Informatiebeveiligingsbeleid

Lannet IT B.V.

Versiebeheer

De verantwoordelijke van dit document is Paul den Otter (directielid). Hieronder is het versiebeheer van dit document vastgelegd.

Versie	Auteur	Datum	Beschrijving	Goedkeuring	Ingangsdatum
1.0	PdO	16-5-2018	Toevoegen versiebeheer	PdO	16-5-2018
1.1	PdO	28-6-2018	Toevoegen digitaal document niet ondertekend	PdO	28-6-2018
1.2	PdO	30-8-2018	Paragraaf Verantwoordelijkheid informatiebeveiligingsbeleid uitgebreid, document geactualiseerd	PdO	30-8-2018
2.0	RJV	12-03-2020	Beleid herzien, scope aanpassing NEN 7510	PdO	12-03-2020
2.1	RJV	21-04-2020	Scope herziening	PdO	21-04-2020
3.0	RJV	20-05-2021	Kleine tekstuele aanpassingen	PdO	20-05-2021
3.1	RJV	16-06-2021	Middelen toegevoegd Tekstuele aanpassingen	PdO	29-06-2021

Inleiding

Dit informatiebeveiligingsbeleid beschrijft het beleid met betrekking tot de beveiliging van informatie. De informatievoorziening is van essentieel belang voor de continuïteit van onze organisatie. 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. Om een en ander gestalte te geven en voor eenieder aantoonbaar te maken is ons Information Security Management System (ISMS) gecertificeerd volgens de ISO-27001:2017 & NEN 7510:2017 normen. Uitgangspunt is tenminste te voldoen aan de eisen van de stakeholders, de geldende wetgeving en de ISO-27001:2017 & NEN 7510:2017 normen.

Verantwoordelijkheid informatiebeveiligingsbeleid

De directie is eindverantwoordelijk voor het informatiebeveiligingsbeleid en heeft dit beleid vastgesteld. De directie en Security 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 de organisatie en informatiebeveiliging. Continue verbetering wordt gewaarborgd door gestructureerd te werken aan de hand van de PDCA-cirkel 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.

Definitie van informatiebeveiliging

Informatiebeveiliging wordt als volgt gedefinieerd:

"Het samenhangend stelsel van maatregelen dat zich richt op het blijvend realiseren van een optimaal niveau van beschikbaarheid, integriteit en vertrouwelijkheid van informatie en informatiesystemen."

Opgemerkt wordt dat informatiebeveiliging een samenhangend stelsel van maatregelen omvat. Dit betekent dat de verschillende maatregelen die samen de informatiebeveiliging vormen niet los van elkaar, maar in onderlinge relatie met elkaar staan.

Het stelsel van beveiligingsmaatregelen heeft tot doel een blijvend niveau van beveiliging te realiseren. Door een zorgvuldige borging wordt bereikt dat het gewenste niveau van beveiliging ook op langere termijn blijft gehandhaafd.

Informatiebeveiliging is gericht op het realiseren van een optimaal niveau van beveiliging. Dit optimum wordt bereikt door een zorgvuldige afweging van kosten en baten.

Doelstelling informatiebeveiligingsbeleid

Het opstellen van het informatiebeveiligingsbeleid heeft tot doel de doelstellingen en uitgangspunten met betrekking tot informatiebeveiliging binnen Lannet IT vast te stellen en vast te borgen. Hiermee vormt het beleid de leidraad voor alle betrokkenen bij informatiebeveiliging binnen Lannet IT.

Doelstellingen informatiebeveiliging

Zoals in de definitie is verwoord, richt informatiebeveiliging zich op de volgende aspecten van de informatievoorziening:

- 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.

Concrete informatiebeveiligingsdoelstelling zijn opgenomen in het ISMS-actieplan.

Scope Information Security Management System

De scope van het ISMS heeft betrekking op de gehele organisatie met de daarbij behorende verantwoordelijkheden ten behoeve van diensten aan klanten, diensten aan de interne organisatie. Externe en interne onderwerpen zijn bij de bepaling overwogen en er is rekening gehouden met de eisen en verwachtingen van alle belanghebbende partijen.

De ISO 27001:2017 scope luidt als volgt:
“Informatiebeveiliging met betrekking tot het ontwerpen, installeren, onderhouden en beheren van netwerken en telecominstallaties bij MKB-bedrijven en mondzorgpraktijken.

Dit in overeenstemming met de Verklaring van Toepasselijkheid ISO 27001:2017 versie 3.1 16-06-2021.

De NEN 7510:2017 scope luidt als volgt:
“Informatiebeveiliging met betrekking tot het ontwerpen, installeren, onderhouden en beheren van netwerken en telecominstallaties bij MKB-bedrijven en mondzorgpraktijken door middel van Kaseya, MS Teams en RDP met behulp van Teamviewer. Het hosten van de data is uitbesteed aan een gecertificeerd datacentrum.

Dit in overeenstemming met de Verklaring van Toepasselijkheid NEN 7510:2017 versie 3.3 29-06-2021, waarin is gespecificeerd welke activiteiten, producten en/of diensten er zijn uitbesteed met de daarbij behorende interfaces er zijn met MKB-bedrijven en mondzorgpraktijken.”

Toepassingsgebied scope

Primaire processen binnen scope:

- Verkoop
- Inkoop
- Support
- Remote beheer

- Onderhoud op locatie
- Storingen en wensen
- Projecten

Locatie:
1 locatie binnen scope te Oisterwijk.

Toelichting op de scope

Lannet IT is een ervaren, deskundige en betrouwbare partner in automatiseringsoplossingen en telecomvoorzieningen. We ontwerpen, installeren, onderhouden en beheren netwerken en telecominstallaties. Wij richten ons met name op het MKB en de dentale branche. Lannet IT combineert haar passie voor informatietechnologie met klantgerichte dienstverlening. Een transparante bedrijfsvoering en persoonlijke service staan daarbij centraal.

Middelen

Lannet IT B.V. heeft de middelen vastgesteld en beschikbaar gesteld die nodig zijn voor het inrichten, implementeren, onderhouden en continu verbeteren van het Information Security Management Systeem. Dit is voornamelijk terug te zien in:

- Inhuur van een externe adviseur & Security Officer As A Service
- 40 uur per kwartaal beschikbaar stellen van medewerkers
- Lannet Wiki-omgeving met beleid en procedures

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. Informatiebeveiligingsbeleid voor leveranciersrelaties
12. Melden van (informatie)beveiligingsincidenten
13. Business Continuity Plan
14. Bedrijfsreglement Lannet IT

Uitgangspunten informatiebeveiliging

Bij de toepassing van informatiebeveiliging binnen Lannet IT, hanteren we de volgende uitgangspunten:

1. We streven ernaar aantoonbaar te voldoen aan de normen ISO 27001:2017 en NEN 7510:2017

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 Lannet IT 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 Lannet IT 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 (zie bedrijfsreglement Lannet IT) 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. Er is een sanctiebeleid opgesteld.

10. We hebben maatregelen getroffen voor de fysieke beveiliging van kantoor, ruimtes en middelen.

11. Alle onderdelen van Lannet IT hebben 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. We hebben 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 Lannet IT door interne en externe partijen toegezien op de naleving van het informatiebeveiligingsbeleid.

16. Alle medewerkers van Lannet IT 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)

Hans van Berkel Paul den Otter Henri Vissers