Informatiebeveiligingsbeleid VGGM

Versie - mei 2020

Versie: 1.4
Auteur: [redacted]
Datum: Mei 2020

1 Documenthistorie

Versiebeheer

Versie	Datum	[redacted]	Opmerkingen
0.1		[redacted]	Eerste concept.
0.2		[redacted]	Reacties verwerkt van collega´s die v0.1 hadden ontvangen.
0.3		[redacted]	Reactie verwerkt van collega's die v0.2 hadden ontvangen.
1.0	Dec 2014	[redacted]	Reacties verwerkt van collega's die v0.3 hadden ontvangen.
1.1	Feb 2019	[redacted]	Herschreven en geactualiseerd.
1.2	Jun 2019	[redacted]	Reacties verwerkt van collega's die v1.1 hadden ontvangen.
1.3	Aug 2019	[redacted]	Aanvulling vanuit directie verwerkt.
1.4	Mei 2020	[redacted]	Aanpassingen in de rollen ivm. reorganisatie Bedrijfsvoering en het van kracht worden van de BIO.

Inhoud

2 Inleiding

Informatie is voor VGGM van strategisch waarde. Een goede beveiliging van die informatie is daarom noodzakelijk voor onze omgeving en voor onszelf. We spreken in dit kader van een hoog afbreukrisico.

Er zijn bovenregionaal afspraken gemaakt over de informatiebeveiliging

- In het 'programma informatievoorziening veiligheidsrisico's 2015 – 2020' dat is vastgesteld in het veiligheidsberaad;
- Binnen Ambulance Zorg Nederland (AZN) is afgesproken om per 1 januari 2018 NEN-7510 gecertificeerd te zijn.

Dit heeft geresulteerd in een informatiebeveiligingsbeleid, waarvan een eerste versie is vastgesteld in december 2015. Dit beleid is in deze versie verder geactualiseerd.

Het beleid vormt de basis voor een analyse van de risico's die we als organisatie lopen en de maatregelen die we moeten treffen. Dit document beschrijft het beleid van VGGM met betrekking tot de beveiliging van informatie.

3 Doel van informatiebeveiliging

Informatiebeveiliging is het geheel van maatregelen, procedures en processen dat zich richt op het blijvend realiseren van een optimaal niveau van beschikbaarheid, integriteit en vertrouwelijkheid van informatie. In dit beleid worden de kaders en uitgangspunten met betrekking tot informatiebeveiliging binnen VGGM vast te stellen.

Het beleidsdocument kent taken, verantwoordelijkheden en bevoegdheden toe aan het management in de rol van verantwoordelijke voor de bedrijfsvoering en als eigenaar van informatiesystemen. Ook worden organisatie overkoepelende zaken met betrekking tot informatiebeveiliging, zoals de technische infrastructuur en de fysieke (toegangs-)beveiliging geregeld.

Informatiebeveiliging richt zich op de volgende drie aspecten van de informatievoorziening en een aspect om de controle te waarborgen. Het totaal wordt ook wel aangeduid als BIV:

- *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.

Met het uitvoeren van het informatiebeveiligingsbeleid, zijn de risico's niet weg en kan een beveiligingsincident ook niet (in alle gevallen) worden voorkomen. Wel kunnen we proberen zoveel mogelijk maatregelen te nemen om risico's te beperken en eventuele beveiligingsincidenten zorgvuldig af te handelen.

Werkingsgebied

Dit informatiebeveiligingsbeleid is van toepassing op alle bedrijfsonderdelen van de Veiligheids- en Gezondheidsregio Gelderland-Midden, Stichting Publieke Gezondheid Gelderland-Midden en Stichting Veilig Thuis Gelderland-Midden. In dit document worden deze drie juridische entiteiten samen VGGM genoemd. Het informatiebeveiligingsbeleid is ook van toepassing op de gegevensuitwisseling van VGGM 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 onze organisatie.

Ambulancezorg Gelderland-Midden is als enige bedrijfsonderdeel gecertificeerd voor NEN 7510:2017. Dit stelt hoge eisen aan de te hanteren normen voor informatieveiligheid. AGM heeft zich ten doel gesteld om blijvend te voldoen aan de norm. De ervaring leert dat men name het bewustzijn over informatie-beveiliging een belangrijke aandachtspunt is en hier wordt dan ook vol op ingezet.

Relatie met andere documenten op het gebied van informatievoorziening

Informatiebeleid: Tijdens het schrijven van dit informatiebeveiligingsbeleid, is het informatiebeleid nog in ontwikkeling. In het informatiebeleid wordt beschreven hoe de informatievoorziening binnen VGGM is georganiseerd.
Continuïteitsplan: Dit plan bevat de kritieke processen/functies die operationeel moeten blijven tijdens een calamiteit. In 2018 is laatste versie van het continuïteitsplan door de directie vastgesteld.
Gegevensbeschermingsbeleid 2020: Dit beleid heeft tot doel de kaders en uitgangspunten met betrekking tot gegevensbescherming binnen VGGM vast te stellen.

4 Uitgangspunten van informatiebeveiliging

Bij de toepassing van informatiebeveiliging, hanteert VGGM verschillende uitgangspunten. De belangrijkste staan hieronder genoemd:
VGGM,

1. streeft ernaar om organisatie breed in ieder geval te voldoen aan de normen volgens de Baseline Informatiebeveiliging Overheid (BIO) en de (uitvoeringswet) AVG;
2. streeft ernaar om de sector Publieke Gezondheid te laten voldoen aan de NEN 7510 normen;
3. heeft de verplichting om haar AGM-organisatie NEN 7510 gecertificeerd te laten zijn.
4. voert een Gegevensbeschermingseffectbeoordeling (GEB/DPIA) uit wanneer er een verhoogd risico wordt verwacht bij het verwerken van persoonsgegevens of wanneer deze GEB conform de eisen van de Autoriteit Persoonsgegevens (AP) uitgevoerd moet worden;
5. ziet de beveiliging van informatie en de bescherming van gegevens als een onderdeel van de integrale managementverantwoordelijkheid;
6. classificeert de bedrijfsprocessen, informatiesystemen en gegevensverzamelingen volgens een gestructureerde methode naar de aspecten beschikbaarheid, integriteit en vertrouwelijkheid;
7. besteedt bij de aanname, tijdens het dienstverband en in geval van ontslag van medewerkers nadrukkelijk aandacht aan de integriteit en betrouwbaarheid van medewerkers en aan de waarborging van de vertrouwelijkheid van informatie;
8. voert een actief beleid om het beveiligingsbewustzijn van management en medewerkers te stimuleren;
9. beschikt over processen, procedures en middelen voor het melden en afhandelen van beveiligingsincidenten en datalekken. De evaluatie van de afhandeling van beveiligingsincidenten wordt benut voor de verbetering van informatiebeveiliging;
10. besteedt bij de ontwikkeling en aanschaf van informatiesystemen nadrukkelijk aandacht aan informatiebeveiliging.

Naleving van wet- en regelgeving

VGGM dient zich te houden aan alle relevante wet- en regelgeving die van toepassing is op het uitvoeren van de dagelijkse werkzaamheden. In het kader van informatiebeveiliging betekent dit dat in ieder geval voldaan wordt aan de Algemene Verordening Gegevensbescherming (AVG), de Uitvoeringswet AVG en de Meldplicht datalekken. Als aanvulling op bovenstaande wettelijke voorschriften zijn ook diverse gedragscodes van toepassing binnen de diverse vakgebieden waarbinnen wordt gewerkt.

5 Beleidsproces voor informatiebeveiliging

Het beleidsproces voor informatiebeveiliging omvat de volgende vier stappen.

Plan (beleid, analyse, planning)

Het proces start met het opstellen van het informatiebeveiligingsbeleid (beschreven in dit document). Als de uitgangspunten helder zijn en het beleid is vastgesteld kan begonnen worden met het in kaart brengen van de risico's. Het doel van deze analyse is:

1. Vaststellen van het huidig en gewenste niveau van informatiebeveiliging.
2. Verkrijgen van inzicht in de reeds geïmplementeerde beveiligingsmaatregelen.

De resultaten van deze fase worden gerapporteerd aan de directeur publieke gezondheid en directeur brandweer. Op basis van de uitkomsten van de analyse wordt een informatiebeveiligingsplan opgesteld.

Do (implementeren en uitvoeren)

Aan de hand van het informatiebeveiligingsplan wordt de implementatie van de aanvullende beveiligingsmaatregelen ter hand genomen. Waar mogelijk gelden de beveiligingsmaatregelen zoveel mogelijk organisatie breed.

Check (controle en evaluatie)

De volgende stap van het beleidsproces voor informatiebeveiliging bestaat uit controle en evaluatie. Het gaat hierbij om

- 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 op het Information Security Management Systeem (door een externe partij).

Act (onderhouden en verbeteren)

Het proces voor informatiebeveiliging is een continu en cyclisch proces. Dit betekent dat op basis van de uitkomst van de controle en evaluaties of door nieuwe ontwikkelingen de noodzaak aanwezig kan zijn om het informatiebeveiligingsbeleid aan te passen of om extra beveiligingsmaatregelen te treffen.

6 Organisatie van informatiebeveiliging

Het is belangrijk om verantwoordelijkheden, taken en bevoegdheden met betrekking tot informatiebeveiliging op een eenduidige wijze te beleggen.

Strategisch, tactisch en operationeel niveau

In het onderstaande overzicht wordt een indeling van activiteiten met betrekking tot informatiebeveiliging beschreven, waarbij het niveau van de activiteiten als onderscheidend criterium is gehanteerd.

Niveau	Activiteit	Verantwoordelijke	Documentatie
Strategisch	Beleidsvorming, en evalueren voor geheel VGGM.	**Directeur Publieke Gezondheid en Directeur Brandweer** ondersteund door afdelingshoofd Mens en Organisatie, afdelingshoofd Informatievoorziening en ICT (I&I), de CISO en evt. de Functionaris Gegevensbescherming	**Informatiebeveiligings-beleid (dit document)** Vastgesteld door directeur publieke gezondheid en directeur brandweer.
Tactisch	Implementatie, evalueren en bijstellen per afdeling	**Afdelingshoofd** ondersteund door afdelingshoofd Mens en Organisatie, afdelingshoofd Informatievoorziening en ICT (I&I), de CISO en de manager ICT	**Informatiebeveiligingsplan** Plan en richtlijnen per sector. Vastgesteld door het DO.
Operationeel	Uitvoering	**Bureauhoofden, teammanager en medewerkers**, ondersteund door de servicemanager en door de aandachtsfunctionaris informatiebeveiliging (per afdeling)	**Operationele procedures**

Generieke rollen voor informatiebeveiliging

Voor ieder informatiesysteem (applicatie) en iedere gegevensverzameling worden de volgende rollen en de bijbehorende verantwoordelijkheden toegewezen.

Rol	Verantwoordelijkheden
Systeemeigenaar	Beslissingsrecht voor het informatiesysteem, c.q. de gegevensverzameling. Denk hierbij aan het verlenen van toegang voor gebruikers en het koppelen met andere informatiesystemen. Bepalen van de beveiligingseisen.
Aandachtsfunctionaris informatiebeveiliging	Ondersteunen van de systeemeigenaar bij het invullen van de specifieke beveiligingsrichtlijnen en –procedures. Ziet toe op een juiste werking van de beveiligingsrichtlijnen en –procedures, c.q. de gegevensverzameling.
Leverancier/ontwikkelaar	Ontwikkelt het informatiesysteem, c.q. de gegevensverzameling, conform de (beveiliging)eisen die door de systeemeigenaar zijn gesteld. Denkt actief mee over de realisatie en de beveiliging van het informatiesysteem, c.q. de gegevensverzameling.
Functioneel beheerder	Ondersteunen van de systeemeigenaar bij het bepalen van de beveiligingseisen. Operationele instandhouding van het informatiesysteem, c.q. de gegevensverzameling. Ziet toe op een juiste werking van het informatiesysteem, c.q. de gegevensverzameling.
Systeembeheerder	Exploitatie van de technische infrastructuur. Ziet toe op een juiste technische werking van de technische infrastructuur.
Systeemgebruiker	Toepassing van het informatiesysteem, c.q. de gegevensverzameling. Naleving van beveiligingsrichtlijnen en –procedures.
Medewerkers	Dienen zich te houden aan het informatiebeveiligingsbeleid en daaruit afgeleide richtlijnen zoals beschreven in: gedragscodes en regels en richtlijnen

De verschillende betrokkenen maken onderling afspraken over de uitvoering van de (beveiliging)taken en leggen deze desgewenst vast in een overeenkomst.

Specifieke rollen en functies voor informatiebeveiliging

Veel onderdelen binnen onze organisatie zijn bij informatiebeveiliging betrokken. In dit informatiebeveiligingsbeleid worden de verantwoordelijkheden van de betreffende functies en rollen beschreven.

Rol	Verantwoordelijkheden
Dagelijks bestuur	Het dagelijks bestuur zal op de hoogte worden gebracht bij grootschalige beveiligingsincidenten en bij datalekken waarbij een hoog risico bestaat voor de betrokkene.
DPG en Directeur brandweer	Eindverantwoordelijke voor de naleving van het gestelde in dit document.
CISO	Heeft inzicht in de risico's en adviseert over de te nemen maatregelen in het kader van informatiebeveiliging om grip te houden op de risico's. De CISO is eigenaar van het informatiebeveiligingsbeleid.
Afdelingshoofd Mens en Organisatie	o.a. Eindverantwoordelijk voor de ondersteunende bedrijfsfuncties zoals: HRM Communicatie, Juridische Zaken, Kwaliteit & IBP en Facilitaire zaken.
Afdelingshoofd Informatievoorziening en ICT (I&I)	Is verantwoordelijk voor de instandhouding van de centrale geautomatiseerde informatievoorziening. En verantwoordelijk voor de ondersteunende bedrijfsfuncties op de onderdelen Informatisering & ICT. Hierin zijn veel raakvlakken met informatiebeveiliging.
Functionaris voor de Gegevensbescherming	Houdt toezicht op de verwerking van persoonsgegevens en daarmee op de toepassing en naleving van de AVG. De functionaris voor de gegevensbescherming (FG) staat in contact met de toezichthoudende instantie, de Autoriteit Persoonsgegevens.
Afdelings-, bureauhoofden en teammanagers	Zijn verantwoordelijk voor de inrichting en uitvoering van de primaire en secundaire bedrijfsprocessen.
Architect	Verantwoordelijk voor het borgen van de uitgangspunten van informatiebeveiliging bij het ontwerp van informatiesystemen.
Informatieadviseur	Verantwoordelijk voor het borgen van de eisen en maatregelen van informatiebeveiliging zonder dat dit een goed gebruik van het informatiesysteem in de weg staat.
Manager ICT	Verantwoordelijk voor het proces kwaliteitsbeheer binnen team ICT waarin alle ICT-gerelateerde risico's worden geïnventariseerd en beoordeeld.
Beleidsmedewerker kwaliteit	Verantwoordelijk voor het beheer van het integrale managementsysteem en het coördineren van kwaliteitsaudits.
Aandachtsfunctionaris informatiebeveiliging	Verantwoordelijk voor het operationeel ten uitvoer brengen van het informatiebeveiligingsbeleid.
Systeembeheerders met aandachtsgebied *Security*	Systeembeheerders binnen het team ICT welke in het dagelijks beheer aandacht hebben voor technische informatiebeveiligingsaspecten.

Overlegstructuren

Om periodiek opvolging te geven aan het thema informatiebeveiliging zijn er verschillende overlegstructuren in plaats:

- *Risicobeheeroverleg:* periodiek overleg waarin de informatiebeveiligingsrisico's en cyberdreigingen besproken worden door stakeholders vanuit de afdeling I&I en de CISO.
- *Informatiebeveiligingsoverleg:* sectoraal overleg waarin de onderwerpen uit de normenkaders (NEN/BIO) thematisch vorm krijgen. Er is hierbij aandacht voor actuele onderwerpen en mogelijke informatiebeveiligingsrisico's.
- *Afdelingsoverleg:* de aandachtsfunctionaris informatiebeveiliging zorgt voor de aansluiting/borging van het onderwerp informatiebeveiliging naar de eigen afdeling en/of team.

7 Veilig personeel

Bij het aannemen of inhuren van nieuw personeel en het laten verrichten van werkzaamheden door (externe) medewerkers wordt bewerkstelligd dat zij hun verantwoordelijkheden begrijpen ten aanzien van informatieveiligheid. Deze verantwoordelijkheden zijn door VGGM vóór het dienstverband vastgelegd in een passende functiebeschrijvingen of opdracht en in de

arbeidsvoorwaarde danwel inhuurovereenkomst. Daar waar nodig wordt een Verklaring Omtrent Gedrag (VOG) gevraagd. Alle medewerkers zijn op de hoogte van de gedragscode integriteit. Daarnaast wordt er door VGGM veel aandacht gegeven aan het versterken van het informatieveiligheidsbewustzijn door met een gerichte campagne aandacht te vragen voor dit onderwerp. Risicobewustzijn van alle medewerkers van VGGM is de sleutel tot een effectieve informatiebeveiliging. Risicobewustzijn wordt volledig ondersteund door de directie en de afdelingshoofden van VGGM en zal gestimuleerd worden door middel van bewustwordingssessies en publicaties via onder meer posters, het intranet en andere nieuwsbrieven.

8 Beheer van bedrijfsmiddelen

IT middelen die aan medewerkers van VGGM beschikbaar worden gesteld, dienen in principe voor zakelijke doeleinden gebruikt te worden. Gebruik voor privé-doeleinden is echter ook toegestaan. Voor een effectieve bescherming van de informatie is vereist dat de waarde van de informatie voor de interne organisatie bekend is.
Met de invoering van de BIO is het basis beveiligingsniveau bepaald dat geldt voor de gehele bedrijfsvoering van VGGM. De processen en systemen waarvan verwacht wordt dat deze meer beveiligingsmaatregelen nodig hebben dan de Baseline worden verder onderzocht. Met een classificatiemethode kan bepaald worden of proces, gegevensverzameling of applicatie binnen of buiten baseline valt. De systeemeigenaar classificeert in samenspraak met de CISO de gegevens die worden verwerkt en stelt op basis hiervan vast welke beveiligingsmaatregelen vereist zijn.

Niveau	Beschikbaarheid	Integriteit	Vertrouwelijkheid
Geen	**0 - Niet zeker** Gegevens kunnen zonder gevolgen langere tijd niet beschikbaar zijn (bijv. ondersteunende tools als Goodhabitz)	**0 - Niet zeker** Informatie mag worden veranderd (bijv. templates en sjablonen)	**0 - Openbaar** Informatie mag door iedereen worden ingezien (bijv: algemene informatie op de externe website)
Laag	**1 - Laag (BBN1)** Informatie mag incidenteel niet beschikbaar zijn (bijv. administratieve gegevens)	**1 - Laag (BBN1)** Het bedrijfsproces staat enkele (integriteits-) fouten toe (bijv. rapportages)	**1 - Bedrijfsvertrouwelijk (BBN1)** Informatie is toegankelijk voor alle medewerkers van de organisatie (bijv. informatie op het intranet)
Midden	**2 - Midden (BBN2)** Informatie moet vrijwel altijd beschikbaar zijn, continuïteit is belangrijk (bijv. primaire proces informatie)	**2 - Midden (BBN2)** Het bedrijfsproces staat zeer weinig fouten toe (bijv. informatie over de bedrijfsvoering)	**2 - Geheim (BBN2)** Informatie is alleen toegankelijk voor een beperkte groep gebruikers (bijv. persoonsgegevens, financiële gegevens)
Hoog	**3 - Hoog (BBN2 + aanvullend)** Informatie mag alleen in uitzonderlijke situaties uitvallen, bijvoorbeeld bij calamiteiten (bijv. LCMS)	**3 - Hoog (BBN2 + aanvullend)** Het bedrijfsproces staat geen fouten toe (bijv. informatie op de externe website)	**3 - Geheim, statelijke actoren (BBN3)** Informatie is alleen toegankelijk voor direct geadresseerden (bijv. medisch dossier)

9 Toegangsbeveiliging

Toegang tot informatie en IT-faciliteiten zal op basis van 'need to know' worden beperkt zodat gebruikers toegang krijgen tot datgene wat noodzakelijk is voor het uitvoeren van de functie (privacy by default). Dit voorgaande geldt natuurlijk niet voor hetgeen de organisatie als informatief voor alle medewerkers noodzakelijk acht en waarvoor transparantie gewenst is.
Fysieke toegang tot de gebouwen van VGGM is alleen mogelijk met de daartoe verstrekte persoonlijke toegangsbadges.

Gegevens op papier worden beschermd door een deugdelijke opslag en regeling voor de toegang tot archiefruimten. Documenten, opslagmedia, in- en uitvoergegevens en systeemdocumentatie worden beschermd tegen onbevoegde openbaarmaking, wijziging, verwijdering en vernietiging.

10 Cryptografie

VGGM zorgt voor correct en doeltreffend gebruik van cryptografische maatregelen om de vertrouwelijkheid, authenticiteit en/of integriteit van informatie te beschermen. De in gebruik zijnde bedrijfsmiddelen worden voorzien van cryptografische maatregelen. Informatie, welke verzonden wordt, dient met behulp van cryptografische middelen te worden verstuurd. Informatie wordt verzonden middels een versleutelde verbinding.

11 Fysieke beveiliging en beveiliging van de omgeving

VGGM heeft IT-voorzieningen geïmplementeerd voor de eigen bedrijfsonderdelen en locaties die onderlinge interne communicatie en samenwerking met partners, patiënten, cliënten en medewerkers (op afstand) mogelijk maakt. Deze IT-voorzieningen zijn deels in beheer en eigendom van VGGM en deels uitbesteed. De beveiliging moet periodiek worden getoetst waarbij aangetoond wordt dat voldaan wordt aan de afgesproken informatiebeveiligingseisen.
Ook aan de verbinding naar de cloud worden hoge eisen gesteld die getoetst moeten worden.
Voor bepaalde diensten wordt gebruik gemaakt van externe publieke netwerken zoals het internet. Hiervoor zijn beveiligingsmaatregelen en beheersmaatregelen geïmplementeerd om de beschikbaarheid, integriteit en vertrouwelijkheid te waarborgen.

12 Beveiliging bedrijfsvoering

VGGM heeft maatregelen genomen om een correcte en veilige bediening van informatieverwerkende faciliteiten te waarborgen. Informatie en informatieverwerkende faciliteiten worden beschermd tegen malware en virussen en er worden maatregelen genomen om bescherming te bieden tegen het verlies van gegevens.
Gebeurtenissen worden waar mogelijk vastgelegd in een logbestand zodat achteraf inzicht verkregen kan worden in de uitgevoerd acties. Er is een beleid voor patch- en releasemanagement. ICT maakt reservekopieën van essentiële bedrijfsgegevens en programmatuur zodat de continuïteit van proces en gegevensverwerking kan worden gegarandeerd. Jaarlijks wordt door proces- of systeemeigenaar een (back-up en) restoretest geïnitieerd.

13 Communicatiebeveiliging

De bescherming van informatie in netwerken en de ondersteunende informatie verwerkende faciliteiten is gewaarborgd. De uitwisseling van informatie binnen de eigen organisatie en met externe entiteiten is daarom altijd beveiligd.

14 Acquisitie, ontwikkeling en onderhoud van informatiesystemen

Om te bewerkstelligen dat beveiliging integraal deel uitmaakt van informatiesystemen behoren in bedrijfseisen voor nieuwe informatiesystemen of uitbreidingen van bestaande informatiesystemen ook eisen voor beveiligingsmaatregelen te worden opgenomen.
De implementatie van wijzigingen behoort te worden beheerst door middel van formele procedures voor wijzigingsbeheer. 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
Er behoort tijdig informatie te worden verkregen over technische kwetsbaarheden van de gebruikte informatiesystemen. De mate waarin de organisatie bloot staat aan dergelijke kwetsbaarheden behoort te worden geëvalueerd en er behoren geschikte maatregelen te worden genomen voor behandeling van daarmee samenhangende risico's.

15 Leveranciersrelaties

De bedrijfsmiddelen van VGGM die toegankelijk zijn voor leveranciers zijn beschermd. Daarbij wordt erop toegezien dat het overeengekomen niveau van informatiebeveiliging en dienstverlening in overeenstemming is met de leveranciersovereenkomsten. Een SLA en verwerkersovereenkomst kunnen hier onderdeel van uitmaken. Jaarlijks vinden er leveranciersgesprekken plaats met de kritische leveranciers waarbij informatiebeveiliging een vast punt op de agenda is.

16 Beheer van informatiebeveiligingsincidenten

Het is van belang dat incidenten op het gebied van de informatiebeveiliging gemeld worden. Bij melding kan er adequaat gereageerd worden en kan de organisatie vergelijkbare incidenten in de toekomst vermijden door te leren van eerdere incidenten. Ook kan bekeken worden of de reeds gekozen beveiligingsmaatregelen aanpassingen behoeven. Om deze redenen dienen alle medewerkers bij het ontdekken of vermoeden van een beveiligingsincident dit onmiddellijk te melden bij de Servicedesk ICT.
In het geval van een datalek, kan er sprake zijn van een meldingsplichtig datalek. In dat geval zal een melding gemaakt worden bij de Autoriteit Persoonsgegevens. De Functionaris Gegevensbescherming treedt op als contactpersoon. We spreken van een datalek als persoonsgegevens in handen vallen van derden die geen toegang tot die gegevens zouden mogen hebben. Ook is er sprake van een datalek wanneer persoonsgegevens verloren zijn geraakt en er geen back-up is. Een datalek is het gevolg van een beveiligingsprobleem. Bij (het vermoeden van) een datalek moet er onmiddellijk melding gemaakt worden bij de Servicedesk ICT. Indien er sprake is van een grootschalig beveiligingsincident, kan het voorkomen dat er een incident responsteam (IRT) gevormd wordt.

17 Informatiebeveiligingsaspecten van bedrijfscontinuïteit

Er zijn voor de belangrijkste processen en systemen continuïteits- en uitwijkplannen beschikbaar. Er worden minimaal jaarlijks oefeningen of testen gehouden om de continuïteitsplannen te toetsen (opzet, bestaan en werking). Aan de hand van de resultaten worden de plannen bijgesteld en wordt de organisatie bijgeschoold.

18 Naleving

Het verbeteren van de kwaliteit van informatieveiligheid is een continu proces en onderdeel van alle processen van VGGM waarin wordt gewerkt met gevoelige informatie. Informatieveiligheid is een kwaliteitskenmerk van het primaire proces, waarop het management van elke afdeling stuurt. Naleving van het beleid wordt gecontroleerd. Niet naleven van het beleid kan disciplinaire maatregelen tot gevolg hebben. Jaarlijks worden er risicoanalyses uitgevoerd, zijn er diverse audits (intern en extern), bewustwordingssessies, collegiale toetsing, pentesten, vulnerability scans, mystery guest en/of eventuele andere acties. Deze acties zorgen ervoor dat het beleid wordt gecontroleerd op zijn toepasbaarheid, volledigheid en werking. Specifieke of afwijkende afdelingsdoelen, worden per afdeling vastgelegd in de managementreview/directiebeoordeling.

Borging vindt plaats door middel van vastlegging van de overeengekomen werkwijze. Dit kan via een of meer van de volgende vormen van vastlegging: procesbeschrijvingen, richtlijnen, gedragscode, procedures, werkinstructies of tooling. Deze informatie dient voor alle relevante medewerkers toegankelijk te zijn. Het ISMS waarborgt door periodieke toetsing op actualisatie en naleving van de overeengekomen werkwijze.