Informatiebeveiligingsbeleid Coöperatie Dichtbij (511-1)

2 juli, 2018

Voorwoord

Als zorgcoöperatie zijn wij verantwoordelijk voor patiëntenzorg. Het leveren van kwaliteit staat bij het uitvoeren van deze taak voorop. Om deze kwaliteit aan de patiënten en andere betrokkenen te kunnen bieden is een betrouwbare informatievoorziening essentieel. De betrouwbaarheid van de informatievoorziening moet zijn gewaarborgd ongeacht de vorm, dus zowel handmatig, bijvoorbeeld in de papieren zorgdossiers, als geautomatiseerd, denk aan het gebruik van Nedap, internet en e-mail. Uitgebreide aandacht voor de beveiliging van de opslag, verwerking en uitwisseling van informatie is continu vereist. Vandaar dat ik dit informatiebeveiligingsbeleid u van harte aanbeveel.

Jort Schuringa

Voorzitter Raad van Bestuur Coöperatie Dichtbij U.A.

Versiebeheer

Versie	Datum	Auteur	Omschrijving
1.0	15 december 2015	Jork Netten	Basis beleid
1.1	8 januari 2016	Jork Netten	Aanpassing beleid op basis van gevoerde audit (risico-analyse) en nieuwe (toekomstige) processen.
1.2	12 februari 2016	Jork Netten	Aanpassen beleid, beleid iets minder streng om het praktisch en werkbaar te houden. Na aandringen van personeel en risico-analyse zijn er bepaalde onderdelen aangepast.
1.3	1 maart 2017	Jork Netten	Onderdelen zijn na een risicoanalyse aangepast.
1.4	2 juli 2018	Jork Netten	Wijzingen AVG doorgevoerd.
1.5	30 juli 2018	Jork Netten	Begonnen met het toevoegen van een 'white list' (hoofdstuk 16). Het blijkt soms voor gebruikers onduidelijk te zijn welke systemen wel zijn goedgekeurd en welke niet. Hierdoor zijn enkele keren systemen voor algemene informatie gebruikt die nog niet waren goedgekeurd.
1.6	31 juli 2018	Desi Meijer	Omzetten in juiste huisstijl

Inhoudsopgave

1. Inleiding

Dit document beschrijft het beleid van de coöperatie met betrekking tot de beveiliging van informatie. De informatievoorziening is van essentieel belang voor de continuïteit van de bedrijfsvoering van de coöperatie. Zowel op papier als geautomatiseerd zijn wij bij ons dagelijks werk afhankelijk van de beschikbaarheid van betrouwbare informatie. 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. Het proces van informatiebeveiliging begint met het definiëren van een beleid op dit punt. Dit beleid is vastgelegd in het onderhavige document.

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 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. 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.

1.2 Doelstelling informatiebeveiligingsbeleid

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

Met het opstellen van het informatiebeveiligingsbeleid wordt invulling gegeven de NEN-norm 7510, Informatiebeveiliging in de zorg, van het Nederlands Normalisatie Instituut.

1.3 Doelstelling informatiebeveiliging

Zoals in de voorgaande definitie is verwoord, richt informatiebeveiliging zich op de volgende drie 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.

1.4 Werkingsgebied

Het informatiebeveiligingsbeleid is van toepassing op de gehele coöperatie. Het informatiebeveiligingsbeleid is ook van toepassing op de gegevensuitwisseling van de coöperatie met andere organisaties. Het beleid richt zich op onze eigen medewerkers, tijdelijk personeel en op personeel dat door derden wordt ingezet om diensten te verlenen aan de coöperatie.

1.5 Verantwoordelijkheid informatiebeveiligingsbeleid

De RvB is eindverantwoordelijk voor het informatiebeveiligingsbeleid. De RvB mag echter bepaalde taken delegeren.

1.6 Ondersteunende documentatie

Dit informatiebeveiligingsbeleid is binnen de coöperatie verder uitgewerkt in de volgende documenten;

- Handboek kwaliteit van zorg

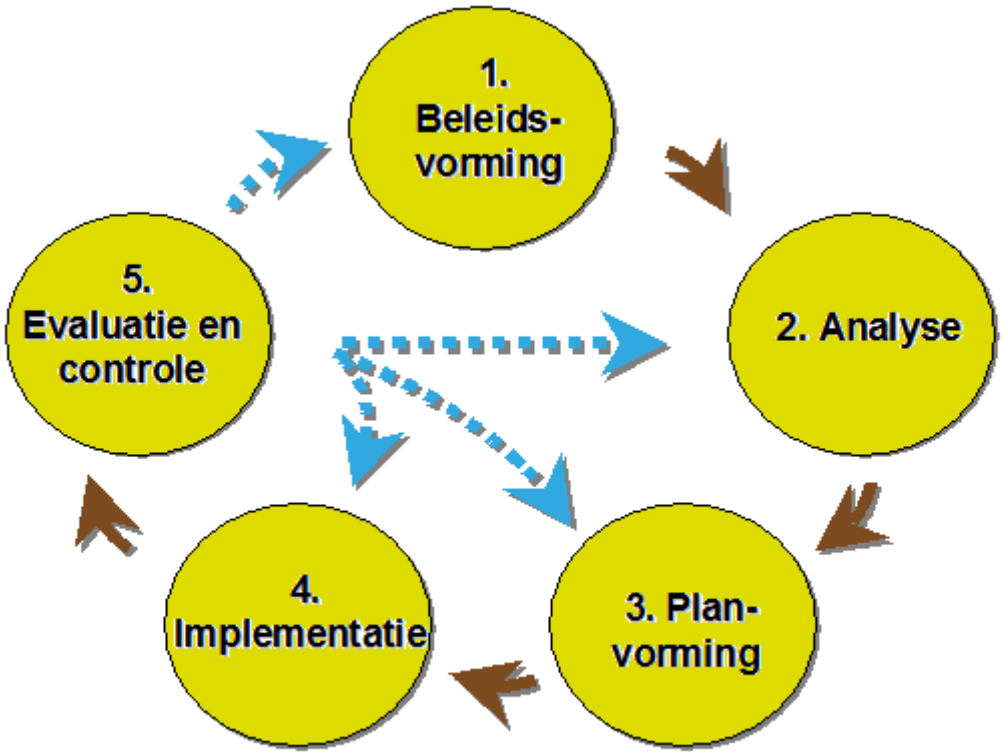
1.7 Inhoud informatiebeveiligingsbeleid

In hoofdstuk 2 wordt aandacht besteed aan het beleidsproces voor informatiebeveiliging. Vervolgens wordt in hoofdstuk 3 de organisatie van informatiebeveiliging omschreven. Daarna wordt in hoofdstuk 4 de uitgangaspunten van informatiebeveiliging beschreven. In hoofdstuk 5 wordt de basis van risicobeheersing beschreven. Vervolgens behandelen we in hoofdstuk 6 de verwijzingen die binnen dit document staan, zodat het terug te leiden is naar een informatie- en registratiesysteem. In hoofdstuk 7 wordt het verdere beheer van bedrijfsmiddelen besproken. Hoofdstuk 8 beschrijft het beleid omtrent personeel en de daarbij horende veiligheidsrisico's. Vervolgens wordt in hoofdstuk 9 de fysieke beveiliging en beveiliging van de omgeving omschreven. Daarna gaan we verder in hoofdstuk 10 verder in op de beheer van communicatie- en bedieningsprocessen. Om daarna weer in te gaan op de toegangsbeveiliging in hoofdstuk 11. In hoofdstuk 12 wordt de verwerving, ontwikkeling en onderhoud van informatiesystemen beschreven. Vervolgens gaan we in hoofdstuk 13 verder in op het beleid met betrekking tot de beheer van informatiebeveiliging, onder andere de registratie van incidenten wordt in dit hoofdstuk behandeld. In hoofdstuk 14 wordt bedrijfscontinuniteitsbeheer behandeld en ten slotte wordt in hoofdstuk 15 de naleving behandeld van dit document.

2. Beleidsproces voor informatiebeveiliging

2.1 Overzicht beleidsproces informatiebeveiliging

Het beleidsproces voor informatiebeveiliging omvat de volgende vijf stappen.



In de volgende paragrafen worden deze vijf stappen toegelicht.

2.1.1 Beleidsvorming

Zoals ook aangegeven in paragraaf 1.1, start het beleidsproces voor informatiebeveiliging met het opstellen van het informatiebeveiligingsbeleid. In dit beleid worden de doelstellingen en uitgangspunten voor informatiebeveiliging van de coöperatie vastgelegd. Hiermee vormt het beleid de leidraad voor de overige stappen van het beleidsproces.

2.1.2 Analyse

De tweede stap van het beleidsproces voor informatiebeveiliging bestaat uit analyse van de bestaande situatie. Deze analyse wordt zowel op centraal als op decentraal binnen de coöperatie uitgevoerd. Het analyseren van de bestaande situatie heeft tot doel:

- Inzicht te krijgen in de kwaliteit van de bestaande beveiligingsmaatregelen.

- Inzicht te krijgen in de risico's die de realisatie van het gewenste beveiligingsniveau in gevaar kunnen brengen.
- Het gewenste niveau van informatiebeveiliging vast te stellen in de vorm van een classificatie van bedrijfsprocessen en informatiesystemen.

Over de uitkomsten van de analyses van bestaande situaties voor informatiebeveiliging wordt op centraal niveau gerapporteerd aan de Raad van Bestuur en op decentraal niveau aan de leiding van het desbetreffende organisatieonderdeel.

2.1.3 Planvorming

Op basis van de uitkomsten van de analyses van bestaande situaties voor informatiebeveiliging wordt, zowel op centraal als op decentraal niveau, een informatiebeveiligingsplan opgesteld. In dit plan worden de verbeteractiviteiten voor de realisatie van het gewenste beveiligingsniveau op projectmatige wijze vastgelegd.

Het informatiebeveiligingsplan wordt op centraal niveau vastgesteld door de Raad van Bestuur en op decentraal niveau door de leiding van het desbetreffende organisatieonderdeel

2.1.4 Implementatie

Aan de hand van het informatiebeveiligingsplan wordt de implementatie van de aanvullende beveiligingsmaatregelen ter hand genomen. Dit betekent onder andere het opstellen van richtlijnen en procedures voor informatiebeveiliging, het invoeren van beveiligingshulpmiddelen en het voorlichten en opleiden van management en medewerkers.

2.1.5 Evaluatie en controle

De laatste stap van het beleidsproces voor informatiebeveiliging bestaat uit evaluatie en controle. Met betrekking tot informatiebeveiliging worden de volgende controlevormen onderscheiden:

- Operationele controle op de naleving van het informatiebeveiligingsbeleid en de hieruit voortvloeiende richtlijnen en maatregelen.
- Controle op de voortgang van de implementatie en borging van het informatiebeveiligingsbeleid en de hieruit voortvloeiende richtlijnen en maatregelen.
- Onafhankelijke controle.

De organisatie van deze controle en de afspraken voor de bijbehorende rapportage wordt in hoofdstuk 4 nader uitgewerkt.

2.2 Cyclisch proces

Het beleidsproces voor informatiebeveiliging is een continue en cyclisch proces. Dit betekent dat op basis van de uitkomst van evaluaties en controles of door nieuwe ontwikkelingen de noodzaak aanwezig kan zijn om het informatiebeveiligingsbeleid aan te passen of om extra beveiligingsmaatregelen te treffen. Ook is het mogelijk dat nieuwe ontwikkelingen, zoals de introductie van nieuwe bedrijfsprocessen of informatiesystemen aanleiding geven om het informatiebeveiligingsbeleid te heroverwegen.

3. Organisatie van informatiebeveiliging

In dit hoofdstuk wordt de organisatie van informatiebeveiliging binnen de coöperatie beschreven. Het is van groot belang dat de verantwoordelijkheden, taken en bevoegdheden met betrekking tot informatiebeveiliging op een eenduidige wijze zijn toegewezen. Deze toewijzing heeft tot doel te voorkomen dat zaken dubbel worden uitgevoerd of dat de uitvoering van beveiligingstaken achterwege blijft. Bovendien levert de toewijzing van taken en verantwoordelijkheden de mogelijkheid om decharge te verlenen voor de uitgevoerde werkzaamheden.

De organisatie van informatiebeveiliging wordt beschreven volgens de volgende invalshoeken:

- Generieke rollen voor informatiebeveiliging, waarbij de rollen van RvB, Leidinggevenden, Eigenaar, functionaris gegevensbescherming, beheerder, en gebruiker worden onderscheiden;
- rollen en functies voor informatiebeveiliging binnen de coöperatie.

Tenslotte wordt in dit hoofdstuk ook aandacht besteed aan de manier waarop controle en rapportage is vormgegeven.

3.1 Generieke rollen voor informatiebeveiliging

Voor ieder informatiesysteem en gegevensverzameling worden de volgende rollen en de bijbehorende verantwoordelijkheden toegewezen.

Rol	Verantwoordelijkheden
RvB	Eindverantwoordelijke
Leidinggevenden	Het leveren van de meest recente informatie van medewerkers, tijdelijk personeel (tevens zzp'ers) en derden die diensten verlenen aan de coöperatie.
Eigenaren	Beslissingsrecht voor het informatiesysteem, c.q. de gegevensverzameling. Bepalen van de beveiligingseisen
Functionaris gegevensbescherming	Ziet er op toe, dat er geen exposure plaatsvindt. Heeft een toezichthoudende rol. Daarnaast is de functionaris gegvensbescherming het contactpersoon met de overheid en andere partijen op het gebied van gegevensbescherming.
Beheerder(s)	Operationele instandhouding van het informatiesysteem, c.q. de gegevensverzameling. Ziet toe op een juiste werking van het informatiesysteem, c.q. de gegevensverzameling.
Gebruiker	Toepassing van het informatiesysteem, c.q. de gegevensverzameling. beveiligings knelpunten aangeven. Naleving van beveiligingsrichtlijnen en Procedures.

Personen kunnen verschillende rollen vervullen en rollen kunnen ook deels buiten de coöperatie liggen. De verschillende betrokkenen maken onderling afspraken over de uitvoering van de

(beveiligings)taken en leggen deze desgewenst vast in dienstverleningsovereenkomsten (bijvoorbeeld in SLA's).

3.2 Rollen en functies voor informatiebeveiliging

Wat betreft al of niet gedelegeerde deeltaken is verantwoordelijkheid als volgt belegd:

Rol	Verantwoordelijken
Opstellen en evalueren van het beleidsdocument	RvB
Signaleren van nieuwe bedreigingen	Eigenaren
Goedkeuring van beveiligingsinitiatieven	RvB
Goedkeuring van middelen voor informatievoorziening	Leidinggevenden
Toezien op contracten	Eigenaren
Toezien op en bespreken van beveiligingsincidenten	Eigenaren
Contact met officiële instanties ingeval van beveiligingsincidenten	Functionaris gegevensbescherming
De bescherming van bedrijfsmiddelen	Eigenaren
Het uitvoeren van voor informatiebeveiliging relevante processen	Leidinggevenden

3.3 Controle en rapportage over informatiebeveiliging

Met betrekking tot informatiebeveiliging worden de volgende controlevormen onderscheiden:

- operationele controle op de naleving van het informatiebeveiligingsbeleid en de hieruit voortvloeiende richtlijnen en maatregelen.
- controle op de voortgang van de implementatie en borging van het informatiebeveiligingsbeleid en de hieruit voortvloeiende richtlijnen en maatregelen.
- onafhankelijke controle.

Operationele controle op de naleving van beleid en richtlijnen wordt verricht door het management. Hierover vindt geen formele rapportage plaats.

Voortgangscontrole en -rapportage vindt twee maal per jaar plaats. De status van de voortgang van de coöperatie brede beveiligingsmaatregelen wordt dan gecontroleerd en gerapporteerd.

Onafhankelijke controle met betrekking tot informatiebeveiliging wordt uitgevoerd door een externe partij die hiervoor voldoende gekwalificeerd voor is, veelal in overleg en in samenwerking met de externe accountant. De verantwoordelijken beschreven in paragraaf 3.3 worden over de uitkomsten van de controles geïnformeerd, waarbij de RvB verantwoordelijk is voor het feit dat zij worden geïnformeerd.

4. Uitgangspunten informatiebeveiliging Coöperatie Dichtbij

Bij de toepassing van informatiebeveiliging binnen de coöperatie worden de volgende uitgangspunten gehanteerd:

1. De coöperatie streeft ernaar aantoonbaar te voldoen aan de norm NEN 7510, Informatiebeveiliging in de zorg.
2. De coöperatie voldoet aan alle, van toepassing zijnde, wet- en regelgeving. In dit verband worden genoemd:
    a. Algemene Wet Bijzondere Ziektekosten
    b. Geneesmiddelenwet
    c. Kwaliteitswet zorginstellingen
    d. Algemene Verordering Gegevensbescherming (AVG)
    e. Wet gebruik burgerservicenummer in de zorg
    f. Wet klachtrecht cliënten zorgsector
    g. Wet kwaliteit, klachten en geschillen zorg (Wkkgz)
    h. Wet maatschappelijke ondersteuning
    i. Wet marktordening gezondheidszorg
    j. Wet op bijzondere medische verrichtingen
    k. Wet op de beroepen in de individuele gezondheidszorg
    l. Wet op de geneeskundige behandelingsovereenkomst
    m. Wet op de medische hulpmiddelen
    n. Wet op het bevolkingsonderzoek
    o. Wet publieke gezondheid
    p. Wet toelating zorginstellingen
    q. Zorgverzekeringswet
3. Beveiliging van informatie is een onderdeel van de integrale managementverantwoordelijkheid. Alle onderdelen van de coöperatie hebben hiertoe verantwoordelijkheden voor informatie-beveiliging toegewezen en vastgelegd. De in hoofdstuk 4 beschreven organisatie van informatiebeveiliging vormt hierbij de leidraad.
4. Wanneer (onderdelen van) de coöperatie 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.
5. De bedrijfsprocessen, informatiesystemen en gegevensverzamelingen van alle onderdelen van de coöperatie zijn volgens een gestructureerde methode geclassificeerd naar de aspecten beschikbaarheid, integriteit en vertrouwelijkheid.
6. De coöperatie voert een actief beleid om het beveiligingsbewustzijn van management en gebruikers te stimuleren.
7. De coöperatie beschikt over een duidelijk beleid voor het gebruik van (algemene) informatievoorzieningen. Op de naleving van het beleid wordt toegezien.
8. Bij overtreding van de regelgeving voor informatiebeveiliging en/of relevante wettelijke bepalingen kan de RvB een sanctie opleggen conform het beleid opleggen.
9. In de coöperatie zijn maatregelen getroffen voor de fysieke beveiliging van mensen en middelen, waaronder vertrouwelijke informatie en apparatuur waarop deze informatie is opgeslagen.
10. In de coöperatie zijn 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.

11. In de coöperatie zijn maatregelen getroffen waardoor is gewaarborgd dat alleen geautoriseerde medewerkers en derden gebruik kunnen maken van de informatie- en communicatievoorzieningen.
12. Bij de ontwikkeling en aanschaf van informatiesystemen wordt in alle fasen van het aanschaf- of ontwikkelingsproces nadrukkelijk aandacht besteed aan informatiebeveiliging.
13. In de coöperatie zijn adequate maatregelen getroffen waardoor de beschikbaarheid van de bedrijfsprocessen en de hierbij gebruikte informatie(systemen) is gewaarborgd, zowel in normale als in buitengewone omstandigheden.
14. Als onderdeel van het beleidsproces voor informatiebeveiliging wordt binnen de coöperatie door interne en externe partijen toegezien op de naleving van het informatiebeveiligingsbeleid.
15. De coöperatie beschikt over middelen voor het melden en afhandelen van beveiligingsincidenten. De evaluatie van de afhandeling van beveiligingsincidenten wordt benut voor de verbetering van informatiebeveiliging.

5. Risicobeheersing

5.1 Beveiligingsniveaus

Zoals eerder beschreven, het informatiebeveiliging maakt onderscheid tussen de kwaliteitsaspecten beschikbaarheid, integriteit en vertrouwelijkheid.

- **Beschikbaarheid**: de mate waarin gegevens of functionaliteit op de juiste momenten beschikbaar zijn voor gebruikers;

- **Integriteit**: de mate waarin gegevens of functionaliteit correct zijn;

- **Vertrouwelijkheid**: de mate waarin de toegang tot gegevens of functionaliteit beperkt is tot degenen die daartoe bevoegd zijn.

Wat betreft beveiligingsmaatregelen worden drie niveaus onderscheiden:

- **Laag (L)**: Verstoring van de beschikbaarheid , integriteit en/of vertrouwelijkheid van de informatie veroorzaakt een belemmering in een van de secundaire processen, maar niet van ernstige of onomkeerbare aard. De verstoring brengt geen merkbare schade toe, mogelijk enig ongemak / lichte schade aan het imago van de instelling;

- **Middel (M)**: Een inbreuk op de beschikbaarheid, integriteit en/of vertrouwelijkheid van informatie veroorzaakt een verstoring in een van de primaire processen, maar niet van zeer ernstige of onomkeerbare aard. Ook mogelijke negatieve effecten voor het imago van de instelling kunnen aanleiding zijn om de classificatie 'gevoelig' toe te kennen.

- **Hoog (H):** Aantasting van beschikbaarheid, integriteit en/of vertrouwelijkheid veroorzaakt een zeer ernstige of onomkeerbare verstoring van een van de primaire processen, brengt ernstige schade toe aan het imago van de coöperatie of houdt een ernstige wetsovertreding in.

5.2 Risicobeheersing

Via classificatie kunnen de risico's die gemoeid zijn met informatie en informatiesystemen effectief en efficiënt worden beheerst. Daarbij worden deze middelen ingedeeld in verschillende risicoklassen die elk een verschillend niveau van beveiligingsmaatregelen kennen. De beheersing zit hem in het implementeren van alle maatregelen zoals bepaald door de toegekende risicoklasse. Aanvullend worden gebruikers gevraagd informatie te behandelen overeenkomstig de risicoklasse van de informatie met de richtlijnen zoals deze van kracht zijn binnen de Coöperatie. Bij informatiebeveiliging worden twee type bedrijfsmiddelen onderscheiden:

- Informatiesystemen;
- Overige hardware.

Deze middelen hebben een Eigenaar die verantwoordelijk zijn voor de algemene veiligheid en werking van het systeem. De Eigenaar bepaalt de risicoklasse van deze middelen.

Welke acties er ondernomen moet worden is op basis van de vraag of één van de onderdelen (Beschikbaarheid, Integriteit en Vertrouwelijkheid) een "Hoog" als classificatie heeft. Dit is schematisch weergegeven in bovenstaande figuur. Een informatiesysteem moet als 'H' worden bestempeld als het niet beschikbaar zijn van het systeem (B), het uitlekken van informatie (V) en/of het incorrect zijn van de informatieverwerking (I) leidt tot (een kans op) onacceptabele schade voor de coöperatie of als daarmee de instelling met (de kans op) dergelijke incidenten een ernstige

overtreding van wet- en regelgeving begaat. Dit is onder meer het geval als het systeem door optredende schade slechts zeer kort niet beschikbaar mag zijn, als er sprake is van zeer vertrouwelijke persoonsgegevens of als een verwerkingsfout (schending van integriteit) kan leiden tot zeer hoge kosten.

Als een informatiesysteem informatie verwerkt die als 'geheim' is bestempeld, geldt het beveiligingsniveau 'Hoog" en is een volledige risicoanalyse nodig die kan resulteren in extra maatregelen. Bij het inventariseren, analyseren en minderen van risico's dient uiteindelijk de Verantwoordelijke te besluiten tot het treffen van extra maatregelen, door af te wegen of de kosten en inspanning die gemoeid zijn met de implementatie van aanvullende beveiligingsmaatregelen opwegen tegen de mogelijke schade als gevolg van het manifest worden van onderkende risico's. Als een Verantwoordelijke besluit tot extra maatregelen dienen de set van extra maatregelen en het accepteren van restrisico in de vorm van een beveiligingsplan te worden gedocumenteerd.

De Verantwoordelijke kan op verschillende manieren met (rest-)risico's omgaan.

Mogelijke strategieën zijn:

1. Risicomijdend
Besluiten om in verhouding veel – zo veel als redelijkerwijs mogelijk is - in beveiliging(smaatregelen) te investeren om zo min mogelijk risico te lopen. Op de langere termijn kan dit resulteren in hogere kosten voor de organisatie voor maatregelen dan kosten die door incidenten zouden zijn veroorzaakt, die de organisatie via maatregelen heeft ingeperkt;

2. Risiconeutraal
Besluiten om te maken kosten voor beveiliging(smaatregelen) vergelijkbaar te laten zijn met de kosten (schade) die incidenten over een langere periode gezien (bijvoorbeeld jaarlijks) veroorzaken;

3. Accepteren
Besluiten om risico te lopen c.q. accepteren, waardoor de organisatie in verhouding minder in beveiliging(smaatregelen) hoeft te investeren. Op de langere termijn kan dit resulteren in hogere kosten voor de organisatie door incidenten dan zou zijn uitgegeven om deze incidenten in te perken. De keuze voor een bepaalde strategie dient door de Verantwoordelijke bewust te worden gemaakt. Het accepteren van restrisico's dient te worden gedocumenteerd.

6. Referenties

In dit hoofdstuk staan de referenties naar de (digitale) documenten die de werking van dit document bewerkstelligen.

7. Beheer voor bedrijfsmiddelen

Doelstelling:
Bereiken en handhaven van een adequate bescherming van bedrijfsmiddelen van de organisatie.

7.1 Inventarisatie van bedrijfsmiddelen

Alle bedrijfsmiddelen behoren duidelijk te zijn geïdentificeerd en er behoort een inventaris van alle belangrijke bedrijfsmiddelen te worden opgesteld en bijgehouden.

Bij de inventarisatie van de bedrijfsmiddelen is vooral de aandacht gevestigd op die middelen die te maken hebben met informatiebeveiliging. En hierbij weer voornamelijk patiënt en personeelsinformatie.

Alle bedrijfsmiddelen worden geïdentificeerd, geregistreerd, geclassificeerd en gedocumenteerd. Daarbij wordt ook direct aangegeven wie verantwoordelijk is voor het desbetreffende bedrijfsmiddel.

7.1.1 Eigendom van bedrijfsmiddelen
Zie paragraaf 7.1.

7.1.2 Aanvaardbaar gebruik van bedrijfsmiddelen
Er behoren regels te worden vastgesteld, gedocumenteerd en geïmplementeerd voor aanvaardbaar gebruik van informatie en bedrijfsmiddelen die verband houden met IT-voorzieningen.

De uitwerking van het beleid, zogenoemd de voorwaarden voor het gebruik van de IT-voorzieningen, worden vastgesteld in de gebruikersovereenkomst. Deze gebruikersovereenkomst dient iedereen te tekenen die gebruik maakt van één of meerdere informatiesystemen of andere IT-voorzieningen van de coöperatie.

7.2 Classificatie van informatie

Doelstelling:
Bewerkstelligen dat informatie een geschikt niveau van bescherming krijgt.

7.2.1 Richtlijnen voor classificatie
Informatie behoort te worden geclassificeerd met betrekking tot de waarde, wettelijke eisen, gevoeligheid en onmisbaarheid voor de organisatie.

Informatie wordt geclassificeerd met betrekking tot de beschikbaarheid, integriteit en vertrouwelijkheid voor de coöperatie. De coöperatie classificeert alle assets, waaronder informatiesystemen.

7.2.2 Labeling en verwerking van informatie
Er behoren geschikte, samenhangende procedures te worden ontwikkeld en geïmplementeerd voor de labeling en verwerking van informatie overeenkomstig het classificatiesysteem dat de organisatie heeft geïmplementeerd.

De coöperatie kent geen voorschriften of procedures voor het labelen van informatie. In beginsel dient alle informatie als ‘Intern’ te worden geclassificeerd en overeenkomstig te worden behandeld. De Eigenaar van de informatie kan in samenspraak met zijn of haar direct Leidinggevende, als de situatie dat vereist, de rubricering aanpassen naar ‘Laag’ dan wel ‘Middel’ of ‘Hoog’.

8. Personeel

Binnen de Coöperatie kennen we verschillende "soorten" arbeidsverhoudingen en overeenkomsten, waarbij alle gebruikers van informatiesystemen aan dezelfde verplichtingen moeten voldoen. Hierna te noemen: gebruikers.

8.1 Voorafgaand aan de overeenkomst

Doelstelling:
Bewerkstelligen dat werknemers, ingehuurd personeel en externe gebruikers hun verantwoordelijkheden begrijpen, en geschikt zijn voor de rollen waarvoor zij worden overwogen, en om het risico van diefstal, fraude of misbruik van faciliteiten te verminderen.

8.1.1 Rollen en verantwoordelijkheden

De rollen en verantwoordelijkheden van werknemers, ingehuurd personeel en externe gebruikers ten aanzien van beveiliging behoren te worden vastgesteld en gedocumenteerd.

Aangezien alle gebruikers dezelfde plichten hebben omtrent informatieveiligheid en gebruik van informatiesystemen wordt hier alleen gebruik gemaakt van het begrip "gebruikers". Er wordt bijgehouden welke rechten een gebruiker heeft bij de informatiesystemen dan wel tot andere bronnen van informatie. Degene die deze rechten registreert (de direct leidinggevende dan wel iemand die het op basis van schriftelijke toestemming heeft verkregen) is verantwoordelijk voor de correctheid en volledigheid van de registratie.

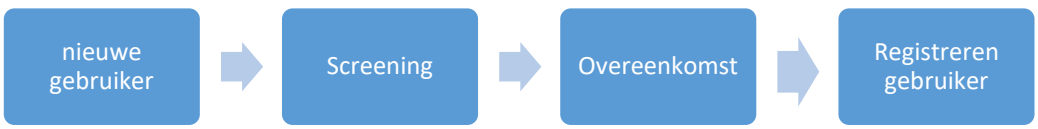
8.1.2 Screening

Verificatie van de achtergrond van alle kandidaten voor een dienstverband, ingehuurd personeel en externe gebruikers behoren te worden uitgevoerd overeenkomstig relevante wetten, voorschriften en ethische overwegingen, en behoren evenredig te zijn aan de bedrijfseisen, de classificatie van de informatie waartoe toegang wordt verleend, en de waargenomen risico's.

Voordat gebruikers worden aangemeld bij Coöperatie Dichtbij wordt gevraagd naar referenties bij de laatste werkgever of opdrachtgever (zakelijk) of referenties vanuit de omgeving (persoonlijk). Indien een gebruiker nog geen zakelijke referenties kan overleggen zal deze eis komen te vervallen en zal er een screening plaats vinden op basis van een internet check. Een internet check bestaat uit het volgende:

1. Zoekmachine zoekopdracht "naam persoon"
2. Kijken in hoeverre cv overeenkomt met Linkedin
3. Sociale kanalen bekijken (Twitter, Facebook, Linkedin, Instagram).

Hieronder staat de flow diagram visueel weergegeven.



8.2 Tijdens het dienstverband

Doelstelling:
Bewerkstelligen dat alle werknemers, ingehuurd personeel en externe gebruikers zich bewust zijn van bedreigingen en gevaren voor informatiebeveiliging, van hun verantwoordelijkheid en aansprakelijkheid, en dat ze zijn toegerust om het beveiligingsbeleid van de organisatie in hun dagelijkse werkzaamheden te ondersteunen, en het risico van een menselijke fout te verminderen.

8.2.1 Directieverantwoordelijkheid

De directie en het management behoort van werknemers, ingehuurd personeel en externe gebruikers te eisen dat ze beveiliging toepassen overeenkomstig vastgesteld beleid en vastgestelde procedures van de organisatie.

De leidinggevende is te allen tijde verantwoordelijk voor het in control zijn met betrekking tot informatieveiligheid. Dit betekent dat het vastgestelde informatiebeleid wordt uitgevoerd door de desbetreffende afdeling en teams onder zijn of haar verantwoordelijkheid. Leidinggevenden zijn tevens verantwoordelijk voor ingehuurd personeel en derden die onder zijn of haar afdeling valt.

8.2.2 Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging

Alle werknemers van de organisatie en, voor zover van toepassing, ingehuurd personeel en externe gebruikers, behoren geschikte training en regelmatige bijscholing te krijgen met betrekking tot beleid en procedures van de organisatie, voor zover relevant voor hun functie.

Bij de aanstelling van gebruikers die informatiesystemen dan wel andere informatie van de coöperatie gaan gebruiken is het verplicht om de gebruikersovereenkomst te tekenen voor aanvang. Pas op het moment dat de gebruikersovereenkomst is ondertekend zal toegang tot de informatie en informatiesystemen worden verleend. Hiermee wordt er getracht om bij aanvang al direct bewustzijn te creëren ten aanzien van informatiebeveiliging.

Periodiek, maar tenminste één maal per jaar wordt er een training gegeven voor gebruikers om bewustzijn ten aanzien van informatiebeveiliging te vergroten.

Periodiek, maar tenminste één maal per jaar wordt er een e-mail gestuurd met hierin informatie omtrent informatieveiligheid.

Daarnaast dienen leidinggevenden activiteiten te verrichten om bewustzijn met betrekking tot informatieveiligheid te vergroten.

8.2.3 Disciplinaire maatregelen

Er behoort een formeel disciplinair proces te zijn vastgesteld voor werknemers die inbreuk op de beveiliging hebben gepleegd.

De RvB is uiteindelijk verantwoordelijk voor de disciplinaire maatregel die wordt genomen in het geval van een gebruiker die inbreuk op de beveiliging heeft gepleegd. Echter, het onderzoek wordt niet door uitgevoerd door de RvB, maar door een interne auditor eventueel in combinatie met een overheidsorgaan dan wel een externe auditor. Dit om waar te borgen dat de gebruiker in kwestie niet zonder geldige reden een sanctie krijgt. De RvB zal dan ook altijd pas een besluit nemen op basis van de uitkomsten van het gedane onderzoek.

De RvB houdt rekening met de ernst van de overtreding, of het herhaaldelijk heeft voorgedaan en de redelijkheid en billijkheid op basis de omstandigheden (kon de gebruiker het weten dat dit tot een incident kon leiden en is dit duidelijk genoeg geweest voor de persoon in kwestie)?

Uiteindelijke maatregelen kunnen zijn;

1. Ontnemen van toegangsrechten
2. (Direct) ontbinden van overeenkomst
3. Verwijdering uit systemen en van locatie(s)
4. Boete

8.3 Beëindiging of wijziging van dienstverband

Doelstelling:
Bewerkstelligen dat werknemers, ingehuurd personeel en externe gebruikers ordelijk de organisatie verlaten of hun dienstverband wijzigen.

8.3.1 Beëindiging van verantwoordelijkheden

De verantwoordelijkheden voor beëindiging of wijziging van het dienstverband behoren duidelijk te zijn vastgesteld en toegewezen.

De Leidinggevenden zijn verantwoordelijk voor het up-to-date houden van het registratiesysteem van de betrokken gebruiken en de bijbehorende rechten op een desbetreffende afdeling dan wel in een team. De Eigenaar van het desbetreffende asset is er verantwoordelijk voor, dat de wijzigingen tenminste één maal per week worden doorgevoerd.

8.3.2 Retournering van bedrijfsmiddelen

Alle werknemers, ingehuurd personeel en externe gebruikers behoren alle bedrijfsmiddelen van de organisatie die ze in hun bezit hebben te retourneren bij beëindiging van hun dienstverband, contract of overeenkomst.

Alle gebruikers dienen bedrijfsmiddelen te retourneren indien de overeenkomst wordt gestopt. Deze bedrijfsmiddelen dienen bij de desbetreffende “leidinggevende” te worden teruggebracht, waarbij de leidinggevende dit dient te registreren. Bij eventuele wijzigingen (dus buiten het stopzetten van het contract) dient de leidinggevende dit ook te registreren.

8.3.3 Blokkering van toegangsrechten

De toegangsrechten van alle werknemers, ingehuurd personeel en externe gebruikers tot informatie en IT voorzieningen behoren te worden geblokkeerd bij beëindiging van het dienstverband, het contract of de overeenkomst, of behoort na wijziging te worden aangepast.

Alle wijzingen met betrekking tot de gebruiker dienen per direct te worden geregistreerd door de leidinggevende. Een belangrijk onderdeel hiervan is de “exit procedure” van een gebruiker waarbij de toegang dient te worden voorkomen. Het volgende proces dient in werking te treden bij een “exit procedure”:

1. Leidinggevende registreert de exit van een gebruiker
2. Eigenaar van assets blokkeren of verwijderen de gebruiker van het systeem dat zij beheren
3. Leidinggevende controleert de status van de blokkering / verwijdering

9. Fysieke beveiliging en beveiliging van de omgeving

9.1 Beveiligde ruimten

Doelstelling:
Het voorkomen van onbevoegde fysieke toegang tot, schade aan of verstoring van het terrein en de informatie van de organisatie.

9.1.1 Fysieke beveiliging van de omgeving
Er behoren toegangsbeveiligingen (barrières zoals muren, toegangspoorten met kaartsloten of een bemande receptie) te worden aangebracht om ruimten te beschermen waar zich informatie en IT-voorzieningen bevinden.

Alle eventuele panden kunnen op slot en is beveiligd met een alarminstallatie. Aan een beperkt aantal geregistreerde medewerkers en/of zzp'ers wordt een sleutel gegeven. Deze gebruikers van het pand hebben allemaal een individuele code voor de toegang tot het pand. De sleutels en de codes worden bijgehouden in een register. Zodra iemand de organisatie verlaat of geen directe diensten meer levert dan dient hij of zijn sleutel in te leveren bij zijn of haar leidinggevende en wordt de code verwijderd uit de alarmering.

De server staat in een versterkte ruimte en is ontoegankelijk voor derden.

Sleutels worden bewaard in een sleutelkast, deze wordt zodanig opgeborgen dat daarvoor kennis voor nodig is. Tevens heeft deze sleutelkast een eigenaar, die verantwoordelijk is, dat alleen mensen met de juiste toegangsrechten toegang hebben tot bepaalde sleutels.

BHV-medewerkers hebben in de rol van BHV'er (het recht op) toegang tot alle panden en ruimten van de coöperatie. De hoofd BHV is verantwoordelijk voor het up-to-date houden van de BHV lijst en dat de beveiligingsbewustzijn wordt gewaarborgd binnen de groep BHV'ers.

9.1.2 Fysieke toegangsbeveiliging
Beveiligde zones behoren te worden beschermd door geschikte toegangsbeveiliging, om te bewerkstelligen dat alleen bevoegd personeel wordt toegelaten.

Alle beveiligde "zones" worden afgeschermd met direct toezicht óf door middel van een sleutelbeveiliging.

9.1.3 Beveiliging van kantoren, ruimten en faciliteiten
Er behoort fysieke beveiliging van kantoren, ruimten en faciliteiten te worden ontworpen en toegepast.

Zie paragraaf 9.1.1 en 9.1.2

9.1.4 Bescherming tegen bedreigingen van buitenaf
Er behoort fysieke bescherming tegen schade door brand, overstroming, aardschokken, explosies, oproer en andere vormen van natuurlijke of menselijke calamiteiten te worden ontworpen en toegepast.

De bedrijfsruimten van de coöperatie zijn zover als nodig beveiligd tegen braak, brand en wateroverlast. De braakwerendheid en alarmering is zodanig dat de mogelijkheid van diefstal van bedrijfsmiddelen zeer beperkt is. Afdoende brandmelders en blusmiddelen dienen voorhanden te zijn. Dit is tevens in te zien in het desbetreffende ontruimingsplan van het pand.

9.1.5 Werken in beveiligde ruimten

Er behoren een fysieke bescherming en richtlijnen voor werken in beveiligde ruimten te worden ontworpen en toegepast.

Bevoegde medewerkers mogen zonder toezicht in beveiligde ruimten werken. Onbevoegde medewerkers of derden mogen alleen onder toezicht van een bevoegde medewerker deze ruimtes betreden.

9.1.6 Openbare toegang en gebieden voor laden en lossen

Toegangspunten zoals gebieden voor laden en lossen en andere punten waar onbevoegden het terrein kunnen betreden, behoren te worden beheerst en indien mogelijk worden afgeschermd van IT voorzieningen, om onbevoegde toegang te voorkomen.

Alle leveranciers betreden alleen "publieke ruimten" en/of de front office. Waarbij er te allen tijde iemand bij de front office aanwezig dient te zijn of waarbij de deur moet zijn gesloten op het moment dat iemand niet aanwezig is.

9.2 Beveiliging van apparatuur

Doelstelling:
Het voorkomen van verlies, schade, diefstal of compromittering van bedrijfsmiddelen en onderbreking van de bedrijfsactiviteiten.

9.2.1 Plaatsing en bescherming van apparatuur

Apparatuur behoort zo te worden geplaatst en beschermd dat risico's van schade en storing van buitenaf en de gelegenheid voor onbevoegde toegang wordt verminderd.

Alle apparatuur met daarop informatie worden intern geplaatst in de daarvoor bedoelde ruimtes of in een datacentrum (in geval van de cloud), zodat de risico's van schade en storing van buitenaf en de gelegenheid voor onbevoegde toegang wordt verminderd. Daarnaast worden de deuren gesloten en wordt er gebruik gemaakt van het mechanisme "high trust, high penalty" waarbij eventuele misbruik hard wordt gestraft.

9.2.2 Nutsvoorzieningen

Apparatuur behoort te worden beschermd tegen stroomuitval en andere storingen door onderbreking van nutsvoorzieningen.

Er hoeft geen noodvoorzieningen om de uitval van nutsvoorzieningen op te vangen. Tenzij er sprake is van een centrale server waarbij er een hoog beschikbaarheid noodzakelijk is. Dit mag tevens worden opgevangen door gebruik te maken van een externe cloud waardoor er bij lang uitval thuis kan worden gewerkt. Dit betekent dat de effectieve downtime tot het minimale geminimaliseerd worden.

9.2.3 Beveiliging van kabels

Voedings- en telecommunicatiekabels die voor dataverkeer of ondersteunende informatiediensten worden gebruikt, behoren tegen interceptie of beschadiging te worden beschermd.

De coöperatie maakt gebruik van leveranciers die deze voedings- en telecommunicatiekabels aanleggen. Er worden formele afspraken met de leverancier inzake de invulling van deze beheersmaatregel.

9.2.4 Onderhoud van apparatuur

Apparatuur behoort op correcte wijze te worden onderhouden, om te waarborgen dat deze voortdurend beschikbaar is en in goede staat verkeert.

De Eigenaren van overige hardware dienen ervoor zorg te dragen, dat de hardware beschikbaar is en te allen tijde in bruikbare staat verkeert.

9.2.5 Beveiliging van apparatuur buiten het terrein

Apparatuur buiten de terreinen behoort te worden beveiligd waarbij rekening wordt gehouden met de diverse risico's van werken buiten het terrein van de organisatie

In de gebruikersovereenkomst die iedereen dient te ondertekenen die gebruik gaat maken van de systemen van de coöperatie zijn onder andere de beveiligingsrichtlijnen en gedragsregels opgenomen. Daarnaast wordt er binnen de gebruikers van de informatiesystemen van de coöperatie bewustzijn gecreëerd over de gevaren van verlies en diefstal o.a. door middel van trainingen.

9.2.6 Veilig verwijderen of hergebruiken van apparatuur

Alle apparatuur die opslagmedia bevat, behoort te worden gecontroleerd om te bewerkstelligen dat alle gevoelige gegevens en in licentie gebruikte programmatuur zijn verwijderd of veilig zijn overschreven voordat de apparatuur wordt verwijderd.

De volgende richtlijnen gelden op het gebied van het veilig verwijderen en hergebruiken (verkopen) van apparatuur:

- Harde schijven en overige schijven dienen te worden overschreven (bijvoorbeeld door middel van killdisk).
- Schijven zoals CD's, DVD's, Blue-Rays dienen te worden vernietigd, indien er gegevens van de coöperatie opstaan.
- Smartphones en tablets dienen volledig te zijn geleegd (factory defaults).
- Documenten dienen te worden vernietigd, papier dient te worden vernietigd door middel van een versnipperaar.

9.2.7 Verwijdering van bedrijfseigendommen

Apparatuur, informatie en programmatuur van de organisatie mogen niet zonder toestemming vooraf van de locatie worden meegenomen.

Eigenaar dient op de hoogte te worden gesteld van het meenemen van een apparaat. Daarnaast dient de Eigenaar hier toestemming voor te geven. Het meenemen van papieren documenten is alleen toegestaan als dit noodzakelijk is voor het primaire proces (zorg verlenen).

10 Beheer van Communicatie- en Bedieningsprocessen

10.1 Bedieningsprocedures en verantwoordelijkheden

Doelstelling:
Waarborgen van een correcte en veilige bediening van IT-voorzieningen.

10.1.1 Gedocumenteerde bedieningsprocedures

Bedieningsprocedures behoren te worden gedocumenteerd, te worden bijgehouden en beschikbaar te worden gesteld aan alle gebruikers die deze nodig hebben.

Wet- en regelgeving op het gebied van veiligheid, betrouwbaarheid en integriteit vereisen dat we zorgvuldig omgaan met bedrijfsmiddelen en informatie. Elke gebruiker binnen de coöperatie is verantwoordelijk voor het bewerkstelligen van de veiligheid, betrouwbaarheid en integriteit van de bedrijfsmiddelen en informatie die de gebruiker ontvangt, verwerkt en doorstuurt.

De minimale eisen die wij als coöperatie hanteren zijn:

Alle fysieke en digitale informatie dient te zijn beheerd, op zo'n wijze dat on-geauthentiseerde derden hier niet bij kunnen zonder toestemming, maar die tevens wel beschikbaar zijn voor geauthentiseerde gebruikers. Dit betekent dat op het moment van het verlaten van de werkplek (niet beperkt tot de werkplek op locatie coöperatie), het volgende in acht dient te worden genomen:

- Publieke computers (bijv. bibliotheek, universiteit, computers van klanten en van overige derden die niet gekoppeld zijn aan de desbetreffende gebruiker) mogen geen bedrijfsmiddelen en informatie verwerken.
- Gebruikers mogen alleen met hun eigen gebruikersnaam en wachtwoord inloggen op de systemen van de coöperatie. Deze gebruikersnaam en wachtwoord dienen te allen tijde door maximaal 1 gebruiker te worden gebruikt, waarbij de gebruiker is te herleiden naar de natuurlijke persoon.
- De computer moet zijn geblokkeerd op zo'n wijze dat alleen geauthentiseerde gebruikers kunnen inloggen op de computer.
- De computer dient altijd na gebruik te worden afgemeld.
- Fysieke informatie (zoals brieven, papieren met aantekeningen, etc) mogen niet te zien zijn door niet geauthentiseerde gebruikers, dit betekent dat alle fysieke informatie moeten zijn vernietigd (versnipperen) of moeten zijn opgeborgen op zo'n wijze dat dit alleen toegankelijk is voor mensen die geauthentiseerd zijn om deze informatie in te zien.
- Er dient zorg te worden gedragen dat bij het mondeling communiceren over bedrijfsmiddelen en informatie die gevoelig van aard zijn (patiëntengegevens, financiële analyses, etc) er maatregelen worden genomen (o.a. het sluiten van deuren en ramen) om eventuele beveiligingslekken te voorkomen.
- Het gebruik van externe opslag (bijv. usb-sticks) zijn ten strengste verboden voor het opslaan van informatie, tenzij hier schriftelijke goedkeuring voor is vanuit de leidinggevende.
- Bedrijfsmiddelen en informatie (fysiek of digitaal) die gevoelig van aard zijn mogen niet naar on-geauthentiseerde derden worden gestuurd, tenzij hier schriftelijke goedkeuring voor is vanuit de leidinggevende.
- Incidenten worden direct gemeld bij de Leidinggevende of opdrachtgever (bijv. informatiesysteem) én de functionaris gegevensbescherming. Dit kan ook worden gedaan door te mailen naar meldingen@dichtbij.coop
- Indien een werkplek niet volledig is (bedrijfsmiddelen die niet of niet volledig werken en/of informatie mist, etc), dan dient te worden aangegeven bij de desbetreffende Eigenaar.

- Bij alle informatiesystemen die persoonsgegevens verwerken dient er gebruik te worden gemaakt van logging.

Om te voorkomen dat informatie en bedrijfsmiddelen niet meer beschikbaar zijn of dat er data wordt gelekt zal er minimaal elke dag een back-up worden gemaakt door de coöperatie dan wel de leverancier. Daarnaast is er een procedure om zo snel mogelijk hinder te voorkomen van missende bedrijfsmiddelen en zijn er beheersmaatregelen genomen om veiligheid te garanderen.

De backup en continuniteitsprocedure zijn afhankelijk per (software) onderdeel binnen de coöperatie. Waarbij de backup (1). de continuïteit (2) en de veiligheid (3) zijn gewaarborgd door de volgende beheersmaatregelen. Er is een *verwerkingsovereenkomst* gesloten met alle partijen waar de Coöperatie een cloud oplossing van afneemt. In deze overeenkomst staat in ieder geval dat de verwerker zijn of haar verantwoordelijkheid draagt voor de *continuïteit*, waaronder de back-up, de *veiligheid* (tegen lekken) en de *integriteit* van de software.

Daarnaast kan er in bepaalde gevallen nog zijn besloten zijn om een *extra back-up* te creëren naast de backup van de desbetreffende cloud provider. De extra backup wordt als asset gezien.

10.1.2 Wijzigingsbeheer

Wijzigingen in IT-voorzieningen en informatiesystemen behoren te worden beheerst.

In de procedures voor wijzigingsbeheer is minimaal aandacht besteed aan:

1. Een impactanalyse van mogelijke gevolgen van de wijzigingen;
2. Voor de installatie van nieuwe ICT-voorzieningen of wijziging van bestaande voorzieningen wordt door de projecteigenaar een goedkeuringsprocedure vastgesteld;
3. In de procedures voor goedkeuringsprocedure is vastgelegd dat ongeautoriseerde ICT voorzieningen niet mogen worden geïnstalleerd of gebruikt en dat elke installatie en bijbehorend doel en gebruik formeel moeten worden goedgekeurd de desbetreffende verantwoordelijke;
4. Zakelijke goedkeuring wordt verleend door de RvB, technische goedkeuring door de desbetreffende Eigenaar die verantwoordelijk zijn voor onderhoud en beheer van de voorziening.

Voor een dienst die wordt verleend door een derde partij, is het beheer van wijzigingen de verantwoordelijkheid van de Eigenaar onder wiens verantwoordelijkheid de overeenkomst met de derde partij is aangegaan. Steeds geldt dat tijdens en na een wijziging een situatie moet bestaan welke voldoet aan de gestelde (beveiligings-)eisen.

10.1.3 Functiescheiding

Taken en verantwoordelijkheidsgebieden behoren te worden gescheiden om gelegenheid voor onbevoegde of onbedoelde wijziging of misbruik van de bedrijfsmiddelen van de organisatie te verminderen.

De coöperatie past functiescheiding toe voor zover de verantwoordelijken van bedrijfsmiddelen de risico's die gemoeid zijn met het ontbreken van functiescheiding niet acceptabel vindt en functiescheiding praktisch uitvoerbaar en realiseerbaar is.

Waar functiescheiding lastig kan worden gerealiseerd of in verhouding te hoge kosten met zich meebrengt, worden door de coöperatie andere (beheers)maatregelen overwogen, zoals het (steekproefsgewijs) controleren van activiteiten, het voorzien in audit trails (logging) en supervisie.

10.1.4 Scheiding van faciliteiten voor ontwikkeling, testen en productie

Faciliteiten voor ontwikkeling, testen en productie behoren te zijn gescheiden om het risico van onbevoegde toegang tot of wijzigingen in het productiesysteem te verminderen.

Naast de productieomgeving kan het voorkomen dat er nieuwe diensten en instellingen worden ontwikkeld en getest. Om ervoor zorgen dat de integriteit en de continuïteit van de bestaande infrastructuur en software niet in geding komt mag er niet ontwikkeld en getest worden op productie omgevingen. Binnen de Coöperatie wordt er geen software ontwikkeld, daarnaast mogen er geen veranderingen worden ingevoerd in de software van derden zonder dat dit daadwerkelijk uitgebreid en bewezen getest is.

10.2 Beheer van de dienstverlening door een derde partij

Doelstelling:
Geschikt niveau van informatiebeveiliging en dienstverlening implementeren en bijhouden in overeenstemming met de overeenkomsten voor dienstverlening door een derde partij

10.2.1 Dienstverlening

Er behoort te worden bewerkstelligd dat de beveiligingsmaatregelen, definities van dienstverlening en niveaus van dienstverlening zoals vastgelegd in de overeenkomst voor dienstverlening door een derde partij worden geïmplementeerd en uitgevoerd en worden bijgehouden door die derde partij.

Alle dienstverlening door derden dient contractueel te worden afgedekt, inclusief de invulling van alle relevante beveiligingsaspecten. De namens de coöperatie in de overeenkomst genoemde gemandateerde functionaris is als Eigenaar verantwoordelijk voor het (doen) opnemen van noodzakelijke informatiebeveiligingseisen en – voorwaarden. Hij ziet er op toe dat tenminste opgenomen wordt:

1. De redenen, eisen en voordelen die de toegang door derden noodzakelijk maken;
2. Beschrijving van de dienst(en) die de instelling afneemt van de derde partij;
3. Respectievelijke aansprakelijkheden van de partijen in de overeenkomst;
4. Toegestane toegangsmethoden en beheer, en het gebruik van toegangscodes en wachtwoorden;
5. Autorisatieproces voor gebruikerstoegang en privileges van gebruikers;
6. Als de gebruikersadministratie niet door de instelling plaatsvindt: de verplichting tot het bijhouden van een overzicht van personen die bevoegd zijn de ter beschikking gestelde dienst te gebruiken, en wat hun rechten en privileges zijn;
7. Het beginsel dat alle toegang die niet expliciet is toegestaan, verboden is;
8. Een procedure om toegangsrechten te herroepen of de verbinding tussen systemen af te breken;
9. Beveiligingseisen voor de uitwisseling van informatie.

Van medewerkers van gecontracteerde derden en overige externen dienen kunnen extra eisen worden gesteld; zoals het ondertekenen van de gebruikersovereenkomst.

10.2.2 Controle en beoordeling van dienstverlening door een derde partij

De diensten, rapporten en registraties die door de derde partij worden geleverd, behoren regelmatig te worden gecontroleerd en beoordeeld en er behoren regelmatig audits te worden uitgevoerd.

De coöperatie bewerkstelligd dat de beveiligingsmaatregelen, zoals beschreven in dit document worden nageleefd door de IT leveranciers. Aangezien alle afspraken zijn vastgelegd in de contracten wordt er periodiek (per 12 maanden of korter indien spoed) gekeken in hoeverre de IT leverancier voldoet aan de gestelde afspraken. Daarnaast zal er dan worden geëvalueerd of er nog onderdelen onvolledig dan wel niet kloppen in de huidige overeenkomst(en). Dit zal vervolgens worden

samengevat per leverancier en indien nodig zal dit worden gecommuniceerd of indien nodig worden veranderd in het contract in samenspraak met de leveranciers.

10.2.2 Beheer van wijzigingen in dienstverlening door een derde partij

De diensten, rapporten en registraties die door de derde partij worden geleverd, behoren regelmatig te worden gecontroleerd en beoordeeld en er behoren regelmatig audits te worden uitgevoerd.

Toekomstige wijzigingen en wijzigingen in de dienstverlening door derden worden geregistreerd. Er worden alleen overeenkomsten gesloten met IT leveranciers die toekomstige wijzigingen (roadmap) aan geven of waarbij de IT leverancier wijzigingen die eventueel de werking van de continuïteit, veiligheid of integriteit van de software aan kunnen aanpassen per e-mail doorgeven. Deze voorwaarde wordt contractueel vastgelegd. Daarnaast wordt periodiek (per 12 maanden of korter indien spoed) gekeken in hoeverre een potentiele wijziging invloed heeft op de werking van de bestaande systemen op het gebied van continuïteit, veiligheid en integriteit. Daarnaast dient de derde partij bewijs te overhandigen waarin blijkt dat ze voldoen aan de gestelde wet- en regelgeving en de eisen zoals gesteld in dit document.

10.2.3 Systeemplanning en –acceptatie (Vervolg op 10.2.2)

Wijzigingen in de dienstverlening door derden, waaronder het bijhouden en verbeteren van bestaande beleidslijnen, procedures en maatregelen voor informatiebeveiliging, behoren te worden beheerd, waarbij rekening wordt gehouden met de onmisbaarheid van de betrokken bedrijfssystemen en -processen en met heroverweging van risico's.

Als blijkt dat de huidige systemen niet voldoen aan de gewenste werking, continuïteit, veiligheid en integriteit dan wordt er een vastgesteld inkooptraject gestart, waarbij de eisen met betrekking tot een IT leverancier en de desbetreffende zijn opgenomen.

10.3 Systeemplanning en –acceptatie

Doelstelling:
Het risico van systeemstoringen tot een minimum beperken.

10.3.1 Capaciteitsbeheer

Het gebruik van middelen behoort te worden gecontroleerd en afgestemd en er behoren verwachtingen te worden opgesteld voor toekomstige capaciteitseisen, om de vereiste systeemprestaties te bewerkstelligen.

Het gebruik van middelen behoort te worden gecontroleerd en afgestemd en er behoren verwachtingen te worden opgesteld voor toekomstige capaciteitseisen om de vereiste systeemprestaties te bewerkstelligen. Bij de coöperatie maakt capaciteitesbeheer integraal onderdeel uit van “Controle en beoordeling van dienstverlening door een derde partij (10.2.2)” en wordt er op het moment van controle gekeken in hoeverre de capaciteiten van de huidige systemen voldoen om vereiste systeemprestaties te leveren in ieder geval de komende twee (2) jaar op het gebied van werking, continuïteit, veiligheid en integriteit.

10.3.2 Systeemacceptatie

Er behoren aanvaardingscriteria te worden vastgesteld voor nieuwe informatiesystemen, upgrades en nieuwe versies en er behoort een geschikte test van het systeem of de systemen te worden uitgevoerd tijdens ontwikkeling en voorafgaand aan de acceptatie.

Systeemacceptatie maakt onderdeel uit van de procedures voor wijzigingsbeheer.

De implementatie van nieuwe informatiesystemen en grotere wijzigingen worden getoetst aan alle vooraf vastgelegde acceptatiecriteria. Toetsing dient tijdig plaats te vinden. Een impactanalyse moet

hebben aangetoond dat het nieuwe informatiesysteem geen nadelige invloed heeft op bestaande systemen. Pas na formele acceptatie door de RvB van nieuwe toepassingen over naar de productieomgeving. Acceptatiecriteria dienen binnen het ingerichte project in een vroeg stadium te worden vastgesteld en gedocumenteerd om gedurende de looptijd van het project de te controleren en gecontroleerde beveiligingsaspecten vast te leggen. Het is aan de (toekomstige) Eigenaren om de specifieke set van te toetsen acceptatiecriteria goed te keuren. Cloud applicaties zijn aan systeemacceptatie onderhevig. De Verantwoordelijke ziet hier op toe, tevens worden de keuzes gerapporteerd.

10.4 Bescherming tegen virussen en 'mobile code'

Doelstelling:
Beschermen van de integriteit van programmatuur en informatie

10.4.1 Maatregelen tegen virussen en 'malicious code'

Er behoren maatregelen te worden getroffen voor detectie, preventie en herstellen om te beschermen tegen virussen en er behoren geschikte procedures te worden ingevoerd om het bewustzijn van de gebruikers te vergroten.

Er dient gebruik te worden gemaakt van een (automatisch) geüpdatete virus- en adware scanner. Daarnaast moeten de computers van de gebruikers altijd up-to-date zijn. Gebruikers mogen tevens geen gevoelige websites bekijken, die kwaadaardige programmatuur kunnen bevatten. Indien een gebruiker gebruik maakt van de systemen van de coöperatie, dan mogen ze niet op websites kijken met illegale of erotische content, omdat deze websites vaak onveilig zijn. Indien een computer geïnfecteerd is of niet meer hetzelfde functioneert, dan dient dit te worden aangegeven bij de desbetreffende leidinggevende van de gebruiker.

Het is tevens niet toegestaan om een publieke computer te gebruiken indien er met informatie(systemen) van de coöperatie wordt gewerkt. Daarnaast dient er gebruik gemaakt van een 2-steps authenticatie proces bij privacygevoelige informatie (waaronder zorgdossiers), zodat zelfs wanneer er een keylogger op een computer staat, er extern geen toegang kan worden verschaft aangezien de 2-steps authenticatie een vereiste is.

10.4.2 Maatregelen tegen 'mobile code'

Als gebruik van 'mobile code' is toegelaten, behoort de configuratie te bewerkstelligen dat de geautoriseerde 'mobile code' functioneert volgens een duidelijk vastgesteld beveiligingsbeleid, en behoort te worden voorkomen dat onbevoegde 'mobile code' wordt uitgevoerd.

Mobiele code is software die van elders is verkregen en lokaal op de eigen apparatuur wordt uitgevoerd. Websites passen mobile code (zoals Java, JavaScript, ActiveX en XML (AJAX)) veelal toe om dynamische pagina's te genereren. Documenten (zoals van MS Office, Adobe PDF en grafische afbeeldingen) kunnen ook mobile code bevatten.

Relevante applicaties (browser software, MS Office, Outlook) op desktops/laptops dienen te zijn geconfigureerd dat:
1. Overbodige mobile code functionaliteit is uitgezet;
2. Mobile code niet automatisch wordt uitgevoerd tenzij de gebruiker goedkeuring verleent of vastgesteld is dat de mobile code afkomstig is van een betrouwbare bron. Bij voorkeur worden extra voorzieningen (extensions/plugins) geactiveerd om dit te realiseren;
3. Beschikbare browser functionaliteit om malafide websites te blokkeren wordt benut;
4. Grafische afbeeldingen, documenten niet automatisch worden gedownload tenzij de gebruiker goedkeuring verleent of als sprake is van een betrouwbare bron (bijvoorbeeld van de coöperatie zelf); 5. De securityinstellingen van applicaties van de coöperatie beheerde desktops en laptops

moeten zoveel mogelijk worden benut. Benodigde instellingen worden bepaald aan de hand van betrouwbare security guides, benchmarks en best practices. De gebruiker kan de instellingen niet wijzigen.

10.5 Back-up en herstel

Doelstelling:
Handhaven van de integriteit en beschikbaarheid van informatie en IT-voorzieningen.

10.5.1 Reservekopieën maken (back-ups)

Er behoren back-up kopieën van informatie en programmatuur te worden gemaakt en regelmatig te worden getest overeenkomstig het vastgestelde back-upbeleid.

Aangezien de coöperatie werkt met cloud oplossingen, worden de back-ups geregeld door deze cloud aanbieders. De afspraken met betrekking tot de beschikbaarheid, integriteit en vertrouwelijkheid zijn vastgelegd in de overeenkomsten gesloten met deze partijen. Er kan door de coöperatie gevraagd worden om te bewijzen, dat er daadwerkelijk correcte back-ups worden gemaakt en met de juiste procedure worden hersteld indien nodig.

10.6 Beheer van netwerkbeveiliging

Doelstelling:
Bewerkstelligen van de bescherming van informatie in netwerken en bescherming van de ondersteunende infrastructuur.

10.6.1 Maatregelen voor netwerken

Netwerken behoren adequaat te worden beheerd en beheerst om ze te beschermen tegen bedreigingen en om beveiliging te handhaven voor de systemen en toepassingen die gebruikmaken van het netwerk, waaronder informatie die wordt getransporteerd.

En

Beveiligingskenmerken, niveaus van dienstverlening en beheerseisen voor alle netwerkdiensten behoren te worden geïdentificeerd en opgenomen in elke overeenkomst voor netwerkdiensten, zowel voor diensten die intern worden geleverd als voor uitbestede diensten.

Het netwerk wordt beheerd door een leverancier. Het netwerk bestaat uit verschillende lagen, gedefinieerd als de zogenoemde OSI lagen, zie de afbeelding hieronder.

Afbeelding 2 - Het OSI model

Fysieke laag
Het is niet toegestaan om het **fysieke** netwerk te veranderen door een gebruiker. Dit is alleen toegestaan door Beheerder of met toestemming van de Eigenaar. Dit betekent, dat gebruikers zonder toestemming van leidinggevende geen (netwerk)kabels mogen wijzigen dan wel aansluiten op netwerkpunten. De cruciale fysieke netwerkpunten dienen alleen te bereiken zijn via beveiligde toegang (bijvoorbeeld sleutel). Deze ruimte is alleen te betreden indien je hiervoor geauthentiseerd bent. Beheerder is tevens verantwoordelijk voor de continuïteit van het netwerk.

Datalinklaag
Dit zijn de signalen die onder andere door de switches worden gestuurd, de acties bevinden zich op MAC adres niveau. De MAC adressen worden gelogd in de access-points op het moment dat iemand zich op het draadloos netwerk bevindt. Naast de bovenstaande actie en de acties voor laag 1 – zijn hier geen verdere acties voor ondernomen.

Netwerklaag
Er kan steekproefsgewijs gebruik worden gemaakt van een *sniffing logging tool*. Dit betekent, dat op het moment iemand op het netwerk van de coöperatie dichtbij sniffert de activiteiten kunnen worden getraceerd. Dit zal voornamelijk van toepassing zijn als er een vermoeden is dat het netwerk is gecomprimeerd.

Transportlaag
Indien mogelijk wordt er gebruik gemaakt van het TCP protocol waarbij UDP wordt vermijden. TCP is een connectie-georiënteerd, waarbij de connectie dient te worden gesloten na een bepaalde tijd (hand-shake-model), het systeem herkent de zender en ontvanger. Waarbij UDP (tegenhanger van TCP) heeft geen autorisatie nodig (geen hand-shake-model).

Sessielaag
Alle informatie dat gevoelige informatie kan bevatten wordt over een lijn gestuurd dat geencrypt is. Met uitzondering van de netwerkmappen, de netwerkmappen versturen de data niet geencrypt indien er op het interne netwerk wordt gewerkt. Echter zal door de beheersmaatregel beschreven in "netwerklaag" en de algemene beheersmaatregelen, zoals overeenkomsten en preventiemaatregelen de eventuele schade minimaal zijn.

De prestatielaag (6) en applicatielaag (7) worden beheerd door IT leveranciers, waarbij overeenkomsten met daarin de verantwoordelijkheden zijn beschreven.

10.7 Verwijderbare media

Doelstelling:
Voorkomen van onbevoegde openbaarmaking, modificatie, verwijdering of vernietiging van bedrijfsmiddelen en onderbreking van bedrijfsactiviteiten.

10.7.1 Beheer van verwijderbare media
Er behoren procedures te zijn vastgesteld voor het beheer van verwijderbare media.

Verwijderbare media zoals USB-sticks en externe harde schijven zijn niet toegestaan, tenzij hier expliciet toestemming voor is gegevens door de Leidinggevende. Deze goedkeuring dient te worden geregistreerd. Dit wordt tevens vermeld in de gebruikersovereenkomst.

Indien er een computer en/of server en/of overige hardware waar data op kan staan wordt verwijderd dat onder beheer valt van de coöperatie dan dient de hardware worden leeggemaakt door middel van een “kill-disc” procedure, waarbij data niet meer terug te halen is.

10.7.2 Verwijdering van media
Media behoren op een veilige en beveiligde manier te worden verwijderd als ze niet langer nodig zijn, overeenkomstig formele procedures.

Zie paragraaf 9.2.6

10.7.3 Procedures voor de behandeling van informatie
Er behoren procedures te worden vastgesteld voor de behandeling en opslag van informatie om deze te beschermen tegen onbevoegde openbaarmaking of misbruik.

De algemene richtlijnen gelden van dit document. Waarbij gebruikers bewust worden gemaakt van de verantwoordelijkheid die zij dragen, dit door middel van training en opleiding.

10.7.4 Beveiliging van systeemdocumentatie
Systeemdocumentatie behoort te worden beschermd tegen onbevoegde toegang.

De algemene richtlijnen gelden van dit document.

10.8 Uitwisseling van data

Doelstelling:
Handhaven van beveiliging van informatie en programmatuur die wordt uitgewisseld binnen een organisatie en met enige externe entiteit.

10.8.1 Beleid en procedures voor informatie-uitwisseling
Er behoren formeel beleid, formele procedures en formele beheersmaatregelen te zijn vastgesteld om de uitwisseling van informatie via het gebruik van alle typen communicatiefaciliteiten te beschermen.

Er mag alleen privacygevoelige informatie worden uitgewisseld met partijen die de *gebruikersovereenkomst* hebben getekend dan wel van rechtswege de veiligheid van deze informatie waarborgen (bijv. (semi)overheidsinstanties). Privacygevoelige informatie mag alleen worden

verzonden over beveiligde lijn (SSL). Niet geencrypte communicatiemiddelen mogen niet gebruikt worden om privacygevoelige informatie te versturen.

De leidinggevenden dienen medewerkers erop te wijzen dat zij passende voorzorgen behoren te nemen, bijvoorbeeld om geen vertrouwelijke of geheime informatie te onthullen via het opvangen of afluisteren van telefoongesprekken, vooral bij gebruik van mobiele telefoons;

Voor het uitwisselen van informatie geldt verder het volgende:

1. Openbare informatie kan zonder beperkingen worden uitgewisseld;
2. Interne informatie kan tussen medewerkers onderling zonder beperkingen worden uitgewisseld. Uitwisseling met derden is mogelijk als daar noodzaak toe bestaat en het de belangen van de coöperatie, gebruikers en andere stakeholders niet schaadt. Zulks ter beoordeling van de medewerker die het initiatief tot uitwisseling neemt;
3. Vertrouwelijke informatie mag alleen worden uitgewisseld met partijen die een "need to know" hebben, als dat noodzakelijk is voor de werkzaamheden. Zulks ter beoordeling aan de Verantwoordelijke van de informatie. Vertrouwelijke informatie wordt alleen uitgewisseld op basis van beveiligde protocollen. Voor zover het medewerkers van de coöperatie betreft gelden geen verdere beperkingen. Voor derde partijen geldt dat voorafgaand aan uitwisseling een geheimhoudingsovereenkomst moet zijn overeengekomen;
4. Voor informatie die als 'geheim' geclassificeerd is, geldt bovendien:
    a. Bij digitaal uitgegeven informatie wordt van de ontvangende partij expliciet geëist dat de informatie na gebruik wordt vernietigd en dat de vernietiging wordt gerapporteerd aan de Verantwoordelijke(n);
    b. De Eigenaar van de informatie houdt een administratie bij waarin is opgenomen:
        i. Welk afschrift aan wie ter beschikking wordt gesteld;
        ii. Aan wie een digitale kopie ter beschikking is gesteld;
        iii. Of het afschrift reeds is terug ontvangen dan wel de kopie reeds is vernietigd.

10.8.2 Uitwisselingsovereenkomsten

Er behoren overeenkomsten te worden vastgesteld voor de uitwisseling van informatie en programmatuur tussen de organisatie en externe partijen.

Onderwerpen die aandacht moeten krijgen zijn onder meer:

1. Het eigenaarschap van informatie en/of software en de verantwoordelijkheid voor de gegevensbescherming, auteursrechten, licenties van software;
2. Maatregelen om betrouwbaarheid - waaronder traceerbaarheid en onweerlegbaarheid - van gegevens te waarborgen;
3. Verantwoordelijkheid en aansprakelijkheid in het geval van informatiebeveiligingsincidenten alsmede procedures over melding van incidenten. Indien mogelijk wordt binnenkomende software (zowel op fysieke media als gedownload) gecontroleerd op ongeautoriseerde wijzigingen aan de hand van een door de leverancier via een gescheiden kanaal geleverde checksum of certificaat.

De beveiligingsinhoud van elke uitwisselingsovereenkomst behoort in overeenstemming te zijn met de classificatie van de betreffende informatie.

10.8.3 Fysieke media die worden getransporteerd

Media die informatie bevatten behoren te worden beschermd tegen onbevoegde toegang, misbruik of corrumperen tijdens transport buiten de fysieke begrenzing van de organisatie.

Er wordt alleen gebruik gemaakt van medewerkers en/of organisaties die de gebruikersovereenkomst hebben getekend dan wel rechtswege de veiligheid van deze informatie waarborgen.

Transport van fysieke media (gegevensdragers) met als vertrouwelijk of hoger geclassificeerde informatie dient tot een absoluut minimum te worden beperkt en dient te geschieden met goedgekeurde middelen, waardoor de inhoud niet zichtbaar, niet kenbaar en inbreuk detecteerbaar is.

Mogelijke beveiligingsmaatregelen zijn:
1. Bescherming door fysieke maatregelen, zoals afgesloten containers;
2. Gebruik van verpakkingsmateriaal waaraan te zien is of getracht is het te openen;
3. Persoonlijke aflevering;
4. Opsplitsing van zendingen in meerdere delen en eventueel verzending via verschillende routes;
5. Gebruik maken van betrouwbare transport- en koeriersdiensten in combinatie met identiteitscontroles van koeriers.

10.8.4 Elektronische berichtenuitwisseling

Informatie die een rol speelt bij elektronische berichtuitwisseling behoort op geschikte wijze te worden beschermd.

Gebruikers dienen op verantwoordelijke wijze van elektronische berichtenuitwisseling gebruik te maken. Voorwaarden voor het gebruik van elektronische berichtenverkeer zijn:
1. Beschermen van berichten tegen toegang door onbevoegden, wijziging of weigeren van dienst;
2. Correcte adressering is gewaarborgd door gebruikers te informeren over de gevaren, daarnaast
3. Apparatuur en berichtensystemen dienen zijn beschermd tegen spam en malware.
4. Al het berichtenverkeer via een verbinding te laten verlopen dat geencrypt is.

10.8.5 Systemen voor bedrijfsinformatie

Beleid en procedures behoren te worden ontwikkeld en geïmplementeerd om informatie te beschermen die een rol speelt bij de onderlinge koppeling van systemen voor bedrijfsinformatie.

Wanneer er bij nieuwbouw of wijzigingen sprake is van onderlinge koppeling van eigen informatiesystemen of koppeling van eigen informatiesystemen met systemen van derden, moet per geval de beveiligingsproblematiek aan de hand van een risicoanalyse worden geïnventariseerd en dienen passende beveiligingsmaatregelen te worden vastgesteld. Er dient tenminste aandacht te zijn voor:

1. Classificatie van de via de koppeling uit te wisselen informatie;
2. Identificatie en authenticatie;
3. Waarborging vertrouwelijkheid en integriteit door passende bescherming van de gegevensoverdracht;
4. Bescherming van toegang tot de uitgewisselde informatie;
5. Bescherming van toegang tot koppelingsfunctionaliteit;
6. Eventuele beïnvloeding van beschikbaarheid (kan het uitwisselen de beschikbaarheid van de gekoppelde systemen beïnvloeden?).

10.9 Diensten voor e-commerce

Doelstelling:
Bewerkstelligen van de beveiliging van diensten voor e-commerce, en veilig gebruik ervan.

De Coöperatie verricht (nog) geen e-commerce diensten.

10.10 Controle

Doelstelling:
Ontdekken van onbevoegde informatieverwerkingsactiviteiten.

10.10.1 Aanmaken audit-logbestanden

Activiteiten van gebruikers, uitzonderingen en informatiebeveiligingsgebeurtenissen behoren te worden vastgelegd in audit-logbestanden. Deze logbestanden behoren gedurende een overeengekomen periode te worden bewaard, ten behoeve van toekomstig onderzoek en toegangscontrole.

Auditlogbestanden worden ten behoeve van toekomstig onderzoek, audits en toegangscontrole tenminste drie maanden bewaard, echter niet langer dan noodzakelijk en door wet- en regelgeving toegestaan. De Eigenaar kan verzoeken aan de functionaris gegevensbescherming om logbestanden voor een bepaald informatiesysteem langer te bewaren.

Aangezien alle privacygevoelige informatie op de cloud wordt opgeslagen, worden de *activiteiten van gebruikers, uitzonderingen en informatiebeveiligingsgebeurtenissen* vastgelegd door de desbetreffende cloud leverancier. Tevens worden dit ook wel de logbestanden genoemd, deze logbestanden staan geregistreerd, de registratie van deze logbestanden worden gedaan door de Eigenaren. In *de audits wordt er steek-proefs-gewijs* ook gekeken in hoeverre iemand gegevens benaderd, waarvoor hij of zij niet geautoriseerd is.

Voor alle systemen moeten tenminste de navolgende gebeurtenissen worden geregistreerd:
1. Inlogpogingen zowel op systeemniveau als op toepassingsniveau (als de toepassing inloggen vereist);
2. Alle vormen van toegang op systeem,- en toepassingsniveau;
3. Het gebruik van de systemen (welke gebruiker heeft welke informatie benaderd?).

In de auditlogbestanden behoren de volgende gegevens te worden vastgelegd:
1. Gebruikers-ID's;
2. Data, tijdstippen en details van de geregistreerde gebeurtenissen;
3. Waar mogelijk de identiteit van de computer of de locatie.

Tijdstippen in logbestanden worden vastgelegd in UTC (Zie paragraaf 10.10.6 Synchronisatie van systeemklokken).

Wachtwoorden worden **nooit** vastgelegd in de auditlogbestanden.

De auditlogbestanden kunnen vertrouwelijke persoonlijke informatie bevatten. De bestanden dienen voldoende beveiligd te zijn en alleen op een “need to know” basis toegankelijk te zijn. De logs van de systemen zijn alleen benaderbaar via het account van de Applicatiebeheerder. Waartoe alleen Applicatiebeheer of derden met toestemming van functionaris gegevensbescherming toegang hebben.

10.10.2 Controle van systeemgebruik

Er behoren procedures te worden vastgesteld om het gebruik van IT-voorzieningen te controleren. Het resultaat van de controleactiviteiten behoort regelmatig te worden beoordeeld.

Wekelijks wordt door de Eigenaren alle geregistreerde gebeurtenissen omtrent het functioneren van de (informatie)systemen bekeken en beoordeeld. Er is tenminste voldoende aandacht voor:

1. Toegang tot (delen) van systemen waar gebruikers niet bevoegd voor zijn;
2. afwijkingen van het normale patroon van het aantal mislukte inlogpogingen;
3. de tijdstippen waarop toegang tot de applicatie is gezocht;
4. de locatie waarvandaan toegang tot de applicatie is gezocht.

10.10.3 Bescherming van informatie in logbestanden

Logfaciliteiten en informatie in logbestanden behoren te worden beschermd tegen inbreuk en onbevoegde toegang.

De logbestanden van de applicaties worden verzorgd door de cloud providers. Als beheersmaatregel zijn ze hier tevens ook verantwoordelijk voor (contractueel vastgelegd). Waarbij alleen daartoe geautoriseerde beheerders hebben leestoegang tot logbestanden.

10.10.4 Logbestanden van administrators en operators

Activiteiten van systeemadministrators en systeemoperators behoren in logbestanden te worden vastgelegd.

Indien informatiesystemen in de beveilingsniveau categorie H zitten dan wordt er in overeenstemming met de Eigenaar bepaald in hoeverre extra maatregelen noodzakelijk zijn om de logging van beheerders te waarborgen.

10.10.5 Registratie van storingen

Storingen behoren in logbestanden te worden vastgelegd en te worden geanalyseerd en er behoren geschikte maatregelen te worden genomen.

Alle storingen worden geregistreerd in een verzamelbestand.

10.10.6 Synchronisatie van systeemklokken

De klokken van alle relevante informatiesystemen binnen een organisatie of beveiligingsdomein behoren te worden gesynchroniseerd met een overeengekomen nauwkeurige tijdsbron.

Voor een betrouwbare analyse van logbestanden zijn alle systeemklokken gebaseerd op UTC (Universal Coordinated Time). De cloud providers zorgen ervoor dat de systeemklokken gesynchroniseerd zijn en dat de tijden kloppen (minder dan 1 minuut verschil).

11 Toegangsbeveiliging

11.1 Bedrijfseisen ten aanzien van toegangsbeheersing

Doelstelling:
Beheersen van de toegang tot informatie.

11.1.1 Toegangsbeleid

Er behoort toegangsbeleid te worden vastgesteld, gedocumenteerd en beoordeeld op basis van bedrijfseisen en beveiligingseisen voor toegang.

De toegang tot informatie en informatiesystemen dient voldoende te worden beheerst, zowel fysiek als logisch. De instelling classificeert haar informatie en informatiesystemen. Naarmate de classificatie hoger is, is een betere toegangsbeveiliging nodig. De coöperatie streeft via het hanteren van principes en procedures doorlopend naar het zo beperkt mogelijk houden van toegangsrechten en –mogelijkheden (“least privilege”). Voor het verlenen van toegang geldt daarnaast het principe 'standaard niet, tenzij het expliciet is toegestaan' (“deny-by-default”). Voor toegang tot informatiesystemen en ruimten waarin zich informatie(middelen) bevinden heeft de gebruiker toegangsrechten nodig. Deze dienen door zijn leidinggevende te worden toegekend op basis van het 'need-to' principe. Dit betekent dat de leidinggevende niet meer rechten aan de gebruiker toekent dan nodig is voor de uitoefening van zijn functie. Ten aanzien van de toegang tot informatiesystemen geldt het volgende:

1. Toegang dient pas te worden verleend na authenticatie;
2. Toegang wordt verleend op basis van het persoonsgebonden instellingsaccount;
3. Classificatie van het informatiesysteem en of het informatiesysteem via internet te gebruiken is, bepaalt het vereiste minimale beveiligingsniveau voor identificatie en authenticatie (document: categorieën) en daarmee op welke wijze de instelling bij registratie de identiteit van de gebruiker moet vaststellen en de wijze van authenticatie (al dan niet multifactor);
4. Tenminste LoA2 (2-factor authenticatie) is vereist voor informatiesystemen die via internet te gebruiken zijn en vertrouwelijke of hoger geclassificeerde informatie verwerken.
5. De coöperatie werkt zoveel mogelijk met standaard gebruikersprofielen voor veel voorkomende rollen, met beperkte toegangsrechten.
6. Bijzondere rechten moeten afdoende zakelijk gemotiveerd en terughoudend toegekend worden. De Toegekende bijzondere rechten worden geadministreerd, onder verantwoordelijkheid van de Eigenaar.
7. Alle gevoelige mutaties in informatiesystemen zijn, voor zover technisch mogelijk, herleidbaar naar een persoonsgebonden instellingsaccount;
8. Raadpleging van geheime informatie dient herleidbaar te zijn naar een persoonsgebonden instellingsaccount;
9. Toegang via niet-persoonsgebonden accounts, zoals groepsaccounts, is - behoudens incidentele geautoriseerde uitzonderingen - niet toegestaan.
10. De coöperatie streeft naar een centraal 2-factor authenticatiesysteem voor al haar informatiesystemen. Toegangsrechten dienen zo snel mogelijk na vertrek van medewerkers of wisseling van functie te worden ingetrokken. De RvB beoordeelt periodiek het toegangsbeleid en de toegangsbeveiliging. Leidinggevenden beoordelen periodiek de toegangsrechten van hun medewerkers.

11.2 Beheer van toegangsrechten van gebruikers

Doelstelling:
Toegang voor bevoegde gebruikers bewerkstelligen en onbevoegde toegang tot informatiesystemen voorkomen.

11.2.1 Registratie van gebruikers

Er behoren formele procedures voor het registreren en afmelden van gebruikers te zijn vastgesteld, voor het verlenen en intrekken van toegangsrechten tot alle informatiesystemen en -diensten.

De coöperatie kent beheerprocedures voor 1) het aanmelden, registreren en afmelden van gebruikers en 2) het toekennen en intrekken van toegangsrechten, voor diverse bedrijfstoepassingen. Dit soort procedures behandelen onder meer:

1. Wijze van registratie, met name vaststelling en verificatie van de identiteit van de gebruiker
2. Autorisatie (ligt bij de Eigenaar en/of de leidinggevende) en controle hierop (verificatie);
3. Het gebruik van een persoonsgebonden instellingsaccount, zodat handelingen kunnen worden herleid tot individuele gebruikers en gebruikers verantwoordelijk kunnen worden gesteld voor gepleegde handelingen;
4. Controle op toepasselijkheid van toegangsrechten (niet te hoog in verhouding tot de functie en toepassing);
5. Controle op conflicten door toekenning van toegangsrechten (zoals het in gevaar brengen van functiescheiding); Schoning inclusief periodieke controle op en verwijderen of blokkeren van overtollige gebruikers;
6. Aansluiting op procedures zoals 'uit dienst' en ‘wijziging van functie’ (voor het zo snel mogelijk intrekken of blokkeren van toegangsrechten van gebruikers die van functie of rol zijn veranderd of de coöperatie hebben verlaten);
7. Het aanreiken van de overeenkomsten, waaronder de gebruikersovereenkomst.

Slechts na identificatie aan de hand van een geldig identiteitsbewijs, in persoon (face-to-face) en al dan niet direct of indirect via een gezaghebbende bron, wordt het persoonsgebonden instellingsaccount aangemaakt en de gebruiker met bijbehorende authenticatiemiddelen aangereikt;

Ook accounts voor externe gebruikers mogen slechts worden aangemaakt en toegangsrechten mogen slechts worden ingesteld, nadat de beheerprocedures geheel zijn doorlopen.

11.2.2 Beheer van speciale bevoegdheden

De toewijzing en het gebruik van speciale bevoegdheden behoren te worden beperkt en beheerst.

Er dient schriftelijk te worden omschreven, wie speciale bevoegdheden toegewezen heeft gekregen en de motivatie met hierin de goedkeuring van de desbetreffende leidinggevende. De Eigenaar van een informatiesysteem is er verantwoordelijk voor dat dit te allen tijde up-to-date is in een document dan wel elektronisch (informatie)systeem.

De Eigenaar is geautoriseerd en verplicht om de rechten van een gebruiker te verminderen indien nodig. Echter, indien de gebruiker meer rechten dient te hebben, dan is toestemming nodig van zijn of haar leidinggevende. De leidinggevende is er verantwoordelijk voor dat bevoegdheden worden ingetrokken indien bepaalde rechten overbodig c.q. ongewenst zijn geworden door verandering van functie / rol.

11.2.3 Beheer van gebruikerswachtwoorden

De toewijzing van wachtwoorden behoort met een formeel beheerproces te worden beheerst.

De volgende richtlijnen worden gehanteerd:

1. Wachtwoorden van gebruikers mogen niet “plain-tekst” worden gedeeld. Tenzij het een tijdelijk wachtwoord is, waarbij de gebruiker direct verplicht is tot het wijzigen van het wachtwoord.
2. Standaard wachtwoorden zijn niet toegestaan.
3. Wachtwoorden moeten minimaal uit acht (8) tekens bestaan.
4. Bij het bekend worden van een wachtwoord dient dit per direct worden gewijzigd door de gebruiker.
5. Een wachtwoord mag maximaal 6 maanden geldig zijn, na deze periode moet de gebruiker een melding krijgen dat hij of zij het wachtwoord dient te wijzigen. Indien mogelijk wordt dit vastgelegd in het informatiesysteem.

11.2.4 Beoordeling van toegangsrechten van gebruikers

De directie behoort de toegangsrechten van gebruikers regelmatig te beoordelen in een formeel proces.

Zie paragraaf 11.2.2

11.3 Verantwoordelijkheden van gebruikers

Doelstelling:
Voorkomen van onbevoegde toegang door gebruikers, en van beschadiging of diefstal van informatie en IT-voorzieningen.

11.3.1 Gebruik van wachtwoorden

Gebruikers behoren goede beveiligingsgewoontes in acht te nemen bij het kiezen en gebruiken van wachtwoorden.

De volgende richtlijnen gelden voor alle gebruikers:

1. Gebruikersaccounts mogen niet gedeeld worden, het is verboden om in te loggen op een account van iemand anders, dan wel het delen van je eigen account.
2. Alle gebruikers hebben de plicht om zo snel mogelijk de functionaris gegevensbeheer te informeren indien er sprake kan zijn van het uitlekken van informatie, waaronder het wachtwoord. Dit kan tevens via meldingen@dichtbij.coop . Daarnaast dient de gebruiker zijn of haar wachtwoord onmiddellijk te wijzigen.
3. Het wachtwoord dient minimaal één (1) keer per half jaar te worden gewijzigd. Echter wordt het de gebruikers aanbevolen om het wachtwoord één keer per twee (2) maanden te wijzigen.
4. Niet tijdelijke wachtwoorden mogen nooit worden opschreven of ge-e-maild.
5. Als het informatiesysteem de mogelijkheid biedt, dient de gebruiker een 2-factor authenticatie te gebruiken.
6. Gebruik bij de coöperatie een ander wachtwoord dan voor andere locaties (privé, ander werk, etc).
7. Gebruikers moeten altijd controleren of de (web)applicatie van de coöperatie of leverancier van de coöperatie is voor het invoeren van de gebruikersnaam en wachtwoord.
8. De Eigenaren zijn verantwoordelijk voor de reset-procedure van gebruikersnamen en wachtwoorden. Waarbij er zeker dient te zijn, dat de persoon in kwestie daadwerkelijk de gebruiker is. Indien er enige onduidelijkheid ontstaat, dan dient een ID bewijs overhandigd worden.

11.3.2 Onbeheerde gebruikersapparatuur

Gebruikers behoren te bewerkstelligen dat onbeheerde apparatuur passend is beschermd.

De volgende richtlijnen hanteert de coöperatie:

1. Gebruikers dienen hun hardware (computer, mobiel, tablet, etc) te vergrendelen indien zij dit tijdelijk niet meer gebruiken.
2. Apparaten dienen automatisch te worden vergrendeld na een periode van 10 minuten inactiviteit.
3. Het is pas mogelijk om een apparaat te gebruiken na het invoeren van een authenticatiecode.

11.3.3 Clean desk- en clear screen-beleid

Er behoort een clean desk beleid voor papier en verwijderbare opslagmedia en een clear screen beleid voor IT-voorzieningen te worden ingesteld.

Clear desk

Papieren en verwijderbare opslagmedia mogen alleen maar op de tafel liggen wanneer er sprake is van actief gebruik. Indien het niet meer wordt gebruikt, dan dient dit opgeborgen te worden in de daarvoor bedoelde plaatsen. Waarbij de kasten op slot moeten, indien er sprake is van gevoelige informatie (vertrouwelijk en gevoelige documenten, contracten en authenticatiemiddelen – bijvoorbeeld digireaders, sleutels, etc.) en er geen toezicht meer over is door een geautoriseerde gebruiker.

Clear screen

Zie paragraaf 11.3.2.

De direct leidinggevende van de desbetreffende gebruiker is verantwoordelijk voor de controle van het handhaven van zowel de clear desk als screen beleid.

11.4 Toegangsbeheersing voor netwerken

Doelstelling:

Het voorkomen van onbevoegde toegang tot netwerkdiensten.

11.4.1 Beleid ten aanzien van het gebruik van netwerkdiensten

Gebruikers behoort alleen toegang te worden verleend tot diensten waarvoor ze specifiek bevoegd zijn.

Zie paragraaf 11.2.2

11.4.2 Authenticatie van gebruikers bij externe verbindingen

Er behoren geschikte authenticatiemethoden te worden gebruikt om toegang van gebruikers op afstand te beheersen.

De coöperatie werkt alleen met cloud oplossingen, waarbij de authenticatiemethoden hetzelfde zijn als intern. Daarnaast is het (interne) netwerk niet toegankelijk vanuit buitenaf. Gebruikers die extern werken worden wel “extra” bewust gemaakt van de gevaren bij het inloggen om eventuele incidenten te voorkomen.

11.4.3 Identificatie van netwerkapparatuur

Automatische identificatie van apparatuur behoort te worden overwogen als methode om verbindingen vanaf specifieke locaties en apparatuur te authentiseren.

De keuze over de automatische identificatie van apparatuur verschilt per informatiesysteem. De keuze hierin ligt bij de Eigenaar van een desbetreffende informatiesysteem.

11.4.4 Bescherming op afstand van poorten voor diagnose en configuratie

De fysieke en logische toegang tot poorten voor diagnose en configuratie behoort te worden beheerst.

Fysiek
De door de coöperatie beheerde centrale systemen zijn geplaatst in een speciale serverruimte, waarbij er een sleutel benodigd is om binnen te komen. De informatiesystemen van leveranciers dienen minimaal aan dezelfde eis te voldoen. (zie 9.1.1), waarbij onbevoegden geen toegang hebben.

Logisch
Het beheer van de informatiesystemen vindt vaak extern van de organisatie plaats, de volgende richtlijnen worden echter toegepast:

1. Contractueel wordt vastgelegd dat leveranciers voldoen aan de hier genoemde gestelde eisen of voldoen aan een bepaalde veiligheidskeurmerk (NEN 7510, ISO 27001, etc).

11.4.5 Scheiding van netwerken
Groepen informatiediensten, gebruikers en informatiesystemen behoren op netwerken te worden gescheiden.

Bij elke gebruiker wordt afzonderlijk gekeken tot welke informatiediensten en op welk authorisatieniveau (rechten) hij of zij toegang moet en mag hebben. Publieke netwerken mogen niet gebruikt worden.

11.4.6 Beheersmaatregelen voor netwerkverbindingen
Voor gemeenschappelijke netwerken, vooral waar deze de grenzen van de organisatie overschrijden, behoren de toegangsmogelijkheden voor gebruikers te worden beperkt, overeenkomstig het toegangsbeleid en de eisen van bedrijfstoepassingen.

Naast de blokkering gesteld, zie 11.4.5, vinden, indien nodig, alleen op applicatieniveau aanvullend validatie van de gebruiker plaats.

11.4.7 Beheersmaatregelen voor netwerkroutering
Netwerken behoren te zijn voorzien van beheersmaatregelen voor netwerkroutering, om te bewerkstelligen dat computerverbindingen en informatiestromen niet in strijd zijn met het toegangsbeleid voor de bedrijfstoepassingen.

Interne netwerken moeten te alle tijden worden beheerd door professionele partijen. Waarbij de verantwoordelijkheid omtrent netwerkroutering is vastgelegd.

11.5 Toegangsbeveiliging voor besturingssystemen

Doelstelling:
Voorkomen van onbevoegde toegang tot besturingssystemen.

11.5.1 Beveiligde inlogprocedures
Toegang tot besturingssystemen behoort te worden beheerst met een beveiligde inlogprocedure.

De volgende richtlijnen dienen te worden gevolgd omtrent de inlogprocedures:

1. Er wordt tijdens het inloggen geen extra informatie vrijgegeven die misbruikt kan worden door derden.
2. Indien een fout optreedt, zal het systeem niet aangeven welke gegevens juist of onjuist zijn.
3. Het toegelaten aantal inlogpogingen is beperkt tot een aantal keer, waarbij de gebruiker tijdelijk moet wachten voordat hij of zij weer kan inloggen.
4. Het ingevoerde wachtwoord wordt nooit plain-tekst weergegeven.

11.5.2 Gebruikersidentificatie en -authenticatie

Elke gebruiker behoort over een unieke identificatiecode te beschikken (gebruikers-ID) voor uitsluitend persoonlijk gebruik, en er behoort een geschikte authenticatietechniek te worden gekozen om de geclaimde identiteit van de gebruiker te bewijzen.

Elke gebruiker heeft een persoonlijke gebruikersnaam (gebruikers-ID) en wachtwoord. Deze gebruikersnaam en wachtwoord is op persoonlijke naam en mag dus niet worden gebruikt door anderen. De acties die worden verricht op basis van deze gebruikersnaam vallen onder de verantwoordelijkheid van de desbetreffende gebruiker.

Toegang via algemene accounts is niet toegestaan, tenzij hier een duidelijk en gedocumenteerd zakelijke noodzaak voor is. Daarnaast is beschreven wie verantwoordelijk is voor de account en monitort de Eigenaar van het desbetreffende informatiesysteem de handelingen van het desbetreffende account.

11.5.3 Systemen voor wachtwoordbeheer

Systemen voor wachtwoordbeheer behoren interactief te zijn en moeten bewerkstelligen dat wachtwoorden van geschikte kwaliteit worden gekozen.

Er is geen centraal aanmeldsysteem actief. De kaders van 11.3.1 zijn geldig voor alle (informatie)systemen.

11.5.4 Gebruik van systeemhulpmiddelen

Het gebruik van hulpprogrammatuur waarmee systeem- en toepassingsbeheersmaatregelen zouden kunnen worden gepasseerd behoort te worden beperkt en behoort strikt te worden beheerst

Dit is niet van toepassing binnen de coöperatie, alle informatiesystemen worden namelijk via een web portaal beheerd.

11.5.5 Time-out van sessies

Inactieve sessies behoren na een vastgestelde periode van inactiviteit te worden uitgeschakeld.

Indien instelbaar dienen sessies na 24 uur activiteit te worden uitgeschakeld. Anders dienen de standaardinstellingen van de programmatuur of service gevolgd te worden.

11.5.6 Beperking van verbindingstijd

De verbindingstijd behoort te worden beperkt als aanvullende beveiliging voor toepassingen met een verhoogd risico.

De standaardinstellingen van de programmatuur of service wordt gevolgd.

11.6 Toegangsbeheersing voor toepassingen en informatie

Doelstelling:
Voorkomen van onbevoegde toegang tot informatie in toepassingssystemen.

11.6.1 Beperken van toegang tot informatie

Toegang tot informatie en functies van toepassingssystemen door gebruikers en ondersteunend personeel behoort te worden beperkt overeenkomstig het vastgestelde toegangsbeleid

De Eigenaren dienen een “least privilege” beginsel toe te passen, zie zie paragraaf 11.1.1). Eigenaren dienen elke week de verwerkingen van de leidinggevenden te controleren en gebruikers te verwijderen die:

1. Geen toegang meer nodig hebben tot het systeem (bijvoorbeeld als gebruikers niet meer voor de coöperatie werken).

En gebruikers te wijzigen die:

1. Andere rechten nodig hebben (bijvoorbeeld minder of meer bevoegdheid);

Leidinggevenden zijn verantwoordelijk om periodiek te controleren in hoeverre de wijzigingen zijn doorgevoerd.

11.6.2 Isoleren van gevoelige systemen

Alle systemen van de cooperatie draaien via verschillende (informatie)systemen. Waarbij er interconnectie bestaat via api’s. Indien er sprake is van een fout of exploit binnen één van de systemen, dient er door de Eigenaar een besluit te worden gemaakt om de connectie (tijdelijk) stop te zetten. Daarnaast dient de Eigenaar de functionaris gegevensbescherming te informeren. Dit kan tevens via meldingen@dichtbij.coop

11.7 Draagbare computers en telewerken

Doelstelling:
Waarborgen van informatiebeveiliging bij het gebruik van draagbare computers en faciliteiten voor telewerken

11.7.1 Draagbare computers en communicatievoorzieningen

Er behoort formeel beleid te zijn vastgesteld en er behoren geschikte beveiligingsmaatregelen te zijn getroffen ter bescherming tegen risico's van het gebruik van draagbare computers en communicatiefaciliteiten.

Naast de punten zoals omschreven in paragraaf 7.1, dient er nog rekening te worden gehouden met het volgende:

1. Indien een mobiel gestolen of op een andere manier verdwenen is, dan dient te worden gemeld aan de direct leidinggevende die het vervolgens weer dient te registreren en indien nodig te rapporteren aan de functionaris gegevensbescherming; Dit kan tevens via meldingen@dichtbij.coop
2. De gebruiker zorgt er voor dat de privé apparatuur voldoende is beveiligd, met tenminste een toegangsbeveiliging (pincode, wachtwoord of iets dergelijks);
3. Het apparaat is veilig, dit betekent dat er geen virussen of andere schadelijke software op zit. Daarnaast is het apparaat up-to-date.

11.7.2 Telewerken

Er behoren beleid, operationele plannen en procedures voor telewerken te worden ontwikkeld en geïmplementeerd.

Zie paragraaf 11.4.2.

12 Verwerving, ontwikkeling en onderhoud van informatiesystemen

12.1 Beveiligingseisen voor informatiesystemen

Doelstelling:
Bewerkstelligen dat beveiliging integraal deel uitmaakt van informatiesystemen.

12.1.1 Analyse en specificatie van beveiligingseisen

In bedrijfseisen voor nieuwe informatiesystemen of uitbreidingen van bestaande informatiesystemen behoren ook eisen voor beveiligingsmaatregelen te worden opgenomen.

Indien er sprake is van een implementatie dan wel beslissingmoment tot het verkrijgen of gebruikmaken van een nieuw of een wijziging van een bestaand informatiesysteem wordt er onder verantwoordelijkheid van de Eigenaar zo snel mogelijk het informatiesysteem geclassificeerd volgens het "standaard" classificatiesysteem van de coöperatie; wat betreft vertrouwelijkheid, integriteit en vertrouwelijkheid,

Alleen indien er sprake is van een beveiligingsklasse "kritiek" dient er een aanvullende risicoanalyse te worden uitgevoerd. De risicoanalyse bestaat uit een gestandaardiseerd format. Alle gestelde (beveiligings)eisen maken integraal onderdeel uit van de acceptatiecriteria en de keuze van een bepaald informatiesysteem wordt weloverwogen gemaakt, waarbij de mogelijke negatieve gevolgen voor de aantasting van beschikbaarheid, integriteit en/of vertrouwelijkheid verder zijn toegelicht.

Standaard inrichtingseisen
De coöperatie kent standaardeisen met betrekking tot nieuwe informatiesystemen. Hieronder staan deze beschreven:

1. Er wordt zoveel mogelijk met bewezen standaardsystemen gewerkt (zoals applicaties, desktops, netwerkapparatuur en cloud oplossingen) oftewel in andere woorden; overal dezelfde types computers, één systeem voor boekhouding, etc.
2. Standaard wachtwoorden zijn niet toegestaan, gebruikers moeten ook niet de mogelijkheid hebben om standaard wachtwoorden te gebruiken voor hun systeem.
3. Systemen moeten zoveel mogelijk 'kaal' zijn. Alle overbodige functionaliteit moeten zijn verwijderd of niet meer te zien zijn voor gebruikers van de informatiesystemen.
4. Eisen m.b.t. back-up van gegevens (zie 10.5.1), (installatie van) beveiligingspatches (zie 12.6.1), bestrijding van malware (zie 10.4.1), logging en monitoring (zie onder meer 10.10), authenticatie van gebruikers en beheerders (zie 11.5) en capaciteitsbeheer (zie 10.3.1).

Beveiligingseisen cloudapplicaties (Webapplicaties)
Indien er cloudapplicaties worden ontwikkeld of verwerft dan ziet de Eigenaar er op toe, dat er minimaal wordt voldaan aan de ICT-beveiligingstandaarden en richtlijnen voor webapplicaties. Als standaard gebruikt de coöperatie tenminste de richtlijnen van het Nationaal Cyber Security Centrum (NCSC).

Bij uitbesteding
Indien de coöperatie besluit kant en klare oplossingen aan te schaffen, dan is de Eigenaar verantwoordelijk voor het feit dat:

1. De juiste procedure wordt gevolgd
2. Er een extra controle plaatsvindt met betrekking tot de beveiligingseisen (voldoet de organisatie en applicatie aan de gestelde beveiligingseisen?).

3. Er een gedocumenteerd document wordt ontwikkeld waarin te zien is hoe de beveiligingseisen zijn getest en geëvalueerd met hierin ook een conclusie, waarbij er gemoti is waarom de eventuele risico's worden geaccepteerd dan wel worden geneutraliseerd.

12.2 Correcte verwerking in toepassingen

Doelstelling:
Voorkomen van fouten, verlies, onbevoegde modificatie of misbruik van informatie in toepassingen.

12.2.1 Validatie van invoergegevens
Gegevens die worden ingevoerd in toepassingen behoren te worden gevalideerd om te bewerkstelligen dat deze gegevens juist en geschikt zijn.

Alle invoer wordt automatisch of handmatig gecontroleerd door de systemen dan wel geautoriseerde gebruikers die bij het invoerproces betrokken zijn. Er wordt minimaal gecontroleerd op ongeldige tekens, syntax controle (format onjuist), onvolledige gegevens en inconsistentie van de gegevens (door middel van verbandscontroles).

12.2.2 Beheersing van interne gegevensverwerking
Er behoren validatiecontroles te worden opgenomen in toepassingen om eventueel corrumperen van informatie door verwerkingsfouten of opzettelijke handelingen te ontdekken.

De informatiesystemen dienen functionaliteit te hebben om verwerkings- en andere onjuistheden te kunnen detecteren en corrigeren.

12.2.3 Integriteit van berichten
Er behoren eisen te worden vastgesteld, en geschikte beheersmaatregelen te worden vastgesteld en geïmplementeerd, voor het bewerkstelligen van authenticiteit en het beschermen van integriteit van berichten in toepassingen.

Alle informatiesystemen dienen encryptie en/of een digitale handtekening te hebben om de authenticiteit en integriteit (juistheid en volledigheid) te waarborgen van alle berichten die worden uitgewisseld.

12.2.4 Validatie van uitvoergegevens
Gegevensuitvoer uit een toepassing behoort te worden gevalideerd, om te bewerkstelligen dat de verwerking van opgeslagen gegevens op de juiste manier plaatsvindt en geschikt is gezien de omstandigheden.

De informatiesystemen dienen de juistheid en volledigheid van uitgevoerde gegevens vast te stellen, dit wordt onder andere gerealiseerd door een controlecijfer, checksum of andere systemen. Een controlecijfer, checksum en dergelijke zijn systemen om redundantie te creëren in gegevens om het invoeren, lezen, schrijven en verzenden ervan te controleren, op een wijze die efficiënter is dan alles twee keer doen. Er wordt een methode gebruikt die weliswaar geen volledige controle biedt maar de kans groot maakt dat een fout wordt gedetecteerd.

Eén mogelijkheid is dat voor en na de te controleren actie een resultaat wordt berekend (compacter dan de gegevens zelf) en de twee resultaten worden vergeleken. Praktisch voorbeeld: totaalsom laten berekenen door het systeem en daarna andere sources gebruiken en alle individuele onderdelen op te tellen.

Bij uitvoergegevens wordt er gecontroleerd dat er goed wordt omgegaan met de aard van vertrouwelijkheid. Gebruikers mogen alleen uitvoergegevens gebruiken dan wel exporteren als zij de bevoegdheid hebben om dit te doen.

12.3 Cryptografische beheersmaatregelen

Doelstelling:
Beschermen van de vertrouwelijkheid, authenticiteit of integriteit van informatie met behulp van cryptografische middelen.

12.3.1 Beleid voor het gebruik van cryptografische beheersmaatregelen

Er behoort beleid te worden ontwikkeld en geïmplementeerd voor het gebruik van cryptografische beheersmaatregelen voor de bescherming van informatie.

Alle externe systemen maken gebruik van cryptografische middelen, de mate complexiteit van maatregel hangt af van de aard van de te gegevens. Voor de beoordeling van de beveiliging wordt gebruik gemaakt van de tabel met de daarin genoemde beveiligingseisen (paragraaf 7.2).

Bij de inzet van cryptografische middelen dient een afweging te worden gemaakt van de risico's aangaande locaties, processen en behandelende partijen in relatie tot de te beveiligen gegevens. Hierbij kan gebruik gemaakt worden van de tabel met beveiligingseisen in Paragraaf 7.2.

12.3.2 Sleutelbeheer

Er behoort sleutelbeheer te zijn vastgesteld ter ondersteuning van het gebruik van cryptografische technieken binnen de organisatie.

De Eigenaar van cryptografische technieken is verantwoordelijk voor de volgende onderdelen:

1. De generatie en onderhoud (intrekken, publiceren, verwijderen, etc) van tijdelijke certificaten. Deze tijdelijke certificaten kunnen verkregen zijn van externe partijen (Comodo, Geotrust, RapidSSL, etc).
2. De installatie van certificaten op informatiesystemen (servers, computers of andere hardware).
3. Dat elke gebruiker binnen de coöperatie alleen geldige certificaten kan gebruiken om toegang te verkrijgen tot een systeem.
4. Het bijhouden van een registratie van sleutels en certificaten, inclusief geldigheidsduur. Onder andere het actualiseren van sleutels en certificaten dan wel het informeren van leveranciers of gebruikers over het feit dat een bepaalde sleutel of certificaat niet meer up-to-date is.

Indien een sleutel is gecompromitteerd, dan volgen de volgende maatregelen:

1. De desbetreffende informatiesystemen zullen (indien mogelijk) per direct afgesloten van extern toegang.
2. Nieuwe sleutel wordt gegeneerd, waarbij de oude komt te vervallen.
3. Gebruikers worden zo snel mogelijk op de hoogte gesteld.
4. Oorzaak dient te worden gevonden en opgelost. Indien nodig zal wederom een nieuwe sleutel moeten worden gegeneerd.

12.4 Beveiliging van systeembestanden

Doelstelling:
Beveiliging van systeembestanden bewerkstelligen.

12.4.1 Beheersing van operationele programmatuur

Er behoren procedures te zijn vastgesteld om de installatie van programmatuur op productiesystemen te beheersen.

Productiesystemen worden continue gebruikt door verschillende gebruikers binnen de coöperatie. Het is dan ook van belang, dat risico van verstoring tot een minimum dient te worden beperkt. Hiervoor zijn de volgende richtlijnen van kracht:

1. Installatie van nieuwe software binnen de productieomgeving van de coöperatie vindt alleen plaats indien het volledige traject doorlopen is, waarbij er een gedocumenteerde analyse heeft plaatsgevonden. Dit betekent dat er rekening wordt gehouden met het volgende en het volgende wordt uitgevoerd:
    a. Risicoanalyse
    b. Terugdraaiscenario document (bij hoog risico profiel).
    c. Software is volwaardig (geen alpha, beta versies).
    d. Handleidingen van leveranciers worden grondig gelezen en in acht genomen.
2. Alle software op de apparaten van de coöperatie worden automatisch bijgewerkt om eventuele exploits te verminderen. Dit geldt alleen voor updates, het uitvoeren van upgrades vindt uitsluitend plaats na goedkeuring als alle tests gedocumenteerd zijn en een positief resultaat hebben.
3. Alle veranderingen van (informatie)systemen en overige assets dienen te worden geregistreerd.

12.4.2 Bescherming van testdata

Testgegevens behoren zorgvuldig te worden gekozen, beschermd en beheerst.

Indien er sprake is van testdata, dan dienen de volgende richtlijnen in acht te worden gehouden:

1. Testdata moet een realistische weergave hebben van de operationele productieomgeving, echter een exacte kopie van de operationele productieomgeving mag alleen worden gemaakt indien er toestemming is van de functionaris gegevensbescherming. Daarnaast gelden bij het gebruik van deze data tenminste dezelfde beveiligingseisen als op de productieomgeving.
2. De toegang tot testdata, indien er sprake is van gevoelige gegevens, wordt beschermd als de zelfde wijze als op de productieomgeving.
3. Alle testgegevens dienen niet langer dan strikt noodzakelijk te worden bewaard.
4. Indien een externe partij de testdata gebruikt, dan ziet de Eigenaar erop toe dat de testdata wordt verwijderd.

12.4.3 Toegangsbeheersing voor broncode van programmatuur

De toegang tot broncode van programmatuur behoort te worden beperkt.

De toegang tot de broncode wordt beschermd tegen onbedoelde wijzigingen. Dit wordt gerealiseerd door alleen geautoriseerde personen toegang tot de broncode.

12.5 Beveiliging bij ontwikkelings- en ondersteuningsprocessen

Doelstelling:
Beveiliging van toepassingsprogrammatuur en -informatie handhaven.

12.5.1 Procedures voor wijzigingsbeheer

De implementatie van wijzigingen behoort te worden beheerst door middel van formele procedures voor wijzigingsbeheer.

Dit is in paragraaf 10.1.2 beschreven.

12.5.2 Technische beoordeling van toepassingen na wijzigingen in het besturingssysteem.

Bij wijzigingen in besturingssystemen behoren bedrijfskritische toepassingen te worden beoordeeld en getest om te bewerkstelligen dat er geen nadelige gevolgen zijn voor de activiteiten of beveiliging van de organisatie.

Indien er sprake is van een wijziging met betrekking tot besturingssysteem op productiesystemen, beoordeelt de coöperatie vooraf in hoeverre dit negatieve gevolgen heeft voor de beveiliging en de bestaande beheersmaatregelen. Er wordt voornamelijk gefocust in hoeverre het onderstaande werkt:

- Logging;
- Monitoring;
- logische toegangsbeveiliging;
- encryptie
- correcte werking van functionaliteiten.

Indien één van de bovenstaande punten niet of onvoldoende werkt, dan dient het besturingssysteem niet te worden gewijzigd.

12.5.3 Restricties op wijzigingen in programmatuurpakketten

Wijzigingen in programmatuurpakketten behoren te worden ontmoedigd, te worden beperkt tot noodzakelijke wijzigingen, en alle wijzigingen behoren strikt te worden beheerst.

Er worden alleen wijzigingen aan software- en cloudoplossingen gebracht indien hier een dwingende reden voor bestaat, zoals een duidelijke en zakelijke aanleiding. Bij een wijziging dient in ieder geval rekening te worden gehouden met:

1. Exploits doordat bestaande beveiligingsmaatregelen onvoldoende werken.
2. Gevolgen omtremt de support door leveranciers.
3. Het missen van bepaalde updates (in verband met het niet meer kunnen updaten).

Alle eventuele wijzigingen worden getest en gedocumenteerd voordat ze worden geïmplementeerd in de productieomgeving. Tevens wordt er een back-up gemaakt van de originele software (zonder de maatwerk).

12.5.4 Uitlekken van informatie

Er behoort te worden voorkomen dat zich gelegenheden voordoen om informatie te laten uitlekken.

Er wordt minimaal naar het onderstaande gekeken en toepast:

1. Onbedoelde of onnodige informatie in de gegevens, documenten en communicatieverkeer.
2. Het vrijgeven van informatie (alleen het noodzakelijke wordt vrijgegeven aan derden die daarvoor voldoende autoriteit hebben).
3. Logging

12.5.5 Uitbestede ontwikkeling van programmatuur

Uitbestede ontwikkeling van programmatuur behoort onder supervisie te staan van en te worden gecontroleerd door de organisatie.

Alle software dient te voldoen aan de gestelde eisen, de Eigenaar ziet erop toe dat alles voldoet aan de eisen gesteld in paragraaf 12.1.

Daarnaast dient te worden gekeken, wie verantwoordelijk is, welke rechten en plichten naar voren komen binnen het proces:

1. Wie wordt de eigenaar van de software?
2. Alles dient te zijn vastgelegd in een overeenkomst (tevens de eisen zoals omschreven in dit document).
3. Controleren of aan alle eisen is voldaan, zoals beschreven in de overeenkomst.
4. Analyse dient plaats te vinden in hoeverre de programmatuur voldoet aan eventuele wijzigingen sinds het maken van de overeenkomst.

12.6 Beheer van technische kwetsbaarheden

Doelstelling:
Risico's verminderen als gevolg van benutting van gepubliceerde technische kwetsbaarheden

12.6.1 Beheersing van technische kwetsbaarheden

Er behoort tijdig informatie te worden verkregen over technische kwetsbaarheden van de gebruikte informatiesystemen. De mate waarin de organisatie blootstaat aan dergelijke kwetsbaarheden behoort te worden geëvalueerd en er behoren geschikte maatregelen te worden genomen voor behandeling van daarmee samenhangende risico's.

De Eigenaren zijn verantwoordelijk voor het geïnformeerd zijn over de technische kwetsbaarheden van de gebruikte informatiesystemen. Maandelijks dienen de Eigenaren de technische kwetsbaarheden van de informatiesystemen te evalueren. Indien nodig dienen zij na overleg met de leidinggevende aanpassingen door te voeren om de informatiesystemen te verbeteren.

13. Beheer van informatiebeveiligingsincidenten

13.1 Rapportage van informatiebeveiligingsgebeurtenissen en zwakke plekken

Doelstelling:
Bewerkstelligen dat informatiebeveiligingsgebeurtenissen en zwakheden die verband houden met informatiesystemen zodanig kenbaar worden gemaakt dat tijdig corrigerende maatregelen kunnen worden genomen.

13.1.1 Rapportage van informatiebeveiligingsgebeurtenissen

Informatiebeveiligingsgebeurtenissen behoren zo snel mogelijk via de juiste leidinggevende niveaus te worden gerapporteerd.

Alle incidenten (gebeurtenissen) worden geregistreerd door de coöperatie, waarbij in het geval van een informatiebeveiligingsgebeurtenis (informatiebeveiligingsincident) er wordt gekeken in hoeverre dit gevolgen heeft voor de coöperatie dan wel andere stakeholders.

Onder informatiebeveiligingsincident vallen:

1. Verlies van apparatuur of voorzieningen
2. Systeemstoring
3. Menselijke fouten op het gebied van informatie en/of informatiesystemen.
4. Niet naleven van beleid en/of richtlijnen van dit document
5. Inbreuk op fysieke beveilingssystemen
6. Onbeheerste systeemwijziging
7. Storing aan programmatuur of apparatuur
8. Toegangsovertredingen
9. Verminking, verlies en onbedoelde openbaarmaking van gevoelige gegevens, waaronder maar niet beperkt tot patiëntengegevens.
10. Zwakke plekken binnen de informatiedeling, systemen en/of diensten.

Deze incidenten worden direct gemeld bij de desbetreffende Leidinggevende of opdrachtgever én de functionaris gegevensbescherming. Dit kan tevens via meldingen@dichtbij.coop

Waarbij tenminste het volgende wordt geregistreerd:

1. Tijdstip van het incident en tijdstip van ontvangst
2. Omschrijving van het incident
3. Betrokken personen
4. Wat er exact is gebeurd (analyse).
5. In geval van datalekken waarbij privacygevoelige informatie (zoals patiëntgegevens) is de functionaris gegevensbescherming verplicht tot het zo spoedig melden aan het CBP. Daarnaast dienen de stakeholders geïnformeerd te worden over het datalek.
6. Vervolgstappen (Wat is er gedaan om dit in de toekomst te voorkomen).
7. Wat heeft dit incident gekost?
8. Wat hebben de maatregelen gekost?

De desbetreffende gebruikers, Eigenaren en Leidinggevenden krijgen een terugkoppeling op basis van de genoteerde gegevens.

13.1.2 Rapportage van zwakke plekken in de beveiliging

Van alle werknemers, ingehuurd personeel en externe gebruikers van informatiesystemen en -diensten behoort te worden geëist dat zij alle waargenomen of verdachte zwakke plekken in systemen of diensten registreren en rapporteren.

In de gebruikersovereenkomst met alle gebruikers van de informatiesystemen staan de verantwoordelijkheden van de gebruikers. Hierin is ook opgenomen dat zij zich conformeren naar het opgestelde beleid (dit document). Daarnaast dienen zij alles te melden op het gebied van beveiligingsincidenten en wordt er overeengekomen dat zij alle waargenomen en verdachte zwakke plekken binnen de informatiedeling, systemen en/of diensten registreren (zoals beschreven in 13.1.1).

13.2 Beheer van informatiebeveiligingsincidenten en –verbeteringen

Doelstelling:
Bewerkstelligen dat een consistente en doeltreffende benadering wordt toegepast voor het beheer van informatiebeveiligingsincidenten.

13.2.1 Verantwoordelijkheden en procedures

Er behoren leidinggevende verantwoordelijkheden en procedures te worden vastgesteld om een snelle, doeltreffende en ordelijke reactie op informatiebeveiligingsincidenten te bewerkstelligen.

Leidinggevenden zijn uiteindelijk eindverantwoordelijk wat er door de gebruikers wordt uitgevoerd. Zij dienen er dan ook op toe te zien, dat gebruikers zich houden aan het beleid en het geldende gebruikersovereenkomst. Daarnaast dienen zij erop toe te zien, dat incidenten direct worden gemeld en dat de aanwijzingen van de Eigenaar en functionaris gegevensbescherming worden uitgevoerd.

13.2.2 Leren van informatiebeveiligingsincidenten

Er behoren mechanismen te zijn ingesteld waarmee de aard, omvang en kosten van informatiebeveiligingsincidenten kunnen worden gekwantificeerd en gecontroleerd.

Alle (beveiligingsincidenten) worden geregistreerd (zie paragraaf 13.1.1), waarbij de aard, omvang en kosten van informatiebeveiligingsincidenten worden vastgesteld. De registratie dient tevens te worden gebruikt voor analyses en waarbij de risico's verder geminimaliseerd kunnen worden. De analyses dienen plaats te vinden tegelijk met de periodieke bespreking van Eigenaren (zie paragraaf 12.6.1).

13.2.3 Verzamelen van bewijsmateriaal

Waar een vervolgprocedure tegen een persoon of organisatie na een informatiebeveiligingsincident juridische maatregelen omvat (civiel of strafrechtelijk), behoort bewijsmateriaal te worden verzameld, bewaard en gepresenteerd overeenkomstig de voorschriften voor bewijs die voor het relevante rechtsgebied zijn vastgelegd.

De opdracht voor het verzamelen van bewijsmateriaal dient te worden gegeven door de RvB. Waarbij het verzamelen van bewijs dient te gebeuren door twee (onafhankelijke) personen die het bewijsmateriaal zal verzamelen. Het volgende dient minimaal te worden geregistreerd:

- Datum van bevinding
- Datum van gebeurtenis
- Plaats van gebeurtenis
- Plaats van gebeurtenis
- Omschrijving van bevinding
- Onderzoeker 1
- Onderzoeker 2

14 Bedrijfscontinuïteitsbeheer

14.1 Informatiebeveiligingsaspecten van bedrijfs-continuïteitsbeheer

Doelstelling:
Onderbreken van bedrijfsactiviteiten tegengaan en kritische bedrijfsprocessen beschermen tegen de gevolgen van omvangrijke storingen in informatiesystemen of rampen en om tijdig herstel te bewerkstelligen.

14.1.1 Informatiebeveiliging opnemen in het proces van bedrijfscontinuïteitsbeheer

Er behoort een beheerd proces voor bedrijfscontinuïteit in de gehele organisatie te worden ontwikkeld en bijgehouden, voor de naleving van eisen voor informatiebeveiliging die nodig zijn voor de continuïteit van de bedrijfsvoering.

Het bestuur van de coöperatie is de eigenaar van dit proces. Zij zijn dus verantwoordelijk voor de volgende onderdelen, waarbij dit schriftelijk dient te kunnen worden gecontroleerd:

1. Het up-to-date houden van dit document;
2. Het periodiek beoordelen van de risico's die bedrijfscontinuniteit kunnen beïnvloeden;
3. Het vaststellen van een begroting voor preventieve en repressieve continuïteitsmaatregelen;
4. Periodiek overleg van de Eigenaren monitoren en de leidinggevenden van de betrokken Eigenaren op functioneren van de controle beoordelen (met betrekking tot dit document).

Business Continuity Management waaronder 'disaster recovery', wordt gezien als een vereiste. Vanwege de strenge beschikbaarheidseisen in de zorg is een grote inspanning van ons vereist om robuustheid en redundancy te bereiken voor de infrastructuur en voor de beschikbaarheid van gebruikers. Daarom zijn Eigenaren verantwoordelijk voor het ontwikkelen van een (back-up / acceptatie) plan voor als het desbetreffende asset niet meer goed functioneert.

14.1.2 Bedrijfscontinuïteit en risicobeoordeling

Gebeurtenissen die tot onderbreking van bedrijfsprocessen kunnen leiden, behoren te worden geïdentificeerd, tezamen met de waarschijnlijkheid en de gevolgen van dergelijke onderbrekingen en hun gevolgen voor informatiebeveiliging.

Tenminste eenmaal per jaar wordt er een risicoanalyse uitgevoerd, waar de Eigenaren van alle informatiesystemen integraal onderdeel van uitmaken. De risicoanalyse dient schriftelijk te worden vastgelegd.

14.1.3 Continuïteitsplannen ontwikkelen en implementeren waaronder informatiebeveiliging

Er behoren plannen te worden ontwikkeld en geïmplementeerd om de bedrijfsactiviteiten te handhaven of te herstellen en om de beschikbaarheid van informatie op het vereiste niveau en in de vereiste tijdspanne te bewerkstelligen na onderbreking of uitval van kritische bedrijfsprocessen.

Per informatiesysteem is er een actielijst ontwikkeld, die wordt opgevolgd op het moment dat er sprake is van een onderbreking of uitval van een kritische bedrijfsproces. Eigenaren van de informatie zijn hier in basis verantwoordelijk voor. Periodiek, zie Paragraaf 14.1.5, wordt er gekeken in hoeverre de organisatie is voorbereid op een uitval of onderbreking.

14.1.4 Kader voor de bedrijfscontinuïteitsplanning

Er behoort een enkelvoudig kader voor bedrijfscontinuïteitsplannen te worden gehandhaafd om te bewerkstelligen dat alle plannen consistent zijn, om eisen voor informatiebeveiliging op consistente wijze te behandelen en om prioriteiten vast te stellen voor testen en onderhoud.

De kaders voor de bedrijfscontinuïteitsplannen zijn als volgt:

1. Indien mogelijk wordt er een duidelijke flowchart ontwikkeld, met zo min mogelijk tekst, maar waarbij de acties duidelijk zijn.
2. De bedrijfscontinuïteitsplannen zijn up-to-date.

14.1.5 Testen, onderhoud en herbeoordelen van bedrijfscontinuïteitsplannen

Bedrijfscontinuïteitsplannen behoren regelmatig te worden getest en geüpdatet, om te bewerkstelligen dat ze actueel en doeltreffend blijven.

Periodiek, maar tenminste éénmaal per jaar worden er oefeningen en testen gehouden om de bedrijfscontinuïteitsplannen en organisatie te toetsen. Door bijvoorbeeld een diefstal te simuleren. Aan de hand van de uitkomsten worden de bedrijfscontinuïteitsplannen geüpdatet en worden er activiteiten gestart om de negatieve consequenties op de organisatie te verbeteren.

15. Naleving

In hoofdstuk 4 staan de uitgangspunten met betrekking tot de kaders van de wet beschreven. In dit hoofdstuk wordt beschreven hoe de Coöperatie er zorg voor draagt dat schending van wetgeving, aangegeven normen, wettelijke en regelgevende of contractuele verplichtingen niet worden geschonden.

15.1 Naleving van wettelijke voorschriften

Doelstelling:
Voorkomen van schending van enige wetgeving, wettelijke en regelgevende of contractuele verplichtingen, en van enige beveiligingseisen.

15.1.1 Identificatie van toepasselijke wetgeving

Alle relevante wettelijke en regelgevende eisen en contractuele verplichtingen en de benadering van de organisatie in de naleving van deze eisen, behoren expliciet te worden vastgesteld, gedocumenteerd en actueel te worden gehouden voor elk informatiesysteem en voor de organisatie.

Alle relevante verplichtingen, (regel- en wetgeving en contractuele) worden centraal bijgehouden. Waarbij er per informatiesysteem wordt geregistreerd welke wettelijke en regelgevende eisen en contractuele verplichtingen van belang zijn voor het gebruik van het informatiesysteem.

De Eigenaar van het desbetreffende informatiesysteem is verantwoordelijk voor het up-to-date houden van de “toepasselijke wetgeving” registratie.

15.1.2 Intellectuele eigendomsrechten (Intellectual Property Rights, IPR)

Er behoren geschikte procedures te worden geïmplementeerd om te bewerkstelligen dat wordt voldaan aan de wettelijke en regelgevende eisen en contractuele verplichtingen voor het gebruik van materiaal waarop intellectuele eigendomsrechten kunnen berusten en het gebruik van programmatuur waarop intellectuele eigendomsrechten berusten.

Alle software, hardware en overige zaken zullen worden gekocht van gespecialiseerde leveranciers of zullen in-house worden ontwikkeld. Er kan gebruik worden gemaakt van (externe) bronnen, naar deze bronnen dient te worden gerefereerd op het moment van publicatie intern of extern. Leveranciers, medewerkers en leden ondertekenen een overeenkomst waarin staat beschreven dat de intellectuele eigendomsrechten bij de coöperatie hoort, indien zij een nieuw product of dienst voor de coöperatie ontwikkelen. Hiervan kan echter af worden geweken, dit dient echter wel te worden geregistreerd, met een expliciete zakelijke reden.

15.1.3 Bescherming van bedrijfsdocumenten

Belangrijke registraties behoren te worden beschermd tegen verlies, vernietiging en vervalsing, overeenkomstig wettelijke en regelgevende eisen, contractuele verplichtingen en bedrijfsmatige eisen.

Registraties kunnen slechts éénmalig worden ingevoerd, waarbij het niet mogelijk is om de registraties individueel te verwijderen.

Voor zo ver mogelijk worden registraties (o.a. logs) centraal geback-upt door de Eigenaar, waarbij de RvB toegang heeft tot de desbetreffende map. De RvB is verantwoordelijk dat dit ook tenminste eenmaal per week gebeurt.

15.1.4 Bescherming van gegevens en geheimhouding van persoonsgegevens

De bescherming van gegevens en privacy behoort te worden bewerkstelligd overeenkomstig relevante wetgeving, voorschriften en indien van toepassing contractuele bepalingen.

De coöperatie verwerkt en beheert de gegevens conform de AVG en eventuele andere eisen die van kracht zijn op de desbetreffende type data. Er wordt tenminste rekening gehouden met onder andere:

1. Doelen van verzamelen en verwerken van gegevens worden geregistreerd, daarnaast wordt er gekeken in hoeverre dit conform de wet- en regelgeving is.
2. Gegevens worden alleen verzamelt en gebruikt in overstemming met het omschreven doel en volgens de richtlijnen van de WPB.
3. Alle persoonsgegevens worden op basis van wettelijke termijnen bewaard. Waarbij indien er een gegronde reden bestaat, er een uitzondering kan worden gemaakt. Indien mogelijk zullen de gegevens worden geanonimiseerd danwel gepseudonimiseerd. Dit houdt in dat de gegevens worden omgezet naar een niet tot de oorspronkelijke persoon herleidbare unieke code.
4. Elke gebruiker dient geheimhouding te betrachten. Dit kan bijvoorbeeld door een arbeidsovereenkomst met een geheimhoudingsclausule of een opdrachtovereenkomst waarin een clausule is opgenomen over geheimhouding.
5. Er worden weloverwegen technische en organisatorische maatregelen genomen om het onbedoeld vernietigen, wijzigen of vrijgeven van persoonsgegevens zo veel mogelijk te minimaliseren. Deze maatregelen garanderen, rekening houdend met de stand van de techniek en de kosten van de tenuitvoerlegging, een passend beveiligingsniveau gelet op de risico's die de verwerking en de aard van te beschermen gegevens met zich meebrengen.
6. Er een verwerkersovereenkomst gesloten met een verwerkelijk, waarbij de wettelijke verplichtingen van zowel de coöperatie als de verwerkelijk zijn opgenomen. Eigenaar van het informatiesysteem verantwoordelijk is dat er krachtens de overeenkomst wordt gehandeld.
7. Alle maatregelen en de risicoanalyse die daarvoor vanaf ging dienen te zijn vastgelegd en te bewaard.
8. Eigenaren zijn verantwoordelijk voor het conformeren aan de eisen genoemd in dit document.
9. Leidinggevenden zijn verantwoordelijk voor de periodieke controle op het voldoen aan de gestelde eisen. Deze controles dienen te zijn geregistreerd. Bij onvoldoende controle wordt de Leidinggevende verantwoordelijk gesteld bij het niet conformeren aan de eis zoals gesteld in dit document.
10. Alle incidenten (definitie is bepaald in 13.1.1) worden geregistreerd. Het onbedoeld vernietigen, wijzigen of vrijgeven van persoonsgegevens dienen binnen 24 uur te zijn gemeld aan de AP en waarbij betrokken stakeholders binnen 72 uur dienen te zijn geïnformeerd. De functionaris gegevensbescherming is eindverantwoordelijk voor het uiteindelijk melden van het incident aan zowel de AP als de stakeholders.

15.1.5 Voorkomen van misbruik van IT-voorzieningen

Gebruikers behoren ervan te worden weerhouden IT-voorzieningen te gebruiken voor onbevoegde doeleinden.

De volgende maatregelen zijn genomen om misbruik van IT-voorzieningen te voorkomen:

1. Alle gebruikers van de informatiesystemen dienen een gebruikersovereenkomst te tekenen, waarin de plichten en de rechten van de gebruiker zijn beschreven.
2. Bewustzijn wordt gecreëerd bij de gebruikers onder andere door middel van trainingen.
3. De Eigenaren dienen een "least privilege" beginsel toe te passen (zie paragraaf 11.1.1).
4. Handelingen van de gebruikers worden gelogd en deze logs worden verder gemonitord. Verder zijn de logs alleen in te zien door de Eigenaren, Leidinggevende, Functionaris

gegevensbescherming, RvB en personen die toestemming hebben van de Eigenaar en/of Leidinggevende.

5. Niet naleving wordt gestraft conform paragraaf 8.2.3.

15.1.6 Voorschriften voor het gebruik van cryptografische beheersmaatregelen

Cryptografische beheersmaatregelen behoren overeenkomstig alle relevante overeenkomsten, wetten en voorschriften te worden gebruikt.

De wet stelt dat maatregelen dienen te worden genomen rekening houdend met de stand van de techniek en de kosten van de tenuitvoerlegging, een passend beveiligingsniveau gelet op de risico's die de verwerking en de aard van te beschermen gegevens met zich meebrengen. Het is vanwege de lage kosten van een goedgekeurde certificaat (externe SSL partij) dat we stellen dat er tenminste een goedgekeurde SSL certificaat moet worden gebruikt met een 2048-bit encryptie indien er persoonsgegevens worden verwerkt.

15.2 Naleving van beveiligingsbeleid en -normen en technische naleving

Doelstelling:
Bewerkstelligen dat systemen voldoen aan het beveiligingsbeleid en de beveiligingsnormen van de organisatie.

15.2.1 Naleving van beveiligingsbeleid en –normen

Managers behoren te bewerkstelligen dat alle beveiligingsprocedures die binnen hun verantwoordelijkheid vallen correct worden uitgevoerd om naleving te bereiken van beveiligingsbeleid en -normen.

Periodiek wordt gecontroleerd in hoeverre een deel of de totale organisatie voldoet aan de gestelde eisen conform dit beleid. De verantwoordelijkheden zijn zoals beschreven in paragraaf 15.1.4 lid 9.

15.2.2 Controle op technische naleving

Informatiesystemen behoren regelmatig te worden gecontroleerd op naleving van implementatie van beveiligingsnormen.

1. Tenminste één maal per jaar wordt gekeken in hoeverre de coöperatie voldoet aan het gestelde beleid door middel van een audit.
2. Steekproeven zullen plaatsvinden indien er onzekerheid is over een bepaald systeem dan wel deelorganisatie.

15.3 Overwegingen bij audits van informatiesystemen

Doelstelling:
Doeltreffendheid van audits van het informatiesysteem maximaliseren en verstoring als gevolg van systeemaudits minimaliseren.

15.3.1 Beheersmaatregelen voor audits van informatiesystemen

Eisen voor audits en andere activiteiten waarbij controles worden uitgevoerd op productiesystemen, behoren zorgvuldig te worden gepland en goedgekeurd om het risico van verstoring van bedrijfsprocessen tot een minimum te beperken.

De verantwoordelijke voor het uitvoeren van audits neemt de volgende normen in acht voordat hij of zij de audit tot uitvoering brengt:

1. De auditor brengt de betrokkenen op de hoogte van wat er gaat gebeuren durende de audit.
2. De scope van de audit moet zijn gedefinieerd.

3. De benodigdheden van de audit dienen te zijn vastgesteld, waarbij dit dient te worden opgevolgd en geprepareerd door de desbetreffende Leidinggevenden. Hier vallen tevens gebruikersaccounts van informatiesystemen onder waarbij de auditor alleen rechten krijgt om te lezen. Indien dit niet mogelijk is mag de auditor gebruik maken van een normale account, echter dient na het gebruik het wachtwoord te worden gewijzigd en dient er iemand toezicht te houden op de desbetreffende auditor.
4. De auditor dient een handtekening van de juiste Leidinggevenden te ontvangen voordat hij of zij verder gaat in het auditproces.
5. De auditor mag geen gegevens wijzigen en mag alleen maar de gegevens uitlezen.
6. Om technische werking te controleren, mag de auditor een kopie maken van de data en het informatiesysteem, de kopie en de auditor dient echter te allen tijde onder toezicht te blijven van de Eigenaar van de informatiesysteem. Na de audit dient de auditor de desbetreffende gegevens te verwijderen, de Eigenaar van het informatiesysteem dient dit te controleren.
7. De auditor dient een logboek bij te houden met de acties die hij of zij verricht. Hierin staat vermeld:
    a. Activiteit
    b. Datum / tijd
8. De normen, kaders, procedures, methodes en desbetreffende verantwoordelijken dienen te zijn gedocumenteerd in het audit eindrapport.
9. Na de audit worden alle kopies en gemaakte gebruikersaccount voor de audit geblokkeerd of indien niet mogelijk verwijderd.

15.3.2 Bescherming van hulpmiddelen voor audits van informatiesystemen

Toegang tot hulpmiddelen voor audits van informatiesystemen behoort te worden beschermd om mogelijk misbruik of compromittering te voorkomen.

Audittools die inbreuk kunnen maken op informatiesystemen mogen alleen door interne of met schriftelijke toestemming door externe auditors worden gebruikt. Deze audittools zijn dan ook niet beschikbaar voor andere gebruikers dan de desbetreffende gebruikers die verantwoordelijk zijn voor de audit.

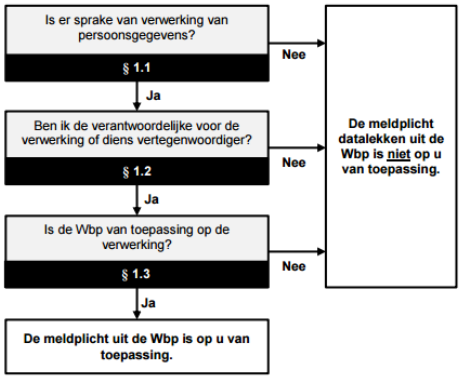
15.4 Melden datalekken

Doelstelling:
Voldoen aan de eisen van de AVG. Daarnaast voldoen aan het gestelde informatiebeveiligingsbeleid.

15.4.1 Registratie van datalekken

Alle datalekken dienen te worden geregistreerd. Op basis van deze registraties wordt er gekeken of iets dient te worden gerapporteerd aan de Autoriteit persoonsgegevens.

Alle datalekken worden centraal geregistreerd en geanalyseerd. Op basis van deze registratie wordt gekeken of de autoriteit persoonsgegevens moet worden gecontacteerd. Het volgende proces moet standaard worden doorlopen.



Afbeelding 3 – melden bij Autoriteit persoonsgegevens.

16. White list van applicaties

Medewerkers van de Coöperatie mogen slechts de volgende applicaties gebruiken om persoonsgegevens te verwerken. Indien een applicatie hier niet bij staat dan mag die niet worden gebruikt en moet er eerst een aanvraag worden ingediend. Deze aanvraag kan worden gedaan bij kwaliteit@dichtbij.coop.

Applicatienaam	**Goedgekeurd voor welke type data**	**Bestandsnaam goedkeuring**	**Goedgekeurd tot datum**
Nedap (https://dichtbij.mijnio.nl/login?jump=https://dichtbij.ioservice.net)	Algemene gegevens, zorggegevens	-	01-01-2019
Ons Dossier App (Via een kantoormedewerker)	Algemene gegevens, zorggegevens	200720118 - Besluit Ons Dossier App.pdf	01-01-2020
Simplicate (https://www.simplicate.nl)	Algemene gegevens	-	01-01-2019
Office 365: - Outlook - Word - Excel - Sharepoint - Access - Visio (https://www.office.com)	Algemene gegevens, zorggegevens	-	01-01-2019
MailChimp (www.mailchimp.com)	Algemene gegevens	-	01-01-2019
Duobus (https://www.duobus.nl	Algemene gegevens, zorggegevens	-	01-01-2019
Mentor (https://duobus.poweredbymentor.nl/)	Algemene gegevens	-	01-01-2019