Technical and Organizational Measures of Security (TOMs) for Nasuni File Data Platform

VERSION	5.0
DATED	28 February 2024
DOCUMENT AUTHOR	Jason Patterson
DOCUMENT OWNER	John Bilotti, CISO

Revision history

VERSION	DATE	REVISION AUTHOR	SUMMARY OF CHANGES	Approved
1.0	01March2017	JBilotti	Initial Release	Yes
2.0	01Apr2018	JBilotti	Updated for 2018-2019	Yes
3.0	26May2021	JPatterson	Updated for 2021-2022	Yes
4.0	17June2022	JPatterson	Updated for 2022-2023	Yes
5.0	28Feb2024	JPatterson	Updated for 2024-2025	Yes

NASUNI

Introduction

This document describes Technical and Organizational Measures of Security (TOMS) implemented by Nasuni to protect Protected Data and ensure the ongoing confidentiality, integrity and availability of Nasuni's File Data Platform.

Nasuni may change these measures from time to time. This may mean that individual measures are replaced by new measures that serve the same purpose or deal with the same risks without materially diminishing the security level.

Within this document, the following definitions apply:

- "Customer" means any purchaser of Nasuni solutions or services.
- The "File Data Platform" means the Software-As-A-Service provided by Nasuni to the Customer for the management of file data destined for cloud storage.
- "Protected Data" means sensitive corporate information and any protected personal data of Customers or contacts that Nasuni collects or stores as part of the delivery of Nasuni services.
- "Personnel" means Nasuni employees and Nasuni authorized independent contractors.
- "Nasuni" means Nasuni Corporation. When Nasuni Personnel or systems are referred to, this includes those of our affiliate companies.
- "Strong Encryption" means the use of industry standard encryption measures with sufficiently large keys, meeting or exceeding that defined by NIST standards.
- "NOC" means Nasuni Orchestration Center.
- "Cloud Provider" means a third-party contracted to deliver infrastructure, application, or software services via a collection of internet accessible managed data centers.
- "Production Data Center" means one or more third-party contracted enterprise cloud-based computer data centers, hosting the virtual private cloud environment where Nasuni's cloud services operate.

This document is a high-level overview of Nasuni's technical and organizational security measures. It is not intended to replace or govern Nasuni's written information security program.

1. Organization of Information Security

Objective

Nasuni has an information security function that is endorsed, supported, and empowered by business leadership, and Nasuni ensures that its personnel are competent in information security.

Measures

a) Nasuni employs personnel whose full-time responsibility is information security.
b) Nasuni encourages advanced training and certifications such as Certified Information Security Manager (CISM), Certificate of Cloud Security Knowledge (CCSK), and Certified Information Systems Security Professional (CISSP).
c) The Nasuni information security department reports directly to the Chief Financial Officer.
d) Nasuni has a comprehensive set of information security policies, approved by senior management and disseminated and reviewed by cross-functional personnel as appropriate.
e) Nasuni security policies are reviewed at least annually and updated as necessary.
f) All Nasuni personnel have signed legal reviewed confidentiality agreements that apply

during and post-employment with Nasuni.

g) Failure of personnel to follow information security policies can result in disciplinary actions up to and including dismissal.
h) All Nasuni personnel are provided monthly information security awareness training and must agree annually to the information security policies contained within the IT Acceptable Use Policy.
i) Information security is a fundamental design and architectural principle for all Nasuni Solutions.
j) Nasuni is committed to continual improvement of its security program.

2. Information Security Management System

Objective

Nasuni has a GRC (Governance, Risk and Compliance) system in place to evaluate risks to the security of Protected Data, to manage the assessment and treatment of these risks, and to continually improve its information security.

Measures

Nasuni has deployed an Information Security program to manage security professionally, and Nasuni continually aligns policies and procedures with industry standards, using control objectives defined by NIST, Cloud Security Alliance CCM, SOC 2 Type II, HIPAA, and ISO 27002:2013. Certification information can be accessed at trustcenter.nasuni.com

3. Physical Access

Objective

Physical access to Protected Data is protected.

Measures

a) Nasuni runs our File Data Platform from an SSAE 16 Certified, SOC Certified, CSA, and ISO 270xx Certified, professional, third-party Production Data Center with a defined and protected physical perimeter, strong physical controls including access control mechanisms, controlled delivery and loading areas, surveillance and 24x7x365 guards. Only authorized representatives of the Cloud Provider have access to the data center premises. Nasuni personnel do not have Physical Access. The compliance audit results are reviewed annually by Nasuni and are available under NDA for Customer review.
b) Power and telecommunications cabling carrying Protected Data or supporting information services at the Cloud Provider are protected from interception, interference, and damage.
c) The Production Data Center and its equipment are physically protected against natural disasters, malicious attacks, and accidents.
d) Equipment at the Production Data Center is protected from power failures and other disruptions caused by failures in supporting utilities and is correctly maintained.
e) Equipment or disk media containing Protected Data (including faulty or end of life disks) are not physically removed from the Production Data Center unless securely erased following NIST 800-88 guidelines prior to such removal or being transferred securely for destruction at a third-party site.

f) When Protected Data is copied electronically by Nasuni outside the Production Data Center, appropriate physical security is maintained, and the data is strongly encrypted at all times.

4. System Access

Objective

Nasuni data processing systems are used only by approved, authenticated users.

Measures

a) Access to Nasuni internal systems is granted only to Nasuni personnel and/or to permitted employees of Nasuni's sub-contractors. It is strictly limited as required for those persons to fulfill their function.
b) All users access Nasuni systems with a unique identifier (user ID).
c) Nasuni has established a multi-factor authentication policy that prohibits the sharing of passwords and requires passwords to be changed regularly and default passwords to be altered. All passwords must comply with defined minimum requirements and are encrypted.
d) Access to restricted online systems containing Protected Data requires a second authentication factor.
e) Nasuni has a thorough procedure to deactivate users and their access when a user leaves the company or a function.
f) An Intrusion Detection System (IDS) or Intrusion Prevention System (IPS) is deployed on the production Virtual Private Cloud (VPC) to help identify potential inappropriate access.
g) For Customer access to the solution, Nasuni provides a wide range of authentication capabilities, including the ability for Customers to set their own password policies and support for integration with directory services and the use of SSO with MFA for administrative access.

5. Data Access

Objective

Persons entitled to use data processing systems only gain access to the Protected Data they are authorized to access.

Measures

a) Nasuni restricts personnel access to restricted files on a least privileged access basis.
b) Personnel training covers access rights and general guidelines on the definition and use of Protected Data.
c) Where appropriate and practical, Nasuni employs data minimization and pseudonymizing to reduce the likelihood of inappropriate access to Protected Data.
d) The production environment for the Nasuni File Data Platform is separate from the development and testing environment, and access to the production environment is restricted to authorized NOC personnel.
e) Nasuni uses up-to-date anti-malware software on all appropriate computers and servers.
f) Nasuni uses well-configured firewalls to secure networks when Protected Data resides.
g)

Nasuni ensures that appropriate personnel receive alerts and notifications from system software vendors and other sources of security advisories and installs system software patches regularly and efficiently.

6. Data Transmission

Objective

Prevent Protected Data from being read, copied, altered or deleted by unauthorized parties during transfer.

Measures

a) Nasuni configures and uses Transport Layer Security (TLS) protocols for all website security where Protected Data is collected or stored.
b) Nasuni Data File Platform uses strong encryption, with support for large keys controlled by Customers prior to all transmission.
c) Nasuni's patented technologies further obfuscate Customer file data, in addition to strong encryption prior to being transmitted for cloud storage.

Note: The Customer is responsible for the security of Protected Data once it has been transmitted via Nasuni to the Customer, or Customer network, and anywhere a Nasuni Edge Appliance is deployed.

7. Confidentiality and Integrity

Objective

Protected Data remains confidential throughout processing and remains intact, complete and current during processing activities.

Measures

Nasuni has a defined and in-depth approach to ensuring confidentiality and integrity, many of the measures in other sections of this document safeguard confidentiality and integrity. Some measures that contribute include:

a) Nasuni has a formal background check procedure, which requires that all new personnel with access to Protected Data are verified prior to receiving access.
b) Nasuni trains and tests its software engineers and quality assurance personnel in application security best practices and secure coding practices.
c) Nasuni has a central, secured repository of product source code, which is accessible only to authorized personnel.
d) Nasuni has a formal product development process and uses a Secure Development Lifecycle (SDLC) that includes a wide range of security testing, flaw reporting and management procedures.
e) Testing includes code review and employing static code analysis tools on a periodic basis to

identify flaws.

f) All changes to software on the Service are via a controlled, approved release mechanism within a change control program that tracks, documents, tests, and approves change requests prior to implementation.

8. Availability

Objective

Protected Data is safeguarded from accidental destruction or loss, and there is timely access, restoration or availability to Protected Data in the event of an incident.

Measures include:

a) Nasuni uses a high level of redundancy in production operations so that an availability failure of a single system or component is unlikely to impact general availability.

b) The Production Data Centers utilized have multiple power supplies, generators on-site and include battery back-up to safeguard power availability to the data center systems.

c) The Production Data Center has multiple access points to the internet to safeguard connectivity.

d) The Production Data Center is monitored 24x7x365 for power, network, environmental and technical issues.

e) Nasuni uses commercially reasonable efforts to create frequent, encrypted back-up copies of Protected Data and these are stored in a geographically separate location.

f) Nasuni has a system in place to ensure that any failures of data retention are flagged and dealt with.

g) Nasuni performs restore tests from those backups at least quarterly.

h) Nasuni has a business continuity plan in place which is regularly updated.

i) Nasuni tests elements of its business continuity plan regularly and learns from the results of such tests.

9. Job Control

Objective

Protected Data processed on a Customer's behalf is processed solely in accordance with the relevant agreement and related instructions of the Customer, which includes the use of sub-processors.

Measures

a) Nasuni acts as data processor with respect to Protected Data and stores and processes Protected Data in order to operate the File Data Platform under instructions of the Customer within the scope of the File Data Platform.

b) Nasuni does not access Customer Protected Data, except to provide services to the Customer which Nasuni is obligated to perform in support of the Customer experience. This includes general operation and monitoring of the File Data Platform, for troubleshooting and maintenance purposes, for security reasons, as required by law, or on request by the Customer.

c) Nasuni uses a limited number of sub-processors to help it provide the File Data Platform. Additional information about third-party companies used as processors can be found at www.nasuni.com/legal/privacy.
d) Nasuni has contracts in place directly with all sub-processors that provide for confidentiality of Protected Data as well as agreements incorporating the EU Standard Contractual Clauses that process relevant Protected Data outside of the European Economic Area.

10. Data Separation

Objective

Protected Data collected for different purposes is processed separately.

Measures

a) Nasuni uses a multi-tenant architecture to achieve logical separation of Protected Data originating from multiple Customers.
b) In each step of the processing, Protected Data received from different Customers can be identified so data is always physically or logically separated.
c) Customers have access only to their own Protected Data.
d) Audit rights given to Customers always exclude the right or ability to look at the data of other Nasuni Customers.

11. Incident Management

Objective

In the event of any security breach of Protected Data, the effect of the breach is minimized, and the Customer is promptly informed.

Measures

a) Nasuni maintains an up-to-date incident response plan that includes responsibilities, how information security events are assessed and classified as incidents, and response plans and procedures.
b) Nasuni logs administrator and user activities at the Production Data Center to provide evidence in the event of an incident.
c) The clocks of all systems at the Production Data Center are synchronized to a single reference time source to aid investigation in the event of an incident.
d) Nasuni regularly tests its incident response plan with “table-top” exercises and learns from tests and potential incidents to improve the plan.
e) In the event of a security breach, Nasuni will notify Customers without undue delay after becoming aware of the security breach.

12. Compliance

Objective

Nasuni tests, assesses and evaluates the effectiveness of these technical and organizational measures.

Measures

a) Nasuni conducts regular internal audits of its security.
b) Nasuni has a formal policy for managing suppliers who have access to Protected Data. This includes criteria for reviewing and approving suppliers, appropriate contractual commitments, and procedures for monitoring and reviewing their performance.
c) Nasuni takes reasonable steps to ensure that personnel are aware of and comply with the technical and organizational measures set forth in this document.