Informatie beveiligingsbeleid Labmicta

1. Inhoud

Doel 4
Principe....4
1. Wat is informatiebeveiliging? 5
1.1 Definitie van informatiebeveiliging....5
1.2 Wat is informatie?....5
1.3 Waarom een informatiebeveiligingsbeleidsplan....5
1.4 Norm NEN 7510....5
2 Relevante wetgeving 7
2.1 Algemene verordening gegevensbescherming (AVG)....7
2.2 Medisch beroepsgeheim 7
2.3 Wettelijk kader met betrekking tot uitwisselen van gegevens....8
3. Doelstelling informatiebeveiliging....9
4 Context van de organisatie 10
4.1 Inzicht in de organisatie en haar context 10
4.2 Inzicht in de behoeften en verwachtingen van belanghebbenden....10
4.3 Het toepassingsgebied van het managementsysteem voor informatiebeveiliging vaststellen....10
4.4 Managementsysteem voor informatiebeveiliging....10
5 Leiderschap 11
5.1 Leiderschap en betrokkenheid 11
5.2 Beleid....11
5.3 Rollen, verantwoordelijkheden en bevoegdheden binnen de organisatie....12
6. Planning....13
6.1 Risico beheersing....13
6.2 Informatiebeveiligingsdoelstellingen en de planning om ze te bereiken....13
7. Ondersteuning 16
7.1 Middelen 16
7.2. Competenties 17
7.3 Bewustzijn 18
7.4 Communicatie....18
7.5 Gedocumenteerde informatie....18
8. Uitvoering....19
8.1 Operationele planning en beheersing....19
8.2 Risicobeoordeling van informatiebeveiliging....19
8.3 Informatiebeveiligingsrisico’s behandelen....19
9. Evaluatie van de prestatie....20
9.1 Monitoren, meten, analyseren en evalueren 20
9.2 Interne audit....20
9.3 Directiebeoordeling 20

10. Verbetering 21
10.1 Afwijkingen en corrigerende maatregelen en verbeteringen 21
10.1.1 Fysieke beveiliging van gebouw en beveiliging van de omgeving 21
10.1.2 Beheer van communicatie en bedieningsprocessen 21
10.1.3 Toegangsbeveiliging 25
10.1.4 Beheer van informatiebeveiligingsincidenten 26
10.1.5 Bedrijfscontinuïteitsbeheer 26
Bijlagen 28
Bijlage 1: Basis van ons informatiebeveiligingsbeleid 28

Doel

Dit document beschrijft het beleid van Labmicta met betrekking tot de beveiliging van informatie.

Principe

Informatievoorziening is van essentieel belang voor de continuïteit van de bedrijfsvoering van Labmicta. Zowel op papier als geautomatiseerd zijn wij bij ons dagelijks werk afhankelijk van de continue beschikbaarheid van betrouwbare informatie. Onze organisatie en onze informatie(-voorziening) wordt blootgesteld aan een groot aantal (mogelijke) 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. Daarnaast zijn we vanuit de wetgeving verplicht onze informatie goed te beveiligen. Dit komt onder andere naar voren in de Algemene Verordening Gegevensbescherming (AVG). Het proces van informatiebeveiliging begint met het definiëren van een beleid op dit punt welke gedragen wordt door Labmicta.

1. Wat is informatiebeveiliging?

1.1 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 dus dat informatiebeveiliging een samenhangend stelsel van maatregelen omvat. Dit betekent dat de verschillende maatregelen die tezamen de informatiebeveiliging vormen, niet los van elkaar worden getroffen, maar in onderlinge relatie met elkaar staan.

1.2 Wat is informatie?

Informatie is een bedrijfsmiddel, dat net als andere belangrijke bedrijfsmiddelen, waarde heeft voor een organisatie (en haar klanten) en voortdurend op een geschikte manier moet zijn beschermd. Informatie kan in verschillende vormen voorkomen. De informatie kan beschikbaar zijn op papier of elektronisch. Ook voor het overdragen van informatie zijn meerdere kanalen beschikbaar zoals post, elektronisch en mondelinge overdracht. Informatie moet altijd op geschikte wijze worden beschermd, rekening houdend met de vorm of de wijze waarop deze wordt gedeeld en/of opgeslagen.

1.3 Waarom een informatiebeveiligingsbeleidsplan

Het opstellen van het informatiebeveiligingsbeleid heeft tot doel de doelstellingen en uitgangspunten met betrekking tot informatiebeveiliging binnen Labmicta vast te stellen en eenduidig vast te leggen. Hiermee vormt het beleid de leidraad en het kader voor alle direct en indirect betrokkenen en belanghebbende(n) bij informatiebeveiliging binnen Labmicta.

Verstoringen in de informatievoorziening en schade als gevolg daarvan kunnen worden voorkomen of beperkt door een geschikte set beheersmaatregelen in te zetten, waaronder beleid, werkwijzen en procedures. Het stelsel van beheersmaatregelen tezamen 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 wordt gehandhaafd. Het vaststellen van het gewenste niveau wordt bepaald door een zorgvuldige afweging van kosten en baten maar ook door goed te kijken naar de “werkbaarheid” van beheersmaatregelen in de praktijk. Deze factoren staan veranderen voortdurend. De afweging zal dan ook telkens opnieuw moeten worden gemaakt. Informatiebeveiliging vereist dan ook een continu besturingsproces.

Door een samenhangend stelsel van maatregelen is de organisatie in staat om op te treden tegen (potentiële) bedreigingen die aspecten van de informatievoorziening kunnen schaden. Of deze bedreigingen juist te voorkomen en/of te beperken. Bedreigingen zijn er in vele vormen. Deze kunnen fysiek van aard zijn, zoals brand en wateroverlast. Of technisch van aard, zoals in de vorm van storingen in programmatuur, apparatuur of de stroomvoorziening. Ook de mens vormt een bedreiging door on- of opzettelijke fouten of vergissingen te maken die de informatievoorziening verstoren. Maar ook opzettelijke (externe) kwaadaardige daden, zoals hacking, phishing, computervirussen en computerfraude kunnen de informatievoorziening schaden.

1.4 Norm NEN 7510

De NEN 7510 geeft aanwijzingen voor het toepassen van informatiebeveiliging in de gezondheidszorg. De norm biedt een gemeenschappelijk kader voor deze inrichting. In de norm wordt aandacht besteed aan het inrichten van het managementsysteem voor informatiebeveiliging en het risicomanagement dat daar deel van uitmaakt.

Daarnaast worden beheersmaatregelen geschetst welke vervolgens invulling geven aan de informatiebeveiliging zelf. Daarbij zijn aandachtspunten en aanbevelingen voor implementatie opgenomen om de beheersmaatregelen in praktijk te brengen. Belangrijk om te vermelden is dat de aandachtspunten en aanbevelingen die genoemd zijn in de norm niet normatief zijn aangezien de organisaties waar de norm zich op richt varieert van individuele zorgverleners tot grote zorginstellingen en andere organisaties in de gezondheidszorg. Het is aan de instellingen zelf om af te wegen of en hoe de norm wordt geïmplementeerd.

Voor het informatiebeveiligingsbeleid van Labmicta is de opbouw van de NEN 7510 norm als uitgangspunt genomen. We bespreken per hoofdstuk welke doelstellingen we nastreven en hoe dit in de praktijk wordt vormgegeven.

2 Relevante wetgeving

2.1 Algemene verordening gegevensbescherming (AVG)

Ons laboratorium verwerkt persoonsgegevens van zowel patiënten als ook van eigen medewerkers. Daarom moeten we voldoen aan de AVG. Hierin staan de belangrijkste regels voor de omgang met persoonsgegevens beschreven. Een belangrijke regel in de AVG in relatie tot informatiebeveiliging is de volgende: de gegevensverwerking moeten op een passende manier worden beveiligd. Voor bijzondere gegevens, zoals over ras, gezondheid en geloofsovertuiging, gelden extra strenge regels.

Er is een sterke relatie tussen privacybescherming en informatiebeveiliging. Privacybescherming richt zich op de zorgvuldige omgang met persoonsgegevens. Naast de patiëntgegevens gaat het hierbij dus ook om gegevens van medewerkers en overige personen. Informatiebeveiliging richt zich op de beveiliging van gegevens, waaronder persoons-, personeels- en bedrijfsgegevens. De maatregelen die in het kader van informatiebeveiliging worden getroffen, leveren dus een bijdrage aan de bescherming van privacygevoelige gegevens en vice versa.

Doordat Labmicta bijzondere persoonsgegevens verwerkt is het noodzakelijk om aangemeld te zijn bij de Autoriteit Persoonsgegevens (AP). Labmicta is aangemeld onder het meldingsnummer M1101078.

Sinds 1 januari 2016 is de meldplicht datalekken van kracht. Hierdoor is het nu wettelijk verplicht om datalekken te melden. De wet spreekt van een datalek wanneer persoonsgegevens verloren raken of onrechtmatige verwerking redelijkerwijs niet kan worden uitgesloten. Onder onrechtmatige verwerking valt onder andere het aanpassen en/of veranderen van persoonsgegevens en onbevoegde toegang tot deze gegevens. Er is dus niet alleen sprake van een datalek als een hacker toegang tot persoonsgegevens krijgt. Ook verlies van een USB-stick in de trein of het verlies van gegevens bij een brand in het datacentrum terwijl er geen back up beschikbaar is, is een datalek. Een extra reden om als laboratorium preventief de juiste beheersmaatregelen te nemen om dergelijke datalekken te voorkomen.

2.2 Medisch beroepsgeheim

Zoals eerder gezegd verwerkt Labmicta gegevens betreffende de gezondheidstoestand en persoonsgegevens van de bij ons bekende patiënten. Deze gegevens mogen niet zomaar gedeeld worden. Dit heeft te maken met het medisch beroepsgeheim waar medische hulpverleners zich aan moeten houden. Op twee plaatsen in de wet is dit opgenomen;

- In de eerste plaats is dat artikel 88 van de Wet op de beroepen in de individuele gezondheidszorg (Wet BIG). Dit artikel bepaalt dat een ieder die een beroep op het gebied van de individuele gezondheidszorg uitoefent, de plicht heeft alles geheim te houden wat hem bij de uitoefening van zijn beroep is toevertrouwd.
- Daarnaast is de medische zwijgplicht vastgelegd in artikel 7:457 van het Burgerlijk Wetboek (BW). Die bepaling is beperkter en geldt alleen voor hulpverleners die een handeling op het gebied van de geneeskunst verrichten. Het onderdeel van het BW waarin deze bepaling is opgenomen wordt ook vaak aangeduid met de afkorting WGBO (Wet inzake de geneeskundige behandelingsovereenkomst).

Belangrijk om te vermelden is dat niet alleen de hulpverlener zelf tot geheimhouding verplicht is. Ook medewerkers die (indirect) bij de zorgverlening betrokken zijn, maar niet vanwege hun eigen handelen een medisch beroepsgeheim hebben, hebben een van de hulpverlener afgeleid medisch beroepsgeheim. Dit geldt dan voor zover deze personen beroepsmatig op de hoogte raken van behandelgegevens van de patiënt. Dat kunnen bijvoorbeeld bestuurders, assistenten, secretaresses, analisten, bewakingspersoneel, ICT-medewerkers en schoonmakers zijn.

Voor de informatiebeveiliging betekent dit dat er extra aandacht moet zijn voor het juist beveiligen van de bij ons bekende informatie. Dit zodat alleen de daarvoor geautoriseerde personen toegang hebben tot bepaalde informatie.

2.3 Wettelijk kader met betrekking tot uitwisselen van gegevens

Enerzijds dienen wij ons te houden aan de privacywetgeving en het medisch beroepsgeheim. Maar voor de uitvoering van ons werk is het uitwisselen van gegevens van groot belang. De grondslag waarop we dit kunnen doen is het volgende artikel uit de WGBO; “Artsen moeten toestemming hebben van de patiënt voor het verstrekken van informatie aan derden. Deze expliciete toestemming geldt niet voor zorgverleners die rechtstreeks betrokken zijn bij de behandelingsovereenkomst. Zij mogen met ‘veronderstelde toestemming van de patiënt’ relevantie informatie van de behandelend arts ontvangen”. Het uitvoeren van een onderzoek binnen ons laboratorium doe wij op basis van (door)verwijzingen van (huis)artsen. In dat geval zijn wij betrokken bij de behandeling en mag er onderling informatie worden uitgewisseld over de betreffende patiënt als deze informatie relevant is.

Er zijn ook twee andere relevante uitzonderingen op het medisch beroepsgeheim waardoor het mogelijk is om gegevens over en van patiënten uit te wisselen. Dit zijn;

- Als een patiënt zelf toestemming heeft gegeven om zijn gegevens met iemand anders te bespreken. Bijvoorbeeld als een man aan zijn huisarts laat weten dat zijn echtgenote zijn bloeduitslagen mag opvragen.
- Als er sprake is van bepaalde besmettelijke infectieziekten, zoals hepatitis, tbc of mazelen. in dat geval is een arts verplicht dat bij de GGD te melden (meldplicht), op basis van de Wet Publieke Gezondheid, zodat er tijdige en juiste maatregelen kunnen worden genomen.

Ook relevant is het verschil in regels omtrent push- en pullverkeer. Momenteel maken wij gebruik van pushverkeer waarbij persoonsgegevens uitsluitend worden verzonden aan één of meerdere zorgaanbieders die een behandelrelatie hebben met de patiënt. Daar is geen uitdrukkelijke toestemming van de patiënt voor nodig. Bij pushverkeer ligt het initiatief voor de uitwisseling bij de verzender en vooraf is duidelijk aan wie de informatie wordt verstrekt.
Pullverkeer is alleen mogelijk met uitdrukkelijke toestemming van de patiënt. Van pullverkeer is namelijk sprake als gegevens over een patiënt beschikbaar worden gesteld aan een groep zorgaanbieders voor raadpleging op hun initiatief. Bij pullverkeer ligt het initiatief (dus) bij de ontvanger/raadpleger. Momenteel verstrekken wij gegevens alleen op basis van pushverkeer. Nieuwe ontwikkelingen, zoals uitslagen beschikbaar stellen via een portal, worden beoordeeld op deze regels.

In het informatiebeveiligingsbeleid gaat het om de beveiliging van informatie. Een afgeleide daarvan is welke informatie we aan wie uitwisselen en of we dit op een veilige manier doen. Bovenstaande maakt duidelijk dat niet elke uitwisseling van gegevens zomaar is toegestaan.

3. Doelstelling informatiebeveiliging

Met het informatiebeveiligingsbeleid wil Labmicta bijdragen aan een optimale kwaliteit van de informatievoorziening en zorgen voor een juiste balans tussen functionaliteit, veiligheid en privacy en de daarmee samenhangende kosten. Labmicta heeft de ambitie om met behulp van dit beleidsdocument de informatieveiligheid structureel naar een hoog niveau te brengen en daar te houden. Dit doet zij door het beschrijven van verantwoordelijkheden, taken en bevoegdheden en wet- en regelgeving. Het informatie-beveiligingsbeleid en de opvolging daarvan, moet Labmicta in staat stellen 'in control' en compliant te zijn. Labmicta heeft als uitgangspunt aantoonbaar te voldoen aan de norm NEN 7510 (Informatiebeveiliging in de zorg) door middel van certificering, en aan de hieruit volgende normen NEN 7512 (Vertrouwensbasis voor gegevensuitwisseling), NEN 7513 (Logging) en NTA 7516 (veilig mailen). Dit doen we middels het inrichten van een set van beheersmaatregelen.

In dit beleidsplan geven we weer wat we als laboratorium nastreven op het gebied van informatiebeveiliging. In sommige gevallen zijn en/of zullen afwijkingen in de praktijk worden geconstateerd ten opzichte van de hier geformuleerde beleidsregels. Geconstateerde afwijkingen zijn expliciet beschreven in dit beleidsplan, waarbij gelijk wordt aangegeven hoe we met deze afwijkingen omgaan (workaround). Belangrijk om te vermelden is dat we in dit document niet in detail aangeven hoe uitvoering wordt gegeven aan de doelstellingen en uitgangspunten. Deze gedetailleerde uitwerking is terug te vinden in de relevante SOP's (Standard Operating Procedures).

<u>Beschikbaarheid, Integriteit, Veiligheid</u>

In ons dagelijks werk zijn we steeds meer afhankelijk van informatiesystemen. De consequentie hiervan is dan ook dat verlies van gegevens ingrijpende gevolgen kan hebben. Voor systemen met patiëntgegevens is hoge beschikbaarheid tevens een belangrijke eis. Integriteit van de gegevens is ook zeker vereist. Verder behoort ter bescherming van de privacy voor alle persoonsgegevens de vertrouwelijkheid te worden gewaarborgd. Met deze eisen dienen we rekening te houden tijdens de inrichting van ons informatiebeveiligingsbeleid.

De basis van ons beleid is dat we meerdere zogenaamde veiligheidsschillen en verschillende middelen toepassen. De verschillende middelen die we toepassen zijn bijvoorbeeld technische, fysieke, procedurele of gedragsmiddelen. De verschillende middelen en schillen zijn complementair aan elkaar. De veiligheid die bereikt kan worden met technische middelen is slechts één van de lagen. Cruciaal voor een goede informatiebeveiliging is bijvoorbeeld de onvoorwaardelijke deelname hieraan van alle medewerkers zelf binnen Labmicta. Het is hiervoor belangrijk om te kijken naar wat we willen bereiken, welke maatregelen we daarvoor toepassen en hoe we ervoor kunnen zorgen dat het personeel zich kan houden aan deze maatregelen. Het goed faciliteren is belangrijk, zodat we er met z'n allen voor kunnen zorgen dat de beveiligingsmaatregelen in de praktijk werken en worden nageleefd.

<u>Niveaus van beveiliging</u>

Naast het inzetten van verschillende middelen zorgen we waar mogelijk altijd voor meerdere 'veiligheidsschillen'. Voor toegang tot alle applicaties is bijvoorbeeld eerst toegang tot een computer vereist en daarna nog een specifieke toegang tot de applicatie zelf. Daarbij kan het gebouw alleen betreden worden met een persoonsgebonden pas en voor bepaalde ruimtes (waaronder serverruimten en het magazijn) is een specifieke autorisatie voor toegangsdeuren vereist. Als een beheersmaatregel niet meer voldoet en/of buiten werking wordt gesteld zijn er dus altijd nog andere maatregelen in werking om de veiligheid te borgen.

4 Context van de organisatie

4.1 Inzicht in de organisatie en haar context

Labmicta heeft als belangrijkste doel om zo goed mogelijke diagnostische diensten (onderzoek en consult) te verlenen aan haar klanten. Dit, bekeken vanuit het oogpunt van informatiebeveiliging, brengt met zich mee dat we kijken naar hoe wij de beveiliging van de grote hoeveelheid gevoelige informatie kunnen waarborgen. Hierin zoeken we de balans tussen het verlenen van goede diagnostiek en consulten, het beveiligen van de beschikbare informatie, het waarborgen van de privacy van klanten en personeel en dit alles op een zo praktisch en kostenefficiënt mogelijke manier.

Het bewerken en beheren van de informatie en daarmee samenhangende informatiebeveiligingsbeleid kan niet losgezien worden van de partners van Labmicta, (data uitwisseling), wet en regelgeving (AVG, NEN 7510/7512/7513, NTA7516) en nieuwe ontwikkeling in de informatievoorziening in de zorg (bijvoorbeeld de PGO).

4.2 Inzicht in de behoeften en verwachtingen van belanghebbenden

Zowel Labmicta als organisatie alsmede de externe partners, zoals huisartsen en ziekenhuizen, en de cliënten wiens medische (laboratorium) data in beheer is van Labmicta stellen als eisen dat vertrouwd kan worden op de beschikbaarheid van de data. Daarbij dient de integriteit van data boven enige twijfel verheven te zijn. Het beschikbaar stellen van de data mag alleen plaatsvinden aan die die er toe gerechtigd zijn (medische behandelaar) of de client zelf. De informatiebeveiliging dient te beantwoorden aan de eisen gesteld zijn in de AVG en de relevante NEN regelgeving. In onze stakeholdersanalyse m.b.t. informatieveiligheid, staan de eisen en wensen van de belangrijkste betrokkenen beschreven.

4.3 Het toepassingsgebied van het managementsysteem voor informatiebeveiliging vaststellen

Labmicta draagt in brede zin zorg voor medisch microbiologisch laboratoriumonderzoek en consultatie ten behoeve van de diagnostiek, behandeling en preventie van infectieziekten bij de mens. Labmicta ondersteunt zo de 1e lijn, 2e lijn en de public health in de regio en heeft samenwerkingsverbanden buiten de regio.

Binnen vrijwel alle processen binnen Labmicta wordt gewerkt met de data of afgeleiden daarvan zodat gesteld kan worden dat informatiebeveiliging vrijwel alle processen van Labmicta raakt. Dit beleidsdocument is daarom leidend in alle (medische) data verwerkende processen binnen Labmicta.

4.4 Managementsysteem voor informatiebeveiliging

Gebruikmakend van de Zenya suite kunnen de functies van een zogenaamd ISMS (managementsysteem voor inrichting van de informatieveiligheid) worden gedefinieerd en uitgerold. Dit omvat het definiëren van beheersmaatregelen, onderkennen van de bijbehorende risico's, het monitoren daarop en het toepassen van verbetermaatregelen. Dit kan door taak-gestuurde opdrachten in een PDCA cyclus.

5 Leiderschap

5.1 Leiderschap en betrokkenheid

Het belang van het managementsysteem voor informatie beveiliging (ISMS) is door de directie van Labmicta als primair gedefinieerd. Dit doet zij door informatiebeveiliging en het ISMS op te laten nemen in de processen en daar waar nodig mensen en middelen beschikbaar te stellen voor de inrichting het beheer van het ISMS. Door het ISMS onderdeel te laten zijn van het algehele kwaliteitsmanagement systeem is geborgd dat ISMS een integraal onderdeel is van de processen binnen Labmicta. Het opnemen van ISMS en informatiebeveiligingsbeleid leidt er tevens toe dat de strategische richting van de organisatie kaders heeft meegekregen die voorwaardelijk zijn voor de uitvoering van de strategische keuzes.

5.2 Beleid

Om te borgen dat het informatiebeveiliging binnen Labmicta goed is georganiseerd en de lijnen duidelijk zijn, is het belangrijk om de verantwoordelijkheden en taken goed te beleggen. Door het beleggen van de verantwoordelijkheden en ons te houden aan de afspraken die hieronder staan beveiligen we de informatie en informatievoorziening van de organisatie. Het gaat hierbij ook om informatie(voorziening) waartoe externe partijen toegang hebben of die door externe partijen worden verwerkt of beheerd, of die naar externe partijen wordt gecommuniceerd.

De aangegeven afspraken zijn een samenstelling van gedragsfactoren, beleidskeuzes en communicatie. Deze zijn;

- Beveiliging van informatie is een onderdeel van de integrale managementverantwoordelijkheid van Labmicta.
- Alle medewerkers hebben een geheimhoudingsverklaring, als onderdeel van de arbeidsovereenkomst, getekend. Daarnaast heeft het medisch personeel zich te houden aan het medisch beroepsgeheim en al het overig personeel aan het afgeleide beroepsgeheim.
- De organisatie beschikt over een privacy-regelement en een huishoudelijk regelement waarin belangrijke zaken in het kader van de organisatie van de informatiebeveiliging en het zorgvuldig omgaan met (de toegang tot) gegevens zijn geregeld. Werknemers dienen zich hieraan te houden. Verwijzing naar richtlijnen zijn beschreven in bijlage 1.
- Voor het goed functioneren van de informatiebeveiliging is het noodzakelijk de rollen en verantwoordelijkheden van de verschillende functies te benoemen. Veel afdelingen en functionarissen binnen onze organisaties zijn bij informatiebeveiliging betrokken. Deze zijn beschreven in paragraaf 5.3
- Het is belangrijk om op de hoogte te blijven van de laatste ontwikkelingen op het gebied van informatiebeveiliging en de risico's die we lopen. De ontwikkelingen, vooral technisch, gaan razendsnel. Bij dergelijke ontwikkelingen is het belangrijk om in te schatten of wij grote risico's lopen en welke beveiligingsmaatregelen getroffen zouden kunnen worden.
- Ook externe partijen zijn betrokken bij onze informatievoorziening. Het is belangrijk dat de externe partijen voldoende beveiligingsmaatregelen in acht nemen en zich houden aan de geheimhouding. Vandaar dat wij schriftelijk afspraken met externe partijen maken, in de vorm van een verwerkersovereenkomst. In deze overeenkomsten worden afspraken gemaakt over het waarborgen van de beveiliging, privacy van gegevens en datalekken.
- Ook bij de aanschaf van nieuwe middelen voor de informatievoorziening dient er altijd aandacht te zijn voor de informatiebeveiliging. Daarom besteden wij hier in het goedkeuringsproces voor nieuwe middelen specifiek aandacht aan.
- Wij vinden het belangrijk om zorgvuldig met de beschikbare gegevens binnen de organisatie om te gaan. Daarom is er een gedragscode opgesteld, aanvullend op het privacy- en huishoudelijk regelement, samen met de medewerkers, waarin beschreven wordt hoe we omgaan met de gevoelige gegevens die beschikbaar zijn. Naast het opstellen van deze code zal er specifiek aandacht worden gegeven aan de naleving van deze code.

Een belangrijk onderdeel van de code is dat we geen herleidbare persoonsgegevens gebruiken en uitwisselen als dit niet strikt noodzakelijk is.

5.3 Rollen, verantwoordelijkheden en bevoegdheden binnen de organisatie

Directie De directie van Labmicta is eindverantwoordelijk voor alle (eigen) activiteiten binnen Labmicta en dus ook voor informatiebeveiliging. Deze verantwoordelijkheid voor informatiebeveiliging omvat: • beleidsvorming, het vaststellen van het informatiebeveiligingsbeleid en daaruit voortvloeiende richtlijnen; • het toezien op de naleving van het vastgestelde beleid; • het periodiek laten evalueren van de toepassing en werking van het beleid en • het stimuleren van het beveiligingsbewustzijn binnen de organisatie.
Functionaris gegevensbescherming De FG is de interne, onafhankelijke privacyfunctionaris ten dienste van de organisatie. De organisatie is verantwoordelijk voor het opstellen en uitvoeren van het privacy beleid. De FG ziet toe op de naleving hiervan en brengt advies uit over de risico's van bestaande verwerkingen en voorgenomen nieuwe producten en diensten. Voor de implementatie van de wet data lekken (onderdeel van de AVG) is het van belang om intern te borgen dat datalekken worden bijgehouden en dat er passende (zowel tijdelijk als structureel) maatregelen worden genomen bij een geconstateerd datalek. De meldplicht vanuit de AVG houdt namelijk in dat bedrijven, overheden en andere organisaties die persoonsgegevens verwerken datalekken moeten melden aan de Autoriteit Persoonsgegevens, en in bepaalde gevallen ook aan de betrokkene(n). Er is een datalek als er persoonsgegevens verloren zijn gegaan of onrechtmatig zijn verwerkt. Deze verantwoordelijkheden zijn belegd bij de functionaris gegevensbescherming. Deze functionaris kan betrokken worden in de beleidsvorming rond informatiebeveiliging en waar nodig aanschuiven bij de stuurgroep informatiebeveiliging. Er vindt periodiek overleg plaats tussen de FG en directie en tussen de FG en de informatiebeveiligingsfunctionaris, onder meer over de datalekregistratie en het voorkomen van datalekken. .
Betrokken afdelingen
Kwaliteitsdienst Kwaliteitszorg richt zich op een continue verbetering van de bedrijfsprocessen teneinde de gewenste kwaliteit te kunnen leveren voor onze aanvragers. Gewenste kwaliteit wordt bepaald door het management, de medewerkers, de klanten van de organisatie en de maatschappelijke omgeving waar de organisatie zich in begeeft. Informatiebeveiliging richt zich op de beschikbaarheid, integriteit en de vertrouwelijkheid van de informatievoorziening. Hiermee kan informatiebeveiliging een bijdrage leveren aan de kwaliteit van de bedrijfsvoering mede in relatie tot onze stakeholders.
Afdeling ICT De afdeling ICT is verantwoordelijk voor de instandhouding van de centrale geautomatiseerde informatievoorziening (hardware/voorzieningen). De maatregelen en manier van organiseren staat beschreven in het document "Informatiebeleid Labmicta"
Afdeling Applicatiebeheer De afdeling applicatiebeheer is verantwoordelijk voor de functionele instandhouding van applicaties waarin veelal geautomatiseerd patiënten informatie wordt opgeslagen en verwerkt.
Gebouwenbeheer Er is een belangrijke relatie tussen het fysieke beveiligingsbeleid en informatiebeveiliging, bijvoorbeeld daar waar het de beveiliging van computerruimten betreft. Maar ook de toegang tot het gebouw en verschillende ruimtes speelt een cruciale rol. Tevens moet in deze context gedacht worden aan noodstroomvoorzieningen voor minimaal

de essentiële processen binnen Labmicta.
Personeelszaken Er is een relatie tussen het personeelsbeleid en informatiebeveiliging, onder andere daar waar het de selectie, beheer en het ontslag van personeel betreft, maar ook de bescherming van de personeelsgegevens op zich. Dit dient op een zorgvuldige manier te geschieden met de waarborging van een goede informatiebeveiliging.

6. Planning

6.1 Risico beheersing

Voor beveiliging vormt het inventariseren van risico's en het beheersen hiervan een essentiële stap. De doelstelling van deze beheersmaatregel is dan ook om deze risico-inventarisatie en het beheer hiervan structureel vorm te geven. Het inventariseren van risico's doen we al op de relevante processen binnen Labmicta vanuit ons kwaliteitssysteem. Het gebruik van ons kwaliteitssysteem borgt dat we in staat zijn om op consistente wijze uitvoering te geven aan de inventarisatie. Het onderdeel informatie beveiliging sluit hierop aan zodat gebruik gemaakt kan van al aanwezig werkwijze, informatie en beleidsstukken. Dit op het gebied van kwaliteit, risicomanagement en de periodieke planning & control cyclus. Periodiek wordt er expliciet naar het informatiebeveiligingsbeleid gekeken. Dit wordt getoetst aan de hand van een PDCA cyclus waarbij gekeken wordt naar de kans van de risico's en de effectiviteit van de beheersmaatregelen. Er wordt elke twee jaar een algemene audit uitgevoerd. Daarnaast vinden er vanuit ons kwaliteitssysteem regelmatig andere audits plaats op afdelingen en/of rondom specifieke processen welke mede een raakvlak hebben met informatiebeveiliging.

We zijn ons bewust van het feit dat het implementeren van een 100% dichtgetimmerde beveiliging een utopie is. Voor het instellen van maatregelen maken we in lijn met de risico's de afweging tussen financieel haalbaar en praktisch hanteerbaar. Die afweging leidt er toe dat we altijd restrisico's lopen, al dan niet bewust. Belangrijk is om in te schatten welke restrisico's we lopen en te bepalen of we deze accepteren, mitigeren (PRIA) of gaan verzekeren. Momenteel heeft Labmicta een algemene aansprakelijkheidsverzekering die een aantal zaken in dit kader dekt. Ook zijn er op de markt speciale cyberverzekeringen die specifiek zaken op het gebied van informatiebeveiliging verzekeren (denk bijvoorbeeld aan ransomware). Periodiek zullen we bekijken of onze huidige verzekering de eventuele restrisico's voldoende dekt of dat we moeten overgaan tot het additioneel afdekken van (rest) risico's door middel van een al genoemde cyberverzekering. Bij het aangaan van "nieuwe" samenwerkingen of sluiten van overeenkomsten wordt tevens standaard geïnventariseerd of er een Verwerkersovereenkomst nodig is.

6.2 Informatiebeveiligingsdoelstellingen en de planning om ze te bereiken

In de NEN 7510 norm wordt gesteld dat het verstandig is om een systeem in te richten zodat het beheersen van de informatiebeveiliging wordt geborgd. Hiermee wordt een cyclus proces bedoeld, waarbij de PDCA-cyclus als uitgangspunt genomen wordt. De doelstelling van deze maatregel is dan ook om een raamwerk te beschrijven voor het organiseren van de informatiebeveiliging.

Goede informatiebeveiliging start initieel met het vaststellen en naleven van dit voorliggende beleidsplan waarin doelstellingen, uitgangspunten en beheersmaatregelen zijn vastgelegd. Hierin wordt feitelijk vastgesteld wat we willen bereiken met ons informatiebeveiligingsbeleid en hoe we dit doen (plan en do fase).

De stap daarna bestaat uit een gedegen risicoanalyse op basis van een periodieke audit waarmee we inzicht krijgen in de mogelijk risico's en in de kwaliteit en de effectiviteit van de bestaande beheersmaatregelen. Vervolgens worden in deze analyse risico's naar rato van hun impact ingedeeld. De relatie tussen de impact van een risico, de kans van optreden en de kosten en maatregelen om dat betreffende risico in te dammen bepaalt de houding en de

te ondernemen acties ten aanzien van een risico. Op basis van de uitkomsten van de risicoanalyse wordt een verbeterplan opgesteld, met een duidelijk tijdschema. Hierbij zal nadrukkelijk gekeken worden naar het opheffen, beheersen of accepteren van dit (rest-)risico (de act-fase).

Naast deze cyclus is een continue bewaking van groot belang. Dit doen we middels (periodieke) monitoring, evaluatie en controle. Monitoring betreft het continu bewaken van het niveau van informatiebeveiliging binnen Labmicta. Daar waar dit niveau (acuut) in gevaar komt door het optreden van bedreigingen treedt incidentmanagement in werking om het gewenste beveiligingsniveau te waarborgen of zo snel mogelijk te herstellen. Dit is een continu en cyclisch proces. Dit betekent dat op basis van de uitkomsten van evaluaties en controles of door nieuwe ontwikkelingen de noodzaak aanwezig kan zijn het informatiebeveiligingsbeleid aan te passen, een nieuwe risicoanalyse uit te voeren, extra maatregelen te treffen of de implementatie hiervan aan te passen. Ook is het mogelijk dat nieuwe ontwikkelingen, zoals de introductie van nieuwe bedrijfsprocessen of informatiesystemen, aanleiding geven om het informatiebeveiligingsbeleid te heroverwegen. Een dergelijke beoordeling vindt periodiek (tenminste elke 2 jaar) jaar plaats, of zoveel vaker als er noodzaak is door grote wijzigingen, en wordt geïnitieerd door de directie van Labmicta.

Deze werkwijze dient een structureel en integraal onderdeel uit te maken van het risicomanagementsysteem binnen Labmicta. Om te voldoen aan de NEN7510 norm is het belangrijk om het informatiebeveiligingsbeleid aanvullend op te nemen in het risico-managementsysteem van Labmicta. Zo wordt mede vanuit kwaliteit geborgd dat er periodiek een risicoanalyse voor informatiebeveiliging wordt uitgevoerd, en zo ook het beleid hieromtrent weer kan worden bijgesteld. Door in te stemmen met dit beleidsdocument wordt ook ingestemd met deze voorgestelde werkwijze.

De doelstellingen:

- Bewerkstelligen dat beveiliging integraal deel uitmaakt van informatiesystemen.
- Beschermen van de vertrouwelijkheid, authenticiteit of integriteit van informatie met behulp van cryptografische middelen.
- Voorkomen van fouten, verlies, onbevoegde modificatie of misbruik van informatie in toepassingen
- Beveiliging van systeembestanden bewerkstelligen.
- Beveiliging van toepassingsprogrammatuur en -informatie handhaven.

Om aan bovenstaande doelstellingen te voldoen, gelden de volgende afspraken:

- Bij de aanschaf van nieuwe systemen is er expliciete aandacht voor de beveiliging van deze systemen. Ook bij het installeren en/of ontwikkelen van software/applicaties is er altijd specifiek aandacht voor de beveiliging van gegevens en apparaten. Hierbij geldt dat security by design een belangrijk uitgangspunt is.
- Als er bij een systeem, applicatie of werkproces sprake is van verwerking van persoonsgegevens, dan wordt standaard een “Quickscan Gegevensverwerking” uitgevoerd, en zo nodig daaropvolgend een DPIA.
- De (vooral technische) ontwikkelingen die het beveiligingsbeleid raken gaan zo snel dat beleid en werkprocessen continu aan verandering onderhevig zijn. Wij zorgen voor een periodieke audit van het beleid dat opgenomen is in het KMS. Tevens is er elk kwartaal een overleg tussen de directie en de FG en een overleg tussen de IT-manager , manager bedrijfsbureau en de FG’s van Labmicta en LabPON waarin de belangrijkste zaken aan de orde komen. Daarbij hebben de betrokken afdelingen, denk hierbij bijvoorbeeld aan ICT en applicatiebeheer, een signalerende rol en functie als het gaat om het onder de aandacht brengen van belangrijke ontwikkelingen die invloed kunnen hebben op de informatiebeveiliging.
- De door Labmicta gehanteerde verwerkingsactiviteiten, zijn geregistreerd in een register van verwerkingsacitiveiten.
- Voor het voorkomen van fouten in de toepassing van de systemen werken wij met validatieprotocollen. Ook bij nieuwe systemen wordt een dergelijk protocol altijd toegepast. Wij controleren regelmatig de invoer in de systemen zelf om zo verwerkingsfouten te ontdekken en in de toekomst te voorkomen.

- Voor het testen van systemen, apparaten en applicaties wordt gebruik gemaakt van testpatiënten en testomgevingen. We werken zoveel mogelijk met testpatiënten maar soms zijn we genoodzaakt om real life te testen. Voor de verschillende systemen, applicaties en apparaten zijn afzonderlijke afspraken gemaakt hoe hiermee wordt gewerkt.
    - Er is aandacht voor het evalueren van technische kwetsbaarheden van de gebruikte informatiesystemen. Het verschilt per systeem of dit een proactieve of reactieve benadering is, afhankelijk van de ingeschatte risico's die we lopen. We werken steeds meer met proactieve monitoring-tools vanuit ICT en applicatiebeheer waardoor automatisch kwetsbaarheden worden geconstateerd en kunnen worden gerepareerd.
    - Wij vinden het van groot belang dat uitslagen op een goede manier getoond worden aan de aanvragers. Om hier nog meer controle over te krijgen is een centraal digitaal aanvraag- en uitslagensysteem noodzakelijk.
    - Er zijn afspraken in het kader van archivering en bewaartermijnen van gegevens.
    - Het is niet mogelijk voor medewerkers om eigen gekozen software of applicaties te installeren op het netwerk. Bij dergelijke verzoeken wordt gekeken naar de noodzaak en wordt de beveiliging altijd als onderwerp meegenomen in de afweging.
    - Het is regelmatig noodzakelijk dat andere personen meekijken in de computersessie van een medewerker. Denk hierbij intern aan ICT-medewerkers of applicatiebeheerders. Ook externe applicatiebeheerders hebben deze toegang regelmatig nodig om verstoringen te verhelpen aan apparaten of programma's. dit meekijken moet altijd kenbaar gemaakt worden aan de gebruiker en traceerbaar zijn. Als het om externen gaat zijn we soms afhankelijk van de software die de externe partij hiervoor gebruikt. Dit is een risico. Wij vinden het belangrijk om dit risico af te dekken. Dit doen we door de meest minimale rechten toe te kennen aan externe applicatiebeheerders.

7. Ondersteuning

7.1 Middelen

Informatiebeveiliging verlangt goed beheer van de middelen die voor de informatievoorziening worden gebruikt. Het begrip 'middelen' wordt hierbij ruim opgevat en omvat zowel gegevens en zaken die daaraan direct zijn gerelateerd, als overige voorzieningen (hardware/software/ installaties) die bij de informatievoorziening worden gebruikt. Het doel van dit onderdeel is het bereiken en handhaven van een adequate beveiliging van bedrijfsmiddelen van de organisatie. En tevens bewerkstelligen dat informatie een passend niveau van bescherming krijgt.

Hoe borgen wij dit?

- Alle afdelingen van Labmicta hebben maatregelen getroffen, al dan niet centraal geregeld, waardoor is gewaarborgd dat alleen geautoriseerde medewerkers gebruik kunnen maken van de informatie- en communicatievoorzieningen. (link naar toegangs en autorisatiebeleid)
- Toegang tot het algehele bedrijfsnetwerk is alleen mogelijk voor medewerkers met een password.
- Wij maken gebruik van een rechtenstructuur waarbij vooraf is gedefinieerd tot welke applicaties en met welke rechten een medewerker, rekening houdend met diens professionele bevoegdheden, toegang heeft tot ons bedrijfsnetwerk. Ook binnen applicaties worden waar nodig en mogelijk aparte rollen toebedeeld waardoor niet alle informatie gelijk vrijelijk toegankelijk is voor iedereen.
- Applicaties met veel gevoelige informatie (denk hierbij bijvoorbeeld aan de laboratorium-applicaties of de personeelsdossiers) zijn beschermd met een eigen (extra) inlogsysteem. Dit heeft als consequentie dat ook domein beheerders (zoals een ICT medewerker) niet in deze systemen kunnen kijken.
- Daar waar inlog vereist is, vindt logging plaats. Voor het centrale besturingssysteem worden alle foute inlogpogingen gelogd. De logging van GLIMS (het laboratorium-informatie-systeem van Labmicta) logt alle toegangen, mutaties, toegangspogingen en ook de communicatie van en naar GLIMS. Deze logbestanden zijn alleen beschikbaar voor domein beheerders en worden zo beschermd tegen onbevoegde toegang en manipulatie. Ook loggen we alle activiteiten op internet van onze medewerkers, dit is een onderdeel van de controletaak van ICT (beleid logging en controle op logging).
- Medewerkers die via 2FA inloggen krijgen via een remote desktop omgeving een lijst met applicaties tot zijn/haar beschikking die zij vanuit hun functie kunnen gebruiken. Dit is gelijk aan de rechten zoals deze gelden op de desktops..
- Externe partijen die via 2FA inloggen krijgen specifieke toegang via een remote desktop omgeving tot de benodigde server. Afhankelijk van de afgesproken bevoegdheden hebben ze toegang tot bepaalde applicaties en tot internet. Van externe partijen loggen we elke inlogpoging (de foute, maar ook de goede pogingen). De verstrekking van 2FA middelen vindt pas plaats na ondertekening van een convenant waarin afspraken staan weergegeven over onder andere een zorgvuldig gebruik van de beschikbare gegevens.
- Daarnaast zijn er nog andere systemen en apparaten waar patiëntgegevens worden opgeslagen en/of vanuit waar patiëntgegevens worden verstuurd. Ook hierbij geldt dat toegang tot de systemen en de daarin beschikbare gegevens, altijd apart verleend moet worden.
- De teamleiders op het laboratorium zijn verantwoordelijk voor een adequate beveiliging van deze middelen en leggen hierover ook verantwoording af.
- Ondanks de digitalisering van de samenleving gebruiken wij nog veel papier (bijvoorbeeld bij patiëntbesprekingen buiten de deur). Ons uitgangspunt is om dit gebruik geleidelijk verder terug te dringen omdat papier niet specifiek te beveiligen is. Het is makkelijk te verliezen en de gegevens die er op staan zijn niet te versleutelen. We kijken constant naar mogelijkheden om dit gebruik terug te dringen en besteden we aandacht aan het zo veilig mogelijk omgaan met gegevens op papier, zoals ze zo snel mogelijk vernietigen en/of

opbergen achter slot en grendel. Er zijn afspraken gemaakt over het vernietigen van vertrouwelijk gegevens op papier.

- We constateren dat er op steeds meer verschillende manieren wordt gecommuniceerd en wij vinden het erg belangrijk dat op een zorgvuldige manier met uitwisseling van gegevens wordt omgegaan. Het gaat hierbij met name om het delen van gegevens met derden (denk aan klanten, andere laboratoria of leveranciers) maar ook de beschikbaarheid van gegevens intern.
- Voor sommige functies is er toegang tot veel gegevens (bijvoorbeeld ICT, applicatiebeheer, personeelszaken, kwaliteitsdienst en het management). Wij volgen hierin het need-to-know principe en leggen de verantwoordelijkheid voor het zorgvuldig omgaan met de gegevens ook neer bij deze medewerkers zelf. Bekijk geen gegevens als je deze functioneel niet nodig hebt en deel geen gevoelige gegevens met collega's en externen als hij/zij deze gegevens niet nodig heeft voor de uitvoer van zijn/haar functie.
- Verzoeken voor het delen van data, intern of extern, buiten de normale en afgestemde communicatiestromen om, worden per geval beoordeeld waarbij we kritisch kijken naar het doel van de aanvraag. Indien medische diagnostische gegevens beschikbaar worden gemaakt dient uiteindelijk een arts-microbioloog zijn of haar akkoord te geven.
- Vanuit onze laboratoriumsystemen worden gegevens (met name uitslagen) verzonden naar de aanvragers van onderzoeken. Deze elektronische berichten uitwisseling gaat via een beveiligde lijn waarmee we waarborgen dat de informatie op een veilige manier bij de andere partij terecht komt.
- Bij externe hosting van onze gegevens wordt per geval beoordeeld of deze manier van hosting de veiligheid en privacy van gegevens waarborgt. We zien daarbij dat er steeds meer systemen en applicaties gebruik maken van gegevens in de 'Cloud' en bij een dergelijk verzoek wordt per geval afgewogen of dit wel of niet wordt toegestaan en wat mogelijke alternatieven zijn. Hierbij zal nadrukkelijk worden gekeken naar de juiste certificering door externe partijen rond databeveiliging met de minimale vereisten van NEN 7510 en ISO/IEC 27001 of ISAE 3402.

7.2. Competenties

De beheersmaatregelen op het onderdeel van competenties hebben als doel om te bewerkstelligen dat werknemers, ingehuurd personeel en externe gebruikers hun verantwoordelijkheden begrijpen en geschikt zijn voor de rollen waarvoor zij worden ingezet. Daarnaast hebben de beheersmaatregelen als doel om het risico van diefstal, fraude of misbruik van faciliteiten te verminderen. Daarbij zijn deze personen zich bewust van bedreigingen en gevaren voor informatiebeveiliging, van hun eigen verantwoordelijkheid en aansprakelijkheid en zijn ze toegerust om het beveiligingsbeleid van de organisatie in hun dagelijkse werkzaamheden te ondersteunen en het risico van een menselijke fout te verminderen.

Hoe borgen wij de beheersmaatregelen voor competenties?

- De betrokken afdelingen hierbij zijn met name de afdelingen personeelszaken en ICT. De meeste beheersmaatregelen op dit gebied worden toegepast door personeelszaken zoals de opgenomen verklaring geheimhouding in de arbeidsovereenkomsten en de werkwijzen omtrent indiensttreding en ontslag.
- Geven van bewustwordingstrainingen en informatie omtrent informatiebeveiliging.
- Zoals al aangegeven in paragraaf 7.1 zijn er voor het gebruik van de systemen, apparaten en applicaties rollen gedefinieerd. De afdelingshoofden/teammanagers beslissen wie welke rol toebedeeld mag krijgen. De afdeling ICT of applicatiebeheerders voeren deze autorisaties uit. Dit gebeurt in een digitaal proces waarbij achteraf getoetst kan worden of de juiste autorisaties zijn toegekend.
- Wij vinden het belangrijk dat de autorisaties voor toegang tot en binnen de softwareapplicaties passend zijn. Daarom worden elk half jaar de autorisaties van kritieke softwareapplicaties door de applicatiebeheerders gecontroleerd aan de hand van een de lijst geautoriseerde medewerkers per applicatie. Autorisaties waarover twijfels zijn, worden voorgelegd aan de betreffende afdelingsverantwoordelijke. Daarnaast wordt één keer per jaar een actuele lijst in zijn geheel te doorlopen in een overleg tussen de FG, afdelingsverantwoordelijken en bestuurder van Labmicta. Hierbij bekijken we ook gelijk wie (intern en extern) een Multi Factor

Authenticatie (MFA/2FA) tool heeft en welke autorisaties daarbij horen. Zo borgen we dat de autorisaties goed zijn ingericht en medewerkers geen onbevoegde toegang hebben tot gegevens.

- Bij overtreding van de regelgeving voor informatiebeveiliging kunnen disciplinaire maatregelen of sancties volgen, zie hiervoor het beleid “disciplinaire maatregelen of sancties”.
- Er zijn richtlijnen voor het in- en uit dienst treden van werknemers. In beide gevallen is specifiek aandacht voor de toegang tot en de omgang met privacy gevoelige gegevens. Ook zijn er door personeelszaken richtlijnen vastgesteld voor het beheer van de personeelsdossiers. Deze richtlijnen voldoen aan de AVG.(link toevoegen? Dit zijn HRM documenten)
- Voor informatiebeveiliging is het handelen van medewerkers een belangrijk onderdeel. Wij vinden het vertrouwen in de medewerkers zelf een groot goed. De verantwoordelijkheid voor de beveiliging van informatie en het zorgvuldig omgaan met gegevens is ook mede de verantwoordelijkheid van de medewerkers zelf. De laboratoria zullen hiervoor de juiste voorwaarden moeten scheppen waardoor het voor de medewerkers mogelijk is om zorgvuldig met de beschikbare gegevens om te gaan. Daarnaast wordt van medewerkers verwacht dat ze afwijkingen in de informatiebeveiliging signaleren. Het menselijk handelen is één van de belangrijkste factoren voor het waarborgen van de informatiebeveiliging, maar daarbij ook gelijk de minst beheersbare.

7.3 Bewustzijn

Door de medewerkers te wijzen op informatiebeveiliging, de risico’s van onbevoegd toegang (direct en indirect) te benoemen en te bespreken creëren we bewustzijn over informatiebeveiliging. Voor het creëren van bewustzijn is het van belang dat de medewerkers begrijpen op welke wijze zij een bijdrage kunnen leveren aan de doeltreffendheid van het managementsysteem voor de informatiebeveiliging. En dat in dat creëren van bewustzijn ook de consequenties worden opgenomen als er niet voldaan wordt aan de eisen van het managementsysteem voor informatie beveiliging.

7.4 Communicatie

Het beveiligingsbeleid wordt periodiek getoetst en waar nodig aangepast. Net als de relevante gedragscodes en externe informatie die binnen het KMS beschikbaar is voor de medewerkers. Indien het noodzakelijk is dat medewerkers kennis nemen van aangepaste beleidsdocumenten of veranderende regelgeving worden zij op de hoogte gesteld en zonodig worden zij uitgenodigd om de betreffende documenten te lezen. Binnen het KMS kan dit op eenvoudige wijze gerealiseerd worden door elke medewerker uit te nodigen en na het lezen van de documenten een leesbevestiging te laten invullen. Indien het van eminent belang is dat de medewerkers van Labmicta direct op de hoogte worden gesteld van een issue op het gebied van informatiebeveiliging kan vanuit de directie directe communicatie (via email en intranet) plaatsvinden.

7.5 Gedocumenteerde informatie

Alle documentatie aangaande informatiebeveiliging is opgenomen in het ISMS. Deze informatie is voor elke medewerker van Labmicta beschikbaar. Voor de verdere informatie wordt verwezen naar de paragrafen 7.1 en 7.2.

8. Uitvoering

8.1 Operationele planning en beheersing

Labmicta voldoet aan de informatiebeveiligingseisen en de in paragraaf 6.1 ‘Maatregelen om risico’s te beperken en kansen te benutten’ genoemde elementen door de benodigde processen te plannen, te implementeren en te beheersen.

8.2 Risicobeoordeling van informatiebeveiliging

Bij elke nieuw proces of aanpassing van een gegevensverwerkingsproces wordt er door de verantwoordelijk manager in samenwerking met de Kwaliteitsdienst en zonodig met advies van de FG een DPIA uitgevoerd. Dit om de risico’s in kaart te brengen van de gegevensverwerking. De DPIA’s en de besluitvorming erover worden uitgevoerd conform de richtlijnen van de Autoriteit Persoonsgegevens.

8.3 Informatiebeveiligingsrisico’s behandelen

Informatiebeveiligingsrisico’s en de beheersmaatregelen worden opgenomen in de risicomodule van het kwaliteitsmanagementsysteem. Afwijkingen worden afgehandeld binnen het reguliere meldingen systeem en de informatie van de afhandeling worden intern bewaard in het kwaliteitsmanagementsysteem conform ‘Bewaartermijnen materiaal en gegevens’.

9. Evaluatie van de prestatie

9.1 Monitoren, meten, analyseren en evalueren

De informatiebeveiliging wordt gemonitord binnen de risicomodule van het KMS door de Functionaris Gegevensbescherming. De informatiebeveiligingsprestaties en de doeltreffendheid voor de informatiebeveiliging wordt periodiek geëvalueerd. De gedocumenteerde informatie van de monitoring en evaluatie wordt binnen het KMS opgeslagen en bewaard conform "Bewaartermijnen materiaal en gegevens".

9.2 Interne audit

Minimaal iedere drie jaar wordt er een interne audit informatiebeveiliging uitgevoerd om informatie te verkrijgen voor informatiebeveiliging. Tijdens deze interne audit wordt getoetst of Labmicta voldoet aan de eisen van de organisatie voor haar managementsysteem voor informatiebeveiliging en de eisen van deze norm. Daarnaast wordt middels de structurele algemene interne audits mede beoordeeld of het informatiebeveiligingsbeleid doeltreffend geïmplementeerd en onderhouden is. In het document 'interne audit' staat informatie over het plannen van een auditprogramma, het vaststellen, implementeren en onderhouden met inbegrip van de frequentie, methoden, verantwoordelijkheden, planningseisen en rapportage.

9.3 Directiebeoordeling

De directie beoordeeld jaarlijks (MR) het managementsysteem voor informatiebeveiliging, om de continue geschiktheid en doeltreffendheid te bewerkstelligen. Bij de directiebeoordeling worden de volgende punten in overweging genomen:

- Status van de acties uit voorgaande directiebeoordelingen;
- Wijzigingen in externe en interne issues die relevant zijn voor het informatiebeveiligingsbeleid;
- Feedback over de informatiebeveiligingsprestaties;
- Feedback van belanghebbenden;
- Resultaten van risicobeoordeling en de status van het risicobehandelplan;
- Kansen voor continue verbetering.

De resultaten van de directiebeoordelingen leiden tot verbeterpunten en eventuele wijzigingen in het managementsysteem voor informatiebeveiliging. De resultaten van de directiebeoordelingen worden conform "Bewaartermijnen materiaal en gegevens".

10. Verbetering

10.1 Afwijkingen en corrigerende maatregelen en verbeteringen

10.1.1 Fysieke beveiliging van gebouw en beveiliging van de omgeving

De fysieke beveiliging van omgeving, gebouwen, ruimten en apparatuur is noodzakelijk ter voorkoming van verstoring van de informatievoorziening, diefstal van gegevens en bezittingen, beschadiging aan gebouwen en bezittingen en onveilige situaties voor patiënten, bezoekers en eigen en externe medewerkers.

Door deze maatregelen willen we voorkomen dat door onbevoegde fysieke toegang, schade aan of verstoring van het terrein en de informatie van de organisatie plaatsvindt. Ook is belangrijk om verlies, schade, diefstal of compromittering van bedrijfsmiddelen (informatie) en onderbreking van de bedrijfsactiviteiten te voorkomen.

En hoe doen we dit?

- Alle onderdelen van Labmicta, al dan niet centraal geregeld, hebben maatregelen getroffen voor de fysieke beveiliging van mensen en middelen, waaronder vertrouwelijke informatie en apparatuur waarop deze informatie is opgeslagen.
- Wij vinden het belangrijk dat niet iedereen zomaar het gebouw en bepaalde (hoog risico) afdelingen kan binnenkomen en hanteren daarom een streng toegangsbeleid. Onbevoegden mogen geen toegang krijgen tot onze faciliteiten en gegevens. Vandaar dat toegang tot het gebouw alleen mogelijk is met een persoonsgebonden pasje. Het gebouw, de parkeerplaatsen en (lift)deuren zijn niet toegankelijk voor onbevoegden.
- Bezoekers moeten zich registreren/inschrijven bij de receptie en krijgen een bezoekerspasje (welke altijd zichtbaar gedragen dient te worden) en moeten altijd worden opgehaald en weer worden weggebracht tot aan de receptie door degene die het bezoek heeft ontvangen en onder wiens verantwoording het toezicht berust.
- Voor het betreden van bepaalde ruimtes is een autorisatie op het pasje vereist via de leidinggevende, anders zal de toegang niet mogelijk zijn. Er zijn verschillende gebruikersgroepen gedefinieerd die toegang hebben tot specifieke ruimtes zoals de technische ruimten, ruimten met ICT voorzieningen, het magazijn, archief en de verschillende labs. Daarnaast werken we met een aanwezigheidsregistratie (aan- en afmelden bij de ingangen) waardoor achteraf gekeken kan worden wie waar aanwezig is geweest. Op strategische plekken om het gebouw zijn tevens camera's geïnstalleerd. Ook is er een inbraakbeveiliging en brandalarm.
- Voor de continuïteit van onze bedrijfsactiviteiten hebben wij een back-up protocol en herstelprocedure welke is belegd bij de afdelingen ICT, apparatenbeheer en applicatiebeheer. Wij vinden het erg belangrijk dat er minimaal tot geen dataverlies is bij een calamiteit en hebben daarvoor de benodigde beheersmaatregelen getroffen.
- Wij werken niet alleen maar op onze laboratoriumlocatie in Hengelo, maar ook thuis, in ziekenhuizen of op andere locaties. Wij vinden het daarom erg belangrijk dat bij het meenemen van apparatuur/informatie/programmatuur vanaf de centrale locatie er prominent aandacht is voor de beveiliging van deze informatie en de informatiedragers. Naast de beveiliging van de informatie is de beschikbaarheid van de gegevens erg belangrijk zodat personeel het werk goed kan uitvoeren, ook op een externe locatie. Enerzijds is dit een technische beveiliging. Anderzijds gaat het hier om menselijk handelen.

10.1.2 Beheer van communicatie en bedieningsprocessen

Goed beheer van (ICT) voorzieningen is van belang voor informatiebeveiliging. Het vastleggen van procedures en verantwoordelijkheden moet een correcte en veilige bediening van ICT-voorzieningen zo veel mogelijk waarborgen. Een goede planning en voorbereiding zijn noodzakelijk om te kunnen garanderen dat de correcte systeemcapaciteit en de correcte hulpbronnen beschikbaar zijn. De integriteit en beschikbaarheid van apparatuur, gegevens en

gegevensverwerkende diensten en communicatiediensten moet worden beschermd om het risico van beveiligingsincidenten tot een minimum te beperken.

Controle en stringente logging behoren tot de belangrijkste maatregelen ter beveiliging van patiëntgegevens. Effectieve controle op en logging van acties kunnen misbruik helpen ontdekken en maken het mogelijk op te treden tegen gebruikers die misbruik maken van hun bevoegdheden. Voor patiënten en artsen, die hun gegevens toevertrouwen aan elektronische informatiesystemen voor het verwerken van patiëntgegevens, is het belangrijk dat verantwoording wordt afgelegd over het gebruik van de gegevens en dat gestimuleerd wordt dat de gebruikers van die systemen zich houden aan de regels voor het juiste gebruik.

Wat willen we bereiken met de beheersmaatregelen op dit onderdeel?

- Een correcte en veilige toepassing van IT-voorzieningen.
- Voorkomen van onbevoegde openbaarmaking, modificatie, verwijdering of vernietiging van bedrijfsmiddelen of gegevens en. onderbreking van bedrijfsactiviteiten
- Het risico van systeemstoringen tot een minimum beperken.
- Beschermen van de integriteit van programmatuur en informatie.
- Handhaven van beveiliging van informatie en programmatuur die wordt uitgewisseld binnen een organisatie en met externe entiteiten.
- Handhaven van de integriteit en beschikbaarheid van informatie
- (Tijdig) ontdekken van onbevoegde informatieverwerkingsactiviteiten door internen of externen.

De implementatie en uitvoering van de volgende procedures leveren een bijdrage aan de geformuleerde doelstellingen:

- Alle onderdelen van Labmicta hebben, al dan niet centraal geregeld, maatregelen getroffen voor de beveiliging en het beheer van de operationele informatie- en communicatievoorzieningen. Maatregelen tegen allerlei vormen van kwaadaardige programmatuur (computervirussen, spam, spyware, ransomware en phishing) vormen hiervan een belangrijk onderdeel.
- Binnen Labmicta zijn bedieningsprocedures beschikbaar met betrekking tot de werking en het onderhoud van het apparatuur. Ook is er een werkwijze omtrent storingen en zijn er back-up procedures. Dit is belegd bij de afdelingen ICT, Applicatiebeheer en apparatuurbeheer.
- Voor het belangrijkste laboratorium-informatiesysteem (LIMS) binnen Labmicta (GLIMS) is een interne gebruikersgroep (2 maandelijks) ingesteld waarin wijzigingen, verbeteringen, meldingen en storingen worden besproken, bekeken en beoordeeld. Met het doel om het systeem zo optimaal mogelijk te laten functioneren en de continuïteit te borgen.
- Gegevens in de databases van deze systemen zijn goed beveiligd en kunnen voor het maken van bepaalde rapportages ingelezen worden. Voor GLIMS is de server alleen bereikbaar voor ICT beheerders. Met een ODBC koppeling worden opgevraagd, maar manipuleren van de data zelf is niet mogelijk.
- Bij de ontwikkeling en aanschaf/beheer van informatiesystemen besteden opdrachtgevers, projectleiders, ontwikkelaars en beheerders in alle fasen van het aanschaf- of ontwikkelingsproces nadrukkelijk aandacht aan informatiebeveiliging en dragen zij zorg voor de realisatie van de gestelde beveiligingseisen. Ook zijn voor de ontwikkeling van systemen afspraken gemaakt waardoor er voor wordt gezorgd dat de ontwikkel/test- en productieomgevingen worden gescheiden om zo de continuïteit van de productieomgeving te waarborgen.
- Er is een back-up beleid. De back-up servers (zogenaamde tweede MER (Main Equipment Room. De MER functioneert als centrale communicatieruimte in het netwerk van het gebouw) staan op een externe locatie zodat bij bijvoorbeeld een brand dit niet verloren gaat. Tevens is de hoofd MER (intern in ons pand) uitgerust met een moderne blusinstallatie.
- Ook willen wij bij een verstoring de ICT processen snel weer werkend hebben. Daarom is sinds de nieuwbouw (eind 2014) een deel van de infrastructuur redundant uitgevoerd. Door redundantie zorgen we er bijvoorbeeld voor dat als zich ergens een breuk in de kabel voordoet de verbinding via andere lijnen doorgaat.

- Bij de nieuwbouw is specifieke aandacht geweest voor de beveiliging en veiligheid van ruimten, systemen, materiaal en gegevens. Het gebouw is voorzien van no-break voorzieningen op afdelingen en een noodstroomaggregaat waarop eventueel extra capaciteit kan worden ingeplugd. Bij calamiteiten (bijvoorbeeld een brand) of sabotage kan Labmicta door draaien zonder verlies van capaciteit of data. Tevens is er een moderne brandmeldinstallatie en een alarmsysteem aanwezig in het gebouw om zo een calamiteit snel te ontdekken waardoor snel ingrijpen mogelijk is.
- Technisch zijn er maatregelen getroffen voor bescherming tegen virussen en andere kwaadaardige programmatuur middels een zogenaamde antivirusscanner. Ons gehele bedrijfsnetwerk is daarnaast beschermd door een next generation firewall waardoor we zijn uitgerust met de bescherming die voldoet aan de laatste technologische ontwikkelingen. Laptops zijn additioneel met een persoonlijke firewall beschermd. We controleren wekelijks inbreukpogingen op de firewall, van buitenaf naar binnen, maar ook van binnen naar buiten. De afdeling ICT volgt de ontwikkelingen op dit gebied en zal waar nodig voorstellen doen richting de stuurgroep voor extra beveiligingsmaatregelen als ze dit nodig achten.
- Het is niet toegestaan om met eigen apparaten een verbinding te leggen via de netwerkpoorten naar ons bedrijfsnetwerk. Het is dus niet toegestaan om eigenstandig een kabel in te pluggen aan een netwerkpoort. Hiervoor zijn ook al technische maatregelen genomen. Ongebruikte netwerkpoorten moeten eerst worden vrijgegeven als daar een nieuw apparaat in wordt aangekoppeld. Wel is het mogelijk in gebruikte netwerkpoorten ander apparatuur in te pluggen waardoor in theorie onbeveiligde apparatuur kan worden aangesloten op ons netwerk. Dit kan wel worden beveiligd maar is een erg administratief belastende configuratie. Omdat niet iedereen zomaar toegang heeft tot het pand en wij van onze medewerkers verwachten dat er op een zorgvuldige manier wordt omgegaan met de beschikbare apparaten/informatie is er vooralsnog niet voor gekozen deze extra beveiligde technologie door te voeren maar in dit plan aan te geven dat het niet wordt toegestaan.
- Naast netwerkpoorten zijn er ook USB-poorten waarop randapparatuur kan worden aangesloten. Wij willen niet dat, niet door ons beveiligde externe USB randapparaten (bijvoorbeeld een privé USB-sticks of externe harddisk), worden aangesloten op ons netwerk. Dit brengt een groot beveiligingsrisico met zich mee doordat er zo vervuilde bestanden en systemen ons netwerk kunnen opkomen. Ook is het mogelijk om zo gegevens onbevoegd te verspreiden. De complicatie is dat een deel van onze apparatuur via USB poorten werkt. Een generiek beleid om onbevoegd gebruik van USB poorten te verhinderen dient nog uitgewerkt te worden.
- Alle email en internet verkeer wordt op ‘malicious code’(kwaadaardige code) gescand en dit verkeer wordt geblokkeerd waar nodig. Wel is het belangrijk dat er aandacht blijft, bij de medewerkers, voor het niet openen van vreemde e-mail en bijlagen, zeker van een onbetrouwbare bron, om zo geen vervuilde e-mail en bestanden binnen te krijgen. Bij twijfel dient altijd de ICT-afdeling te worden geraadpleegd. Daarnaast zullen we hier structureel aandacht aan besteden tijdens de plenaire sessies omtrent informatiebeveiliging.
- De informatie op draagbare apparaten wordt versleuteld opgeslagen. Bij diefstal of verlies zijn de gegevens (zoals uit de e-mail) voor derden niet toegankelijk. Dit geldt dus voor laptops, mobiele telefoons en USB-sticks. De afdeling ICT verstrekt beveiligde USB-stick waar de data geëncrypt wordt opgeslagen.
- Het is niet mogelijk om met BYOD laptops en andere apparatuur rechtstreeks verbinding te maken met ons bedrijfsnetwerk. Toegang wordt dan verleent via de remote desktop omgeving inclusief 2FA. Dit zorgt ervoor dat de data niet op het werkstation kan komen, waarmee je op remote desktop inlogt. Data wordt (dus) niet opgeslagen op de (externe) laptop/computer. Er worden persoonlijke tokens uit te geven zodat dan worden gelogd wie wanneer welke toegang heeft gekregen. Link maken naar het BYOD beleid?
- Als medewerkers op een externe locatie inloggen, bijvoorbeeld thuis, wordt regelmatig gebruik gemaakt van privéapparatuur. Doordat we met een beveiligde verbinding werken en een remote desktop, vormt dit geen beveiligingsrisico. Pas na toestemming van de direct leidinggevende krijgt een medewerker de beschikking over een persoonlijk token en laptop. Een telefoon kan tevens ter beschikking worden gesteld. ICT zorgt voor dat deze apparaten afdoende beveiligd zijn.
- De medewerker tekent een document waarin de medewerker aangeeft zorgvuldig om te gaan met de verkregen apparatuur en de daarop staande gegevens.

- Privégebruik van bedrijfsapparatuur is om beveiligingsredenen niet toegestaan, waarbij onder strikte voorwaarden kortstondig gebruik toegestaan kan worden. Een voorbeeld hiervan is de gedragscode internet en e-mailgebruik waarin staat vermeld dat het internetsysteem aan de werknemer voor zakelijk gebruik beschikbaar wordt gesteld. Gebruik is derhalve verbonden met taken die voortvloeien uit de functie. Werknemers mogen het internetsysteem voor persoonlijke doeleinden, bij uitzondering gebruiken, mits dit niet storend is voor de dagelijkse werkzaamheden en het computernetwerk en het beperkt blijft tot incidenteel en kortstondig gebruik. Het is niet de bedoeling om voor eigen persoonlijk gewin bedrijfsapparatuur te gebruiken.
- Aan het gebruik van internet zijn risico's verbonden die nopen tot het stellen van gedragsregels. Tegen de achtergrond van deze risico's wordt van werknemers verantwoord gebruik van internet en e-mail verwacht. Om de risico's te verkleinen is de toegang tot bepaalde internetsites afgeschermd. Dit gaat op basis van best effort en overleg met de stuurgroep Informatie beveiliging. Het is namelijk niet mogelijk om alles vooraf te blokkeren. Er wordt gekeken of middels het afdwingen van gedragsregels het doel ook bereikt kan worden. Hierbij is het vooral belangrijk om geen excessief gebruik van bijvoorbeeld privégebruik van internet toe te staan. Het toezien hierop is wel van essentieel belang. Als functioneel het noodzakelijk is om (kortstondig) toegang te krijgen tot bepaalde nu afgeschermde internetsites moet dit worden overleg met leidinggevende en ICT.
- Alle communicatiemiddelen die door het bedrijf ter beschikking zijn gesteld zijn afdoende beveiligd om gevoelige gegevens mee te verwerken. Om deze beveiligingsreden is het niet mogelijk om zelf applicaties en software te installeren op de computer. Als het functioneel nodig is om iets te installeren is dit alleen mogelijk in overleg met leidinggevende en ICT.
- We delen alleen gegevens die gedeeld mogen worden. Als we gegevens delen zorgen we voor een betrouwbare en zorgvuldige levering en deling van deze gegevens.
- Naast het beveiligen van de informatie in onze databases is een veilige manier van het verzenden van informatie zeer belangrijk. De afspraak is dat gegevens die privacygevoelig zijn altijd beveiligd, anoniem of niet herleidbaar verstuurd worden. De beveiliging van het e-mailverkeer wordt verzorgt door een beveiliging van de email via derde partijen. Tevens wordt bij het verzenden van e-mail een beveiligde verbinding opgebouwd, via TLS1.2. Als de ontvangende server dit niet ondersteund vallen we terug op een niet beveiligde verbinding.
- Gegevens mogen niet zomaar gedeeld worden. Vandaar dat wij in de gedragscode er specifiek op zullen wijzen om geen gegevens op te slaan, te kopiëren of te verzenden naar privé-apparatuur.
- Als oplossing voor het veilig delen van informatie grote hoeveelheid informatie is het pakket Sharefile geïmplementeerd, waardoor medewerkers de mogelijkheid hebben om documenten op een veilige manier met andere personen te delen. Het gebruik van cloudopslagsystemen is niet toegestaan en wordt dan ook geblokkeerd.
- Op de medische administraties zijn de werkwijzen omtrent het aanvraag- en uitslagenproces beschreven waarbij prominente aandacht is voor het zorgvuldig omgaan met patiëntengegevens. Naast de normale (digitale) uitslagprocessen worden ook uitslagen telefonisch of per fax doorgegeven. Hier zijn strikte richtlijnen voor met waarborgen voor de beveiliging van de gegevens en waarborgen voor de privacy van de klanten/patiënten waarbij de verificatie van de juiste (vragende) persoon een hoge prioriteit heeft. Aan dit onderwerp wordt specifiek aandacht besteed in de bewustwordingssessies omtrent informatiebeveiliging. We bespreken dan hoe we klantgericht zijn en tegelijkertijd de privacy van klanten en beveiliging van gegevens kunnen borgen.
- Digitale informatie wordt beschermd tegen onbevoegde toegang middels rechtenstructuur. We stellen per gebruiker (aan de hand van rechtengroepen, rollen) in waar hij/zij bij mag op het bedrijfsnetwerk. Voor niet digitale informatie zijn minder duidelijke afspraken gemaakt (bijvoorbeeld; wat berg je op achter slot en grendel en is dus niet voor iedereen beschikbaar). Wij vinden het belangrijk dat ook deze informatie goed beschermd wordt.
- We installeren op systemen waarop ingelogd kan worden SSL-certificaten waar mogelijk, zodat gebruikersnaam en wachtwoord niet kunnen worden afgeluisterd. Een SSL-certificaat zorgt ervoor dat alle informatie tijdens het transport vertrouwelijk blijft en niet leesbaar is door derden. Een voorbeeld hiervan is dat onze internetsites zijn versleuteld via SSL.

- Wij zorgen ervoor dat alle netwerkcomponenten, servers, werkstations en firewalls worden gelijkgesteld aan een interne tijdserver. De tijdserver in kwestie haalt van onze provider de juiste (atoomklok)tijd op. Dit is belangrijk om fouten (tijdverschillen) in registraties tegen te gaan. Daarnaast is het belangrijk om de continuïteit van de systemen te waarborgen.
- We beschikken we over een beveiligde, versleutelde dark fiber verbinding met een commercieel datacentrum in Enschede . Een dark fiber verbinding is een niet gedeelde glasvezel verbinding. Hierdoor is het mogelijk om een veilige en snelle verbinding tot stand te brengen omdat het netwerkverkeer het eigen netwerk niet verlaat. Van daaruit is het mogelijk om verbindingen met andere locaties te maken. Het datacentrum in Enschede is verbonden met Ndix waarop meerdere datacentra zijn aangesloten. Hierdoor is het mogelijk om ook verbindingen te gaan leggen met andere externe locaties om zo een veilige en snelle verbinding tot stand te brengen. De data wordt over de lijnen versleuteld verstuurt. Dit zorgt er voor dat we op een snelle, uniforme en veilige manier onze data naar bepaalde locaties kunnen verzenden.

10.1.3 Toegangsbeveiliging

Toegangsbeveiliging moet ervoor zorgen dat toegang tot voorzieningen en gegevens wordt verleend aan gebruikers die daartoe zijn gerechtigd en wordt geweigerd aan anderen. Het doel ervan is te waarborgen dat het lezen, toevoegen, wijzigen en verwijderen van gegevens en programmatuur alleen door bevoegden en gecontroleerd kan plaatsvinden.

Toegang tot gegevens moet worden beperkt met het oog op de integriteit en vertrouwelijkheid van de informatie. De beschikbaarheid kan echter tegenovergestelde eisen stellen. De classificatie van gegevens is bepalend voor de te treffen maatregelen. Toegangsbeveiliging strekt zich uit over alle middelen voor de informatievoorziening: centrale computers, netwerken, werkstations, systeem- en toepassingsprogrammatuur en gegevens. Voor verschillende middelen kunnen verschillende eisen worden gesteld aan de toegangsbeveiliging. Aan de andere kant kunnen verschillende gebruikers van dezelfde middelen ook verschillende toegangsrechten hebben. Toegangsbeveiliging is dus bijzonder complex.

Daarnaast kunnen zich bovendien omstandigheden voordoen die het nodig maken in bepaalde gevallen de reguliere toegangsbeveiliging te doorbreken. Dan moet controle achteraf mogelijk zijn. De toegangsbeveiliging zal daarom moeten voorzien in mogelijkheden voor registratie van verleende toegang. De beheersmaatregelen in dit kader leveren een bijdrage aan de volgende doelstellingen:

- Toegang voor bevoegde gebruikers bewerkstelligen en onbevoegde toegang tot informatiesystemen voorkomen.
- Voorkomen van onbevoegde toegang door gebruikers, en van beschadiging of diefstal van informatie en IT voorzieningen.
- Het voorkomen van onbevoegde toegang tot netwerkdiensten, besturingssystemen en tot informatie in toepassingssystemen.
- Beheersen van de toegang tot informatie.
- Waarborgen van informatiebeveiliging bij het gebruik van draagbare computers en faciliteiten voor telewerken.

De al genoemde maatregelen hebben deels overlap met de maatregelen die belangrijk zijn om de toegangsbeveiliging te waarborgen. Een aantal (aanvullende) specifieke maatregelen in dit kader:

- Wij hanteren een algemeen geaccepteerd wachtwoord richtlijn(complexiteit en lengte wachtwoord) en geen streng wachtwoordbeleid voor ons bedrijfsnetwerk ondanks dat er in onze systemen veel gevoelige gegevens worden opgeslagen. Onderzoek wijst uit dat een te streng wachtwoordbeleid niet perse leidt tot een hogere veiligheid. Tevens kunnen onbevoegden niet zomaar ons pand te betreden en trachten gebruik te maken van ons netwerk. Daarnaast is voor toegang tot de gevoelige gegevens altijd nog een extra inlog in een bepaald systeem nodig waarmee een extra barrière is ingebouwd. Voor draagbare apparaten die buiten het pand

worden gebruikt hebben wij nog een extra toegangsbeveiliging ingebouwd zoals al beschreven in eerdere paragrafen.

- We gebruiken zo min mogelijk algemene accounts (dus toegang komt dan niet tot stand op persoonlijke titel maar wordt door een persoon uit een gedefinieerde groep tot stand gebracht) omdat controle op goed gebruik daarvan lastig is. Acties kunnen niet worden teruggeleid naar één persoon, wat ervoor kan zorgen dat er minder veilig omgaan wordt met de beschikbare gegevens. Voor extra inlog in systemen met privacy gevoelige gegevens mogen nooit algemene accounts gebruikt worden.
- De inzet is een clean desk en clean screen policy. Wij vinden het uitermate belangrijk dat gevoelige gegevens niet zomaar te benaderen zijn. In de gedragsregels omtrent zorgvuldig omgaan met gevoelige gegevens wordt hier aandacht aan besteed.
- Inactieve computersessies worden automatisch ontoegankelijk gemaakt na een vooraf afgesproken time-frame (900 seconden). Er moet altijd een balans worden gevonden tussen enerzijds de beveiliging en anderzijds de werkbaarheid. Het is wel belangrijk om een goed tijdslot in te bouwen zodat gegevens niet lang onbeheerd toegankelijk zijn en blijven. Bijvoorbeeld na reguliere werktijd en in algemene ruimten, zoals vergaderzalen, is het niet wenselijk dat gevoelige informatie voor anderen beschikbaar is. Momenteel geldt het afgesproken tijdslot ook voor laptops.
- Naast de net genoemde technische maatregel (beeldschermbeveiliging) is het belangrijk dat medewerkers altijd de computer vergrendelen bij het verlaten van de werkplek. De automatische beeldschermbeveiliging is een maatregel voor als de medewerkers dit zelf vergeten. Hier wordt aandacht voor gevraagd in de gedragscode.

10.1.4 Beheer van informatiebeveiligingsincidenten

Belangrijk om te bewerkstelligen is dat informatiebeveiligingsgebeurtenissen en (structurele) zwakheden die verband houden met informatiesystemen zodanig kenbaar worden gemaakt dat tijdig corrigerende maatregelen kunnen worden genomen. Daarnaast moet ook worden bewerkstelligd dat een consistente en doeltreffende benadering wordt toegepast voor het beheer van informatiebeveiligingsincidenten.

Hoe hebben wij dit geïmplementeerd?

- Er is een intern meldingssysteem beschikbaar en daarbij kunnen afwijkingen altijd gemeld worden bij de verantwoordelijke afdeling (ICT, applicatiebeheer of apparatuurbeheer). Bij twijfel is de functionaris gegevensbescherming te raadplegen. Evenals datalekken worden informatiebeveiligingsincidenten geregistreerd in een instellingsregister.
- Voor de nieuwe wet data lekken (onderdeel van de AVG) is een functionaris aangesteld die datalekken bijhouden en op basis daarvan de organisatie adviseert over hoe dat te voorkomen is.
- Om de aard, omvang en kosten van informatiebeveiligingsincidenten te kunnen kwantificeren en te volgen zijn meerdere werkwijzen beschikbaar. Als er iets aan de hand is met een specifieke applicatie wordt dit door de applicatiebeheerders opgepakt Als er wat mis is met de ICT-infrastructuur wordt dit door de afdeling ICT opgepakt. En als er een belangrijk informatiebeveiligingsincident is, wordt dit opgepakt door de functionaris gegevensbescherming.

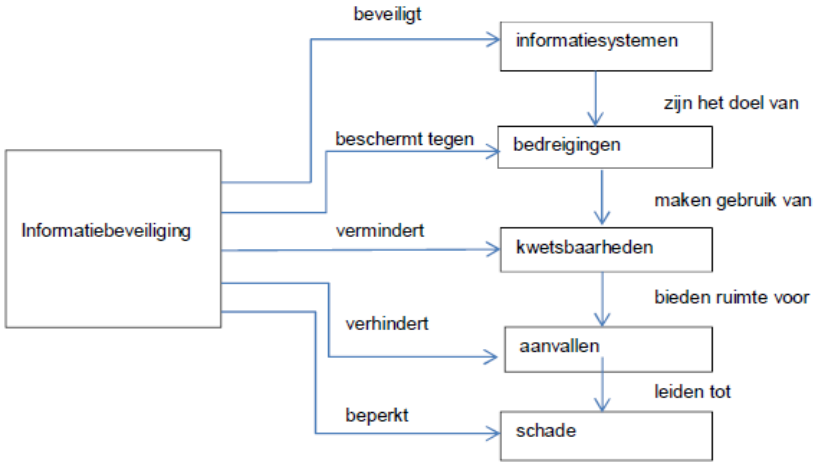
10.1.5 Bedrijfscontinuïteitsbeheer

Belangrijk is om het onderbreken van bedrijfsactiviteiten tegen te gaan en kritische bedrijfsprocessen te beschermen tegen de gevolgen van omvangrijke storingen in informatiesystemen of rampen en om tijdig herstel te bewerkstelligen.

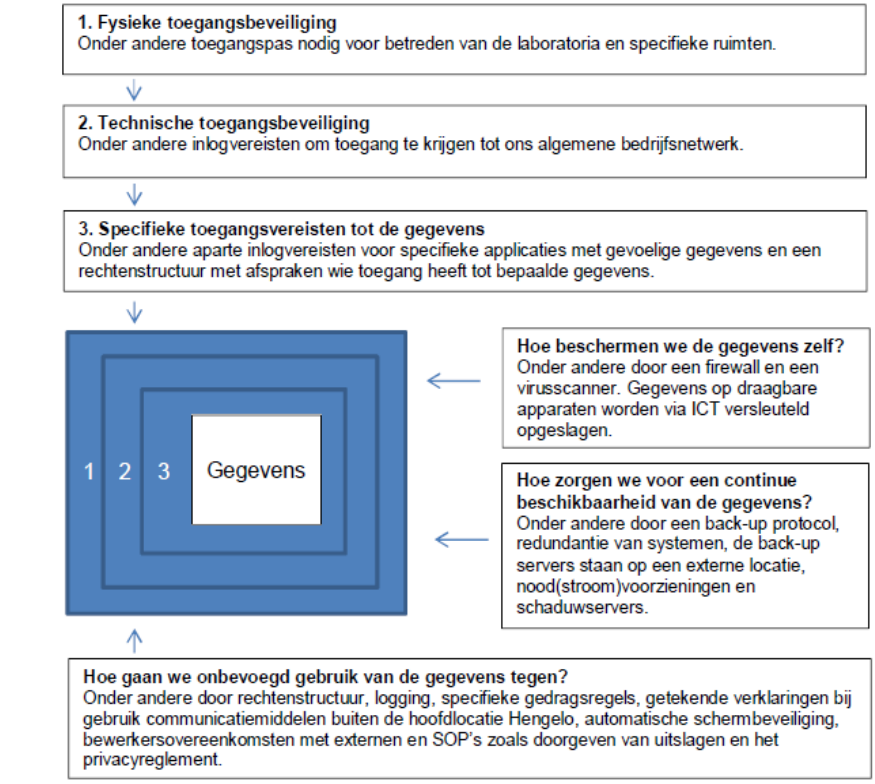
Veel beheersmaatregelen zijn al eerder besproken zoals het back-up beleid. In dit kader is er een calamiteitenplan en een noodprocedure voor de verschillende afdelingen waardoor geborgd wordt dat na een onderbreking of uitval de beschikbaarheid van informatie op het vereiste niveau zo snel mogelijk beschikbaar komt om zo de bedrijfsactiviteiten (grotendeels) te handhaven of snel te herstellen.

Bijlagen

Bijlage 1: Basis van ons informatiebeveiligingsbeleid



Figuur 1 - 'Speelveld' van informatiebeveiliging



Figuur 2 - Basis van ons informatiebeveiligingsbeleid