Proud Nerds
Information Security Policy

Reference:	20231122PNMG - Proud Nerds - Information Security Policy – External - V1.1
Date:	November 22nd, 2023
Version:	1.1
Classification:	Public

Introduction

This information security policy outlines the policy concerning the security of information. Information provision is crucial for the continuity of Proud Nerds. In our daily operations, whether on paper or in digital form, we depend on the availability, integrity, and confidentiality of information.

The management of Proud Nerds aims, through this policy, to deliver secure and reliable services, instilling trust in our customers and employees by safeguarding information and personal data against internal and external threats, both intentional and unintentional. These threats could potentially harm the continuity and reputation of the company and our customers or result in financial losses.

Our information security focuses on the following four aspects:

- **Availability**: Information must be available at the required times.
- **Integrity**: Information must be accurate and complete, and information systems must store and process accurate and complete information.
- **Confidentiality**: Information must only be accessible to those authorized to access it.
- **Privacy**: Protecting personal data and the rights of individuals involved.

To give substance to this and make it demonstrable for everyone, our Information Security Management System (ISMS) is certified according to the ISO-27001:2023 and NEN 7510:2020 standards. Our aim is to at least comply with applicable legislation and the ISO-27001:2023 and NEN 7510:2020 standards. Additionally, we aspire to safeguard the interests of our internal and external stakeholders.

Responsibility for Information Security Policy

The executive management holds ultimate responsibility for the information security policy and has established this policy. Both the executive management and the Security & Privacy Officer are responsible for maintaining the information security policy. The information security policy is periodically reviewed for accuracy, adequacy, and effectiveness, or whenever significant changes occur. Adjustments are made as necessary. Changes may arise due to shifts in the organizational context, risk analysis, legal and regulatory developments, outcomes of internal and external audits, management reviews, and other factors.

Continuous Improvement

Continuous improvement is crucial for Proud Nerds and our information security. This is ensured by working in a structured manner through the PDCA cycle of Deming. This model is used to establish, implement, monitor, control, and maintain the Information Security Management System (ISMS). The steps are briefly explained below:

Plan:
In the design phase, an information security policy is developed and established. This document outlines information security objectives, relevant processes, and procedures that ensure the management of risks. These objectives must always support the business goals of the organization.

Do:
In this phase, the implementation of the information security policy and underlying procedures and controls is ensured. Responsible parties are designated for each information system and/or process.

Check:
In this phase, internal audits are conducted to check and, where possible, measure whether the information security policy and supporting procedures are being executed correctly.

Act:
In this final phase, corrective and preventive actions are taken based on the results of internal audits, and if necessary, the ISMS is updated. Through this structured approach, information security is systematically and process-oriented, in a controllable manner.

This structured approach ensures a systematic, process-oriented, and controllable implementation of information security.

Definition of Information Security:

Proud Nerds adheres to the following definition of Information Security:

> *"The cohesive set of measures aimed at sustainably ensuring an optimal level of availability, integrity, and confidentiality of information and information systems."*

It is important to note that information security encompasses an integrated system of measures. This means that the various measures forming information security are not independent but interconnected.

The system of security measures aims to achieve a sustained level of security. Through careful assurance, it is guaranteed that the desired security level is maintained in the long term.

Information security strives to achieve an optimal security level. This optimal level is reached through a careful consideration of costs and benefits.

Objectives of our Information Security Policy:

The primary objective of Proud Nerds' information security policy is to ensure the continuity of business operations, provide secure and reliable services, and prevent incidents and resulting damages (social, reputational, financial, or otherwise). Additionally, it aims to instil confidence in customers and employees that potential risks are adequately managed.

The policy adheres to the following points:

- The information security policy is outlined and promoted by the management of Proud Nerds.
- The information security policy applies to all (external) employees of Proud Nerds.
- The foundation for the information security policy management system is ISO27001:2023 and NEN7510:2020. This allows the operation of this management system to be verified and confirmed by independent parties.
- The information security policy provides the basis for compliance with applicable laws and regulations.
- Measures arising from the information security policy are periodically assessed for effectiveness.

Security Objectives:

Our information security focuses on the following four aspects:

- **Availability**: Information must be available at the desired moments.
- **Integrity**: Information must be accurate and complete, and information systems must store and process accurate and complete information.
- **Confidentiality**: Information must only be accessible to those authorized to access it.
- **Privacy**: Protecting personal data and the rights of the individuals involved.

Concrete information security objectives are included in the ISMS (Information Security Management System).

Scope of the ISMS:

The scope of the ISMS (Information Security Management System) includes all internal processes and information systems of all organizational units of Proud Nerds. It encompasses the following activities:

- Designing, developing, managing, and hosting web and software applications, e-commerce environments, and apps.
- Designing, developing, and offering SaaS (Software as a Service).
- Establishing, delivering, and managing IT infrastructure and cloud solutions.

This scope applies to both ISO 27001:2023 and NEN7510:2020. The individual norm elements that are applicable are described in the Statement of Applicability for ISO 27001:2023 and the Statement of Applicability for NEN7510:2020.

Explanation of the scope:

All activities are carried out from Proud Nerds' registered address. Our service portfolio includes several activities for which we engage partners. Proud Nerds has outsourced the following relevant activities to suppliers:

- Surveillance services.
- Conducting security monitoring and periodic penetration tests.
- Hosting and data centers.
- ICT services related to network and connectivity, server and storage capacity, and end-user computing.

With these suppliers, Proud Nerds has, depending on the services provided, made contractual agreements regarding information security and privacy. If personal data is processed, these agreements are supplemented with a Data Processing Agreement.

Supporting Documentation:

To support this information security policy, the following supporting procedures and policy documents have been developed:

1. Policy for mobile devices and telecommuting
2. Screening policy
3. Information classification

4. Access security policy
5. Password policy
6. Policy on the use of cryptographic controls
7. Clear desk and clear screen policy
8. Backup policy
9. Information transport policy
10. Secure development policy
11. On- and offboarding policy
12. Information security policy for supplier relationships
13. Reporting (information) security incidents
14. Business Continuity Plan
15. Company regulations Proud Nerds

Principles of Information Security:

In the application of information security within Proud Nerds, we adhere to the following principles:

1. We aim to demonstrably comply with the ISO 27001:2023 and NEN 7510:2020 standards.
2. We comply with all applicable laws and regulations, including but not limited to:
    a. General Data Protection Regulation (GDPR)
    b. Occupational Health and Safety Legislation
3. Information security is an integral part of management responsibility. The management team at Proud Nerds holds ultimate responsibility for all aspects.
4. When entering into collaborations with external parties, whether substantive or related to the development or management of information provision (if relevant to information security), explicit attention is given to information security. Agreements in this regard are documented in writing, and compliance is monitored, ensuring adherence to legal and contractual obligations.
5. The business processes, information systems, and data collections of relevant units within Proud Nerds are classified according to a structured method based on the aspects of availability, integrity, and confidentiality (BIV).
6. During the hiring process, throughout employment, and in the case of employee termination, special attention is given to the reliability of employees and the safeguarding of information confidentiality.
7. An active policy is implemented to promote security awareness among management and employees.
8. Code of conduct for the use of (general) information provisions is in place, and compliance with these rules is monitored.
9. In the case of serious violations of information security regulations and/or relevant legal provisions, the Management can impose sanctions in line with the provisions outlined in the employment contract and personnel handbook regarding suspension, disciplinary actions, and termination of employment. A sanction policy has been established.

10. Measures have been taken for the physical security of offices, spaces, and resources.
11. Proud Nerds has implemented measures for the security and management of operational information and communication provisions. Measures against various forms of malicious software (computer viruses, spam, spyware, etc.) are integral to this.
12. Measures have been implemented by Proud Nerds to ensure that only authorized employees can use information and communication provisions.
13. When acquiring information systems and relevant resources, information security is given explicit attention at all stages of the acquisition or development process.
14. Adequate measures have been taken to ensure the availability of business processes and the information(systems) used in both normal and extraordinary circumstances.
15. As part of the information security policy process, both internal and external parties oversee compliance with information security policies within Proud Nerds.
16. All employees of Proud Nerds have access to resources for reporting and handling security incidents. The evaluation of incident handling is utilized to improve information security throughout the organization.

Finally, the Management will ensure that every employee is familiar with this information security policy and acts in accordance with it.

Signature of the Management (This document is not signed due to security considerations)

M. van de Poel

General Director