Information Security Policy - Public

Updated August 2026

Table of Contents

1. **Objective 3**
2. **About Information 4**
   - 2.1 Information Security 4
     - 2.1.1 Definition of Information Security 4
     - 2.1.2 Information Security Domains 5
3. **Technical Organizational Measures (TOMs) 7**
   - 3.1 Identity & Access Management (IAM) 7
   - 3.2 Privileged Account Management (PAM) 7
   - 3.3 Authentication & Passwords 7
   - 3.4 Network Access and Network Controls 7
   - 3.5 SaaS, PaaS, IaaS 7
   - 3.6 Cryptography & Encryption 7
   - 3.7 Incident Management 8
   - 3.8 Business Continuity/Disaster Recovery 8
   - 3.9 Change Management 8
   - 3.10 Training, Awareness & Communications 8
   - 3.11 Joiners Movers Leavers Management 8
   - 3.12 Internal Controls & Audit 8
   - 3.13 Risk Management 9
   - 3.14 Vendor Management 9
   - 3.15 Physical & Environmental Security 9
   - 3.16 Equipment & Asset Security 9
   - 3.17 Secure Software Development Life Cycle (SSDLC) 9
4. **Further Information 10**

1. Objective

The Information Security Policy of Nitro is designed to establish management direction on what Nitro and its affiliates shall do with regards to Information security. The policy lays the foundation for Nitro's information security and how information security enables the business of Nitro.

The protection of information is the main purpose of information security, which is achieved by implementing a suitable set of controls, including organizational structures, policies and procedures, processes and technical IT controls. These controls need to be designed, implemented, monitored, reviewed and improved to ensure that the information assets of Nitro and its affiliates, its partners or customers are secure at all times.

2. About Information

2.1 Information Security

2.1.1 Definition of Information Security

Information security concerns the protection of information and the associated corporate assets against unauthorized access, modification or destruction.

Information is a critical business asset. It is of vital importance to Nitro and our customers. It can exist in several different forms:

- Physical: for example, printed or written on paper
- Electronic: for example, stored electronically on IT systems or transmitted via IT networks
- Human: for example, information known to employees or spoken in a conversation

Nitro Information Security is concerned with the Confidentiality, Integrity and Availability of Nitro information in all its forms.

Information security therefore concerns the protection of information assets against accidental or intentional breaches of:

- **Confidentiality:** To ensure that only authorized users have access to information assets
- **Integrity:** To ensure the accuracy and completeness of information assets
- **Authenticity:** To ensure the person's identity is maintained; that they are who they say they are
- **Availability:** To ensure that authorized users have access to information assets when required

Information security is achieved by implementing a suitable set of controls, including organizational structures, policies and procedures, processes and technical IT controls. These controls need to be designed, implemented, monitored, reviewed and improved. This is the accountability of Nitro's management.

2.1.2 Information Security Domains

At the highest level, Information Security can be divided into the following four domains:

- **Information Security Governance**: Information security governance is the combination of information security processes and structures implemented by Nitro management to inform, direct, manage and monitor the information security activities of the organization towards the achievement of its information security objectives.
- **Information Risk Management:** Information risk management encompasses the establishment of information security controls for the protection of Nitro's information regardless of the form or source of that information. The establishment of information security controls is based on a risk-based approach that uses the criticality of information with regards to the previously defined information security dimensions (i.e., confidentiality, integrity and availability) to select the required information security controls. This process is known as information classification. Information risk management also encompasses the implementation of a number of transversal security control domains such as human resources security, information security incident management, business continuity management and compliance.
- **Physical Security:** Physical security encompasses the establishment and implementation of physical security controls for all physical premises of Nitro such as office spaces, archives, technical rooms and data centers. The objective of physical security is to ensure the protection of information assets contained in the physical premises against unauthorized access, modification or destruction.
- **IT Security:** IT Security encompasses the establishment and implementation of IT security controls for information in electronic form that is processed, stored or transmitted on IT infrastructure created or managed by Nitro. The IT security controls can be technical IT controls, organizational IT controls as well as IT control processes. Their purpose is to avoid unauthorized access, modification or destruction of information situated on IT systems.

3. Technical Organizational Measures (TOMs)

Technical organizations measures are technical measures implemented within Nitro for safeguarding of the highest protection goals – Confidentiality, Integrity, Authenticity, Availability and Resilience.

3.1 Identity & Access Management (IAM)

To The principle of “Confidentiality” is primarily implemented by controlling access to information. Access Management allows Nitro to control ‘who’ accesses ‘what’ information ‘when’ and ‘how’.

3.2 Privileged Account Management (PAM)

Allocation and use of privileges is restricted and controlled.

3.3 Authentication & Passwords

In order to access anything within Nitro, a user is authorized and authenticated against the system. SSO is enforced and authentication can be a combination of multi-factor options available.

3.4 Network Access and Network Controls

Network perimeter security controls access to the Nitro network to allow only authorized users access to applications, data and services running on the network.

3.5 SaaS, PaaS, IaaS

Nitro uses a combination of SaaS, PaaS and IaaS resources and the shared security model of the providers to ensure security measures are appropriately implemented.

3.6 Cryptography & Encryption

Nitro enables and ensures protection of data during its transmission and at rest by using several mechanisms:

- Password protection
- Cryptographic modules

- Secrets and Keys

3.7 Incident Management

An Information Security Incident means any incident that occurs by accident or deliberately, and that impacts Nitro's communications or information processing systems. An incident may be any event or set of circumstances that threatens the confidentiality, integrity or availability of information, data or services at Nitro.

3.8 Business Continuity/Disaster Recovery

Important data is regularly saved in a backup system and synchronized to an external location according to defined schedules (Cloud backup). Backups are encrypted at rest and in transit.

Disaster recovery at Nitro is a method of regaining access and functionality to its IT infrastructure after events like a natural disaster, cyber-attack, or even business disruptions. Nitro's disaster recovery relies upon the replication of data and computer processing in an off-premises location not affected by the disaster.

3.9 Change Management

Change management is a systematic approach to dealing with the transition or transformation of Nitro's goals, solutions/products, processes or technologies. It allows Nitro to implement strategies for effecting change, controlling change and helping people to adapt to change. Any change that impacts solutions, technologies used, network, and IT at Nitro are tracked through RFC processes.

3.10 Training, Awareness & Communications

Training and awareness within Nitro is staggered and implemented at several levels – onboarding, annual and ad-hoc, as part of external audit, when a security incident occurs, etc.

- All new hires are required to join onboarding security and privacy training
- All employees undergo annual security and privacy training
- Department or role specific training is ad-hoc

3.11 Joiners Movers Leavers Management

The People team at Nitro manages the people resources as they join the organization, change roles or leave Nitro.

3.12 Internal Controls & Audit

Common controls framework is implemented to audit the effectiveness and efficiency of security solutions, services and processes.

3.13 Risk Management

Nitro keeps track of security and privacy risks of its solutions, services and processes by performing periodic vulnerability scanning, penetration testing, bug bounty, common controls framework, etc.

3.14 Vendor Management

Procurement of services from vendors is managed managed and assessed as part of third-party risk management process.

3.15 Physical & Environmental Security

Access to Nitro resources is protected by physical and environmental security measures that prevent physical tampering, damage, theft, or unauthorized physical access.

3.16 Equipment & Asset Security

Physical equipment and assets are managed, maintained and secured according to the agreed internal policy.

3.17 Secure Software Development Life Cycle (SSDLC)

Nitro's engineering and development broadly incorporates practices recommended in the NIST SSDLC Framework, OWASP Top 10, and other industry-standard secure software development frameworks.

4. Further Information

Nitro maintains a public Trust Centre where the current status of our certifications, control coverage and infrastructure is published and kept up to date. For more details, visit the links below:

Trust Centre overview - gonitro.com/security-compliance
Our overall approach to security, compliance and trust.

Compliance and certifications - gonitro.com/security-compliance/compliance
Independent third-party audits and certifications, including ISO 27001:2022, SOC 2 Type 2, HIPAA, QTSP accreditation under eIDAS, and the EU–U.S. Data Privacy Framework. Includes a per-product breakdown of control coverage - identity management, encryption, incident response, business continuity and secure development - and the cloud providers and regions hosting each solution.

Security - gonitro.com/security-compliance/security
Our information security statement, data centre security, and the technical and organisational measures protecting Nitro products and infrastructure.

Responsible disclosure - gonitro.com/security-compliance/security/responsible-disclosure
How to report a suspected vulnerability, and our programme for recognising qualifying reports.

Legal and eSignature validity - gonitro.com/security-compliance/legal
Compliance of Nitro Sign with electronic signature law, including eIDAS, the ESIGN Act, UETA, ZertES, and Singapore and Hong Kong requirements.

Artificial intelligence - gonitro.com/security-compliance/artificial-intelligence
How security and privacy are built into Nitro's AI features, including our position on the use of customer data for model training.

ESG policies - gonitro.com/security-compliance/esg
Our environmental, social and governance commitments.

Customers requiring further documentation, certification evidence or completed assessments can request these directly from Nitro at security@gonitro.com

© 2025 Nitro Software, Inc. All rights reserved.