INFORMATION SECURITY POLICY

Author	Ira Goel, Filip Verreth
Approver	Dave Lenoe
Created Date	March 10, 2022
Approved Date	April 04, 2022
Status	**APPROVED**
Version	**1.01**
Classification	**PUBLIC**

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 Security

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.

Figure 1 - Information Security Dimensions

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:

Figure 2 - Information Security 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.

2.2 Privacy and Data Protection

The protection of personal data is generally referred to as the protection of individuals' privacy. This document establishes applicable guidelines with regards to handling of private information, generally referred to as Personal Data Protection.

2.2.1 What constitutes Personal Data

Personal data means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

2.2.2 What is Data Controller

The Data Controller is the organization that, alone or jointly with others, determines the purposes and means of the processing of personal data.

The term “jointly” is used where two or more organizations act together to decide the purpose and manner of any data processing – for example, a network of town-center CCTV cameras is operated by a local council jointly with the police. Both are involved in deciding how the CCTV system is run and what the images it captures are used for.

2.2.3 What is Data Processor

The Data Processor is any organization that processes personal data on behalf of the controller. This can be any third party involved in the processing of the information, including but not limited to the storage of the information, hosting of supporting information systems, management of the applications used to process the information, or execution of the information processing itself.

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)

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. 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 our 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 – annual and ad-hoc, as part of external audit, when a security incident occurs, etc.

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 IT risks to the security of its solutions, services and processes in several ways such as vulnerability scanning, penetration testing, bug bounty, common controls framework, etc.

3.14 Vendor Management

Vendors are managed and assessed as part of the CAB and TAB process for Nitro's Tech Stack Governance.

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.

4. Document History

Date	Version	Update History
April 04, 2022	V1.0	First version approved
April 10, 2022	V1.1	Minor typo update