets
- Search and analytics suite
- Database for orchestration platform
- Open-source workflow orchestration platform that maintains an application's state at scale and to ensure correctness regardless of point of failure
- Multi-platform, open-source analytics and interactive visualization web application that provides charts, graphs, and alerts for the web when connected to supported data sources
- System logging

People

The Company develops, manages, and secures the NCM Security Central 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, performing penetration tests, and 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 (https://www.nutanix.com/support-services) is a team of global support professionals who support Nutanix products and services, provide consulting services, and provide training and certification.

Procedures

Procedures include the automated and manual procedures involved in the operation of the NCM Security Central 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 NCM Security Central System:

Procedures	
Procedure	**Description**
Nutanix Acceptable Use Policy	Outlines the acceptable use of computing resources and is applicable to Nutanix employees and contractors.
Information Security Management and Privacy Information Management Manual	Outlines how Nutanix manages and mitigates security risks to safeguard the confidentiality, integrity 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 NCM Security Central 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.
Security Patch Management Procedure	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.

Data

Data refers to transaction streams, files, data stores, tables, and output used or processed by the Company. Through the API, the customer or end-user defines and controls the data they load into and store in the NCM Security Central 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 of confidential or sensitive information over public networks. Encryption is enabled for databases housing sensitive customer data.

The following table details the types of data contained in the production application for the NCM Security Central System:

Data	
Data Type	**Description**
Customer data	Customer backups, universal VMs, users and role membership, customer-owned security information (e.g., certificates, encryption keys, Secure Socket Shell [SSH] keys, user credentials).
Personally identifiable information (PII) and end-user identifiable information (EUII)	Customer names, email addresses, IP addresses that could identify an individual person, phone numbers, and physical addresses.
Administration sensitive data	Secure Sockets Layer (SSL) certificates with private keys, data-at-rest encryption keys, SSH keys to the NCM Security Central System infrastructure, and auditing data.
System metadata and operations data	Customer IDs, customer VM names, role names, the NCM Security Central System cluster information, service logs (not containing customer data, service configuration [without administration sensitive data]), IP addresses that only identify a company, or company address pool and not an individual person.

Access to Customer Data

The NCM Security Central System does not access customer data, and protection of customer data remains the responsibility of the customer. The NCM Security Central System accesses only the metadata of the customer's cloud accounts for the purpose of delivering the optimization service, and access to that metadata by the NCM Security Central System service is controlled by the customer.

User Entity Responsibilities

Management of user entities is responsible for the following, which should not be regarded as a comprehensive list of all controls that should be employed by user entities:

- 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.
- Controls to provide reasonable assurance that the Company is notified of changes in:
  - User entity vendor security requirements
  - The authorized users list

- It is the responsibility of the user entity to have policies and procedures to:
  - Inform their employees and users that their information or data is being used and stored by the Company.
  - Determine how to file inquiries, complaints, and disputes to be passed on to the Company.
- User entities grant access to the Company's system to authorized and trained personnel.
- 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.
- User entities deploy 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.

Subservice Organizations and Complementary Subservice Organization Controls (CSOCs)

The Company uses AWS, Akamai, and Okta as subservice organizations for IaaS, data transmission protection, and sign-on services, respectively. The Company's controls related to the NCM Security Central System cover only a portion of the overall internal control for each user entity of the NCM Security Central System.

Although the subservice organizations have been carved out for the purposes of this report, certain service commitments, system requirements, and applicable criteria are intended to be met by controls at the subservice organizations. CSOCs are expected to be in place at AWS, Akamai, and Okta related to physical security and environmental protection, as well as backup, recovery, and redundancy controls related to availability. AWS, Akamai, and Okta's physical security controls should mitigate the risk of unauthorized access to the hosting facilities. AWS, Akamai, and Okta's environmental protection controls should mitigate the risk of fires, power loss, climate, and temperature variabilities.

Company management receives and reviews the AWS, Akamai, and Okta SOC 2 report 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 facilities, and relay any issues or concerns to AWS, Akamai, or Okta management.

It is not feasible for the service commitments, system requirements, and applicable criteria related to the NCM Security Central System 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 AWS, Akamai, and Okta as described below.

Criteria	Complementary Subservice Organization Controls
CC4.1 CC4.2 CC7.1 CC7.2 CC7.3	• AWS, Akamai, and Okta should identify potential threats that would impair the system and communicate those to Nutanix immediately.

Criteria	Complementary Subservice Organization Controls
CC6.1 C1.1	• AWS, Akamai, and Okta should encrypt databases in their control at rest.
CC6.4	• AWS, Akamai, and Okta should restrict data center access to authorized personnel. • AWS, Akamai, and Okta should monitor data centers 24/7 by closed circuit cameras and security personnel.
CC6.5 CC6.7	• AWS should securely decommission and physically destroy production assets in their control.
CC9.1 A1.2	• AWS, Akamai, and Okta should automate the recovery of production hosts when necessary to maintain the availability of the system.
CC7.2 A1.2	• AWS, Akamai, and Okta should install fire suppression and detection and environmental monitoring systems at the data centers. • AWS, Akamai, and Okta should protect data centers against a disruption in power supply to the processing environment by an uninterruptible power supply (UPS). • AWS, Akamai, and Okta should oversee the regular maintenance of environmental protections at their data centers.

Attachment B

Principal Service Commitments and System Requirements

Principal Service Commitments and System Requirements

Nutanix designs its processes and procedures related to the NCM Security Central 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 Services Agreement (NLSA), found at: https://www.nutanix.com/legal/eula, which incorporates support and service level agreements for the NCM Security Central 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 NCM Security Central 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 NCM Security Central 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 NCM Security Central 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 NCM Security Central System.