Information Security Management System

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

Als directie van Lannet IT B.V. (hierna te noemen: Lannet IT) richten we ons beleid bij het voorbereiden en uitvoeren van het algemeen ondernemingsbeleid, mede op een organisatie waarin de kwaliteit van de informatiebeveiliging hoog in het vaandel staat. Kwaliteit is voor ons synoniem met klanttevredenheid, de klant en al zijn wensen staan bij ons vanzelfsprekend centraal. Daarnaast wordt ook rekening gehouden met eisen en wensen van andere belanghebbenden en speelt de organisatie in op externe en interne kansen en bedreigingen.

Om een en ander gestalte te geven en voor eenieder aantoonbaar te maken kiezen wij ervoor om het Information Security Management System (ISMS) te laten certificeren volgens de ISO-27001:2013 & NEN 7510:2017 normen. Uitgangspunt is tenminste te voldoen aan de eisen van de stakeholders, de geldende wetgeving en de ISO-27001:2013 & NEN 7510:2017 normen.

Door de organisatie zal gestreefd worden naar de continue verbetering van kwaliteit van informatiebeveiliging. Daartoe wordt regelmatig het managementsysteem getoetst door middel van audits. Op basis van de bevindingen zal periodiek een activiteitenplan worden opgesteld waarin de doelstellingen worden opgenomen. Een directiebeoordeling zal twee keer per jaar plaatsvinden door de directie.

Bovenstaand beleid hebben we samengevat in onderstaand figuur:

Verbeteringen komen tot stand door te luisteren naar:

- Klanten
- Medewerkers
- Leveranciers
- Andere belanghebbenden

Van iedere medewerker wordt verwacht dat hij de activiteiten uitvoert conform het personeelshandboek en overige regels en een actieve bijdrage levert aan de uitvoering van dit beleid.

Om gestructureerd aan verbeteringen te werken, worden jaarlijks door de directie verbeterdoelstellingen opgesteld. Deze worden, waar mogelijk, gekoppeld aan persoonlijke doelstellingen.

De directie zal erop toezien dat elke werknemer bekend is met dit ISMS-beleid en hiernaar werkt. Ter vergroting van de bewustwording rondom het onderwerp Informatiebeveiliging worden er informatiesessies gehouden over dit beleid en het gehele project. Daarnaast is het een geïntegreerd onderdeel van de functionerings- en

beoordelingscyclus en is informatiebeveiliging een structureel onderdeel van vrijwel alle interne overlegstructuren.

Algemene toelichting

Dit document beschrijft het beleid van Lannet IT met betrekking tot de beveiliging van informatie. De informatievoorziening is van essentieel belang voor de continuïteit van ons bedrijf. Zowel op papier als geautomatiseerd zijn wij bij ons dagelijks werk afhankelijk van de beschikbaarheid van betrouwbare informatie. Ook vereist het feit dat klanten informatie over hun klanten bij ons in bewaring gegeven, dat we hier zeer zorgvuldig mee omgaan.

Onze organisatie en onze informatievoorziening wordt blootgesteld aan een groot aantal bedreigingen, al dan niet opzettelijk van aard. Deze bedreigingen maken het noodzakelijk om gerichte maatregelen te treffen om de risico's tot een aanvaardbaar niveau te reduceren en daarmee het vertrouwen dat klanten ons geven, ook daadwerkelijk waar te maken. Nog los van eventuele wettelijke eisen waarop we op dit vlak moeten voldoen.

Het proces van informatiebeveiliging begint met het definiëren van een beleid op dit punt.

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.

Het bijdragen aan verbeterde interne controle over informatiebeveiliging

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 en ontwikkeling van software. Externe en interne onderwerpen zijn bij de bepaling overwogen en er is rekening gehouden met de eisen en verwachtingen van alle belanghebbende partijen.

De scope luidt als volgt:

> “Het ontwerpen, installeren, onderhouden en beheren van netwerken en telecominstallaties bij MKB-bedrijven en mondzorgpraktijken.”

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.

Verantwoordelijkheid informatiebeveiligingsbeleid

De directie is eindverantwoordelijk voor het informatiebeveiligingsbeleid en heeft dit beleid vastgesteld. De Information security officer is verantwoordelijk voor het onderhoud van het informatiebeveiligingsbeleid. We zijn ons bewust dat regelmatig onderhoud aan het ISMS noodzakelijk is. Veranderingen worden veroorzaakt door wijzigingen in onze context (issues stakeholders, risico's, wet- en regelgeving) de organisatie zelf, resultaten van (interne) audits en overige. Het ISMS zal hierop worden aangepast, waar nodig. Tevens zal het ISMS worden herzien bij ernstige beveiligingsincidenten.

Ondersteunende documentatie

Dit informatiebeveiligingsbeleid is binnen Lannet IT verder uitgewerkt in de volgende documenten;

- Context analyse (SWOT-analyse, Stakeholder, Risicoanalyse Lannet IT);
- Bedrijfsreglement van Lannet IT;
- Gebruikersovereenkomsten;
- Procedures, instructies en formulieren van het ISMS;
- Aanvullende ISMS beleidstukken/documenten:
    a) Toegangsbeveiliging beleid
    b) Classificatie van informatie (en verwerking)
    c) Fysieke en omgevingsbeveiliging
    d) Onderwerpen die gericht zijn op de eindgebruiker zoals:
        - ❖ Aanvaardbaar gebruik van bedrijfsmiddelen
        - ❖ Clean desk en clear screen beleid
        - ❖ Informatietransport
        - ❖ Mobiele apparatuur en telewerken
        - ❖ Beperkingen van software-installaties en -gebruik
    e) Back-up beleid
    f) Informatietransport beleid
    g) Bescherming tegen malware
    h) Beheer van technische kwetsbaarheden
    i) Cryptografische beheersmaatregelen
    j) Communicatiebeveiliging
    k) Privacy en bescherming van persoonsgegevens
    l) Leveranciersrelaties

Uitgangspunten informatiebeveiliging

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

1. We streven ernaar aantoonbaar te voldoen aan de norm NEN-ISO/IEC 27001:2013 zoals opgesteld door het Nationaal Cyber Security Centrum (NSCS).

2. We voldoen aan alle, van toepassing zijnde, wet- en regelgeving. In dit verband wordt expliciet genoemd:
    a. Algemene verordening gegevensbescherming (AVG)

3. Beveiliging van informatie is een onderdeel van de integrale managementverantwoordelijkheid. Voor alle onderdelen van Lannet IT is de Information Security Officer verantwoordelijk.

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 ontwikkeling en aanschaf van informatiesystemen en aanschaf van 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.

Alle onderdelen 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