Proud Nerds
Informatiebeveiligingsbeleid

Kenmerk: 20231122PNMG - Proud Nerds - Beveiligingsbeleid -Extern - V1.0
Datum: 22 november 2023
Versie: 1.0
Classificatie: Publiek

Inleiding

Dit informatiebeveiligingsbeleid beschrijft het beleid met betrekking tot de beveiliging van informatie. De informatievoorziening is van essentieel belang voor de continuïteit van Proud Nerds. Zowel op papier als digitaal of welke vorm dan ook, zijn wij bij ons dagelijkse werkzaamheden afhankelijk van de beschikbaarheid, integriteit en vertrouwelijkheid van informatie.

De directie van Proud Nerds wil door middel van dit beleid veilige en betrouwbare diensten leveren en vertrouwen bieden aan onze klanten en medewerkers door informatie en persoonsgegevens te beschermen tegen interne en externe bedreigingen, zowel opzettelijke als onbedoelde, die de continuïteit en reputatie van de onderneming en onze klanten kunnen schaden of kunnen leiden tot financiële schade.

Onze informatiebeveiliging richt zich op de volgende vier aspecten:

- **Beschikbaarheid**, de informatie moet op de gewenste momenten beschikbaar zijn;
- **Integriteit**, de informatie moet juist en volledig zijn en de informatiesystemen moeten juiste en volledige informatie opslaan en verwerken;
- **Vertrouwelijkheid**, de informatie moet alleen toegankelijk zijn voor degene die hiervoor bevoegd is;
- **Privacy**, de bescherming van persoonsgegevens en de rechten van de betrokkenen.

Om een en ander gestalte te geven en voor eenieder aantoonbaar te maken is ons Information Security Management System (ISMS) gecertificeerd volgens de ISO-27001:2023 en de NEN 7510:2020 normen. Uitgangspunt is tenminste te voldoen aan de geldende wetgeving en de ISO-27001:2023 en NEN 7510:2020 normen. Daarnaast hebben we als doelstelling de belangen van onze interne- en externe belanghebbenden te behartigen

Verantwoordelijkheid informatiebeveiligingsbeleid

De directie is eindverantwoordelijk voor het informatiebeveiligingsbeleid en heeft dit beleid vastgesteld. De directie en de Security & Privacy Officer zijn verantwoordelijk voor het onderhouden van het informatiebeveiligingsbeleid. Het informatiebeveiligingsbeleid wordt met geplande tussenpozen of als zich significante wijzigingen voordoen, op juistheid, adequaatheid en doeltreffendheid gecontroleerd en waar nodig aangepast. Veranderingen kunnen worden veroorzaakt door wijzigingen in de context van de organisatie, risicoanalyse, wet- en regelgeving, resultaten van interne- en externe audits, directiebeoordelingen en overige.

Continue verbetering

Continue verbetering is belangrijk voor Proud Nerds en onze informatiebeveiliging. Continue verbetering wordt gewaarborgd door gestructureerd te werken aan de hand van de PDCA-cyclus van Deming. Dit model wordt gebruikt voor het vaststellen, implementeren, monitoren, controleren en onderhouden van het Information Security Management Systeem (ISMS). Hieronder worden de stappen kort uitgelegd:

Plan:
In de ontwerpfase wordt een informatiebeveiligingsbeleid ontwikkeld en vastgesteld. Hierin worden de informatiebeveiligingsdoelstellingen, de relevante processen en procedures vastgesteld, die er zorg voor dragen dat de risico’s gemanaged worden. Deze doelstellingen dienen te allen tijde de business doelstellingen van de organisatie te ondersteunen.

Do:
In deze fase wordt zorggedragen voor de implementatie van het informatiebeveiligingsbeleid en de

onderliggende procedures en beheersmaatregelen. Per informatiesysteem en/of proces worden verantwoordelijken aangewezen.

Check:
In deze fase wordt door middel van interne audits, gecontroleerd en waar mogelijk gemeten of de het informatiebeveiligingsbeleid en ondersteunende procedures correct worden uitgevoerd.

Act:
In deze laatste fase worden corrigerende en preventieve activiteiten genomen, gebaseerd op de resultaten van de interne audits en wordt waar nodig het ISMS geactualiseerd. Door middel van deze gestructureerde aanpak, wordt op een planmatige, procesgerichte en beheersbare wijze vormgegeven aan informatiebeveiliging.

Door middel van deze gestructureerde aanpak, wordt op een planmatige, procesgerichte en beheersbare wijze vormgegeven aan informatiebeveiliging.

Definitie van Informatiebeveiliging:

Proud Nerds hanteert de volgende definitie van Informatiebeveiliging:

> *"Het samenhangende stelsel van maatregelen dat zich richt op duurzaam waarborgen van een optimaal niveau van beschikbaarheid, integriteit en vertrouwelijkheid van informatie en informatiesystemen."*

Belangrijk is op te merken dat informatiebeveiliging een geïntegreerd systeem van maatregelen omvat. Dit houdt in dat de diverse maatregelen die tezamen informatiebeveiliging vormen, niet los van elkaar staan maar onderling met elkaar verbonden zijn.

Het systeem van beveiligingsmaatregelen beoogt een blijvend niveau van beveiliging te realiseren. Door zorgvuldige borging wordt gegarandeerd dat het gewenste beveiligingsniveau ook op de lange termijn gehandhaafd blijft.

Informatiebeveiliging streeft naar het realiseren van een optimaal beveiligingsniveau. Dit optimale niveau wordt bereikt door zorgvuldige afweging van kosten en baten.

Doelstelling informatiebeveiligingsbeleid

Het informatiebeveiligingsbeleid van Proud Nerds heeft als primair doel het waarborgen van de continuïteit van de bedrijfsvoering, het leveren van veilige en betrouwbare diensten en voorkomen van incidenten en daaruit voorvloeiende schade (maatschappelijk, reputatie, financieel of anderzijds).

Daarnaast moet het vertrouwen bieden aan klanten en medewerkers dat mogelijke risico's adequaat worden beheerd.

Het beleid voldoet aan de volgende punten:

- Het informatiebeveiligingsbeleid wordt op hoofdlijnen vastgesteld en uitgedragen door het management van Proud Nerds.
- Het informatiebeveiligingsbeleid is van toepassing op alle (externe) medewerkers en van Proud Nerds.
- De basis voor het informatiebeveiligingsbeleid-managementsysteem is ISO27001:2023 en de NEN7510:2020. Zo kan de werking van dit managementsysteem door onafhankelijke partijen worden geverifieerd en bevestigd.

- Het informatiebeveiligingsbeleid biedt de basis om te voldoen aan geldende wet- en regelgeving.
- Maatregelen die voortvloeien uit het informatiebeveiligingsbeleid worden met enige regelmatig getoetst op effectiviteit.

Doelstellingen informatiebeveiliging

Onze informatiebeveiliging richt zich op de volgende vier aspecten:

- **Beschikbaarheid**, de informatie moet op de gewenste momenten beschikbaar zijn;
- **Integriteit**, de informatie moet juist en volledig zijn en de informatiesystemen moeten juiste en volledige informatie opslaan en verwerken;
- **Vertrouwelijkheid**, de informatie moet alleen toegankelijk zijn voor degene die hiervoor bevoegd is;
- **Privacy**, de bescherming van persoonsgegevens en de rechten van de betrokkenen.

Concrete informatiebeveiligingsdoelstelling zijn opgenomen in het ISMS.

Toepassingsgebied ISMS

Het toepassingsgebied (scope) van het ISMS zijn alle interne processen en informatiesystemen van alle organisatieonderdelen van Proud Nerds. Het betreft de volgende activiteiten:

- Het ontwerpen, ontwikkelen, beheren en hosten van web- en softwareapplicatie, e-commerce omgevingen en apps;
- Het ontwerpen, ontwikkelen en aanbieden van SaaS;
- Het opzetten, leveren en beheren van IT-infrastructuur en cloudoplossingen.

Deze scope geldt voor zowel de ISO 27001:2023 als de NEN7510:2020. De individuele normelementen die van toepassing zijn staan beschreven in de Verklaring van Toepasselijkheid ISO27001:2023 en Verklaring van Toepasselijkheid NEN7510:2020.

Toelichting op het toepassingsgebied

Alle activiteiten worden uitgevoerd vanuit het vestigingsadres van Proud Nerds.

Onze dienstenportfolio bevat een aantal activiteiten waar wij partners voor inzetten. De volgende relevante activiteiten heeft Proud Nerds uitbesteed aan leveranciers:

- Bewakingsdiensten;
- Uitvoeren van Security monitoring en Periodieke penetratietests;
- Hosting en Datacenters;
- ICT diensten op het vlak van netwerk en connectiviteit, server- en opslagcapaciteit en end-user computing.

Met deze leveranciers heeft Proud Nerds, afhankelijk van de te leveren dienstverlening, contractuele afspraken gemaakt over informatiebeveiliging en privacy. Indien er persoonsgegevens verwerkt worden zijn deze afspraken aangevuld met een Verwerkersovereenkomst.

Ondersteunende documentatie

Ter ondersteuning van dit informatiebeveiligingsbeleid zijn de volgende ondersteunende procedures en beleidsdocumenten opgesteld.

1. Beleid voor mobiele apparatuur en telewerken
2. Screeningsbeleid
3. Informatieclassificatie
4. Toegangsbeveiligingsbeleid
5. Wachtwoordbeleid
6. Beleid inzake het gebruik van cryptografische beheersmaatregelen
7. Clear desk- en Clear screen beleid
8. Back-up beleid
9. Beleid voor informatietransport
10. Beleid voor beveiligd ontwikkelen
11. Beleid voor on- en offboarding
12. Informatiebeveiligingsbeleid voor leveranciersrelaties
13. Melden van (informatie)beveiligingsincidenten
14. Business Continuity Plan
15. Bedrijfsreglement Proud Nerds

Uitgangspunten informatiebeveiliging

Bij de toepassing van informatiebeveiliging binnen Proud Nerds, hanteren we de volgende uitgangspunten:

1. We streven ernaar aantoonbaar te voldoen aan de normen ISO 27001:2023 en NEN 7510:2020
2. We voldoen aan alle, van toepassing zijnde, wet- en regelgeving. In dit verband wordt expliciet genoemd:
    a. Algemene verordening gegevensbescherming (AVG)
    b. Arbowetgeving
3. Beveiliging van informatie is een onderdeel van de integrale managementverantwoordelijkheid. Voor alle onderdelen van Proud Nerds is de directie eindverantwoordelijk.
4. Wanneer we (mits relevant voor informatiebeveiliging) samenwerkingsverbanden aangaan met externe partijen, hetzij inhoudelijk, hetzij voor de ontwikkeling of het beheer van de informatievoorziening, wordt nadrukkelijk aandacht besteed aan informatiebeveiliging. Afspraken hierover worden schriftelijk vastgelegd en op de naleving hiervan wordt toegezien. Daarbij waarborgen wij dat we onze wettelijke en contractuele verplichtingen naleven.
5. De bedrijfsprocessen, informatiesystemen en gegevensverzamelingen van de relevante onderdelen van Proud Nerds zijn volgens een gestructureerde methode geclassificeerd naar de aspecten beschikbaarheid, integriteit en vertrouwelijkheid (BIV).

6. Bij de aanname, tijdens het dienstverband en in geval van ontslag van medewerkers wordt nadrukkelijk aandacht besteed aan de betrouwbaarheid van medewerkers en aan de waarborging van de vertrouwelijkheid van informatie.
7. We voeren een actief beleid om het beveiligingsbewustzijn van management en medewerkers te stimuleren.
8. We beschikken over gedragsregels voor het gebruik van (algemene) informatievoorzieningen. Op de naleving van deze gedragsregels wordt toegezien.
9. Bij grove overtreding van de regelgeving voor informatiebeveiliging en/of relevante wettelijke bepalingen kan de Directie een sanctie opleggen conform hetgeen hierover met betrekking tot op non-actiefstelling, disciplinaire straffen, en beëindiging van het dienstverband is vastgelegd in de arbeidsovereenkomst en personeelshandboek. Er is een sanctiebeleid opgesteld.
10. We hebben maatregelen getroffen voor de fysieke beveiliging van kantoor, ruimtes en middelen.
11. Proud Nerds heeft maatregelen getroffen voor de beveiliging en het beheer van de operationele informatie- en communicatievoorzieningen. Maatregelen tegen allerlei vormen van kwaadaardige programmatuur (computervirussen, spam, spyware, etc.) vormen hiervan een belangrijk onderdeel.
12. Proud Nerds heeft maatregelen getroffen waardoor is gewaarborgd dat alleen geautoriseerde medewerkers gebruik kunnen maken van de informatie- en communicatievoorzieningen.
13. Bij de aanschaf van informatiesystemen en relevante middelen worden in alle fasen van het aanschaf- of ontwikkelingsproces nadrukkelijk aandacht besteed aan informatiebeveiliging.
14. We hebben adequate maatregelen getroffen waardoor de beschikbaarheid van de bedrijfsprocessen en de hierbij gebruikte informatie(systemen) is gewaarborgd, zowel in normale als in buitengewone omstandigheden.
15. Als onderdeel van het beleidsproces voor informatiebeveiliging wordt binnen Proud Nerds door interne en externe partijen toegezien op de naleving van het informatiebeveiligingsbeleid.
16. Alle medewerkers van Proud Nerds beschikken over middelen voor het melden en afhandelen van beveiligingsincidenten. De evaluatie van de afhandeling van beveiligingsincidenten wordt benut voor de verbetering van informatiebeveiliging in de gehele organisatie.

Ten slotte zal de directie erop toezien dat elke werknemer bekend is met dit informatiebeveiligingsbeleid en hiernaar handelt en werkt.

Handtekening directie (Dit document is vanwege veiligheidsoverwegingen niet ondertekend)

M. van de Poel
Algemeen directeur