2023

Informatiebeveiligingsbeleid

Veiligheidsregio Flevoland
Veiligheidsregio Gooi en Vechtstreek

Versiebeheer

Versienr.	Datum	Auteur(s)	Status	Opmerking
0.5	22-11-2021	Michel Springer	Concept	Eerste opzet
0.7	30-11-2021	Michel Springer	Concept	Op- en Aanmerkingen verwerkt van Yara en Arold
0.9	12-01-2022	Michel Springer	Concept	Op- en Aanmerkingen verwerkt van Marc van de Geer, Arold, Richard Schreuder en Martin van Loveren
0.91	03-03-2022	Michel Springer	Concept	Aanvullingen Richard Schreuder, Chris Rolandus, Chiel de Nennie en Martin van Loveren
0.92	22-04-2022	Yara van der Laan	Concept	Hoofdstuk 3 verwijzing naar document Rollen en Verantwoordelijkheden IB.
0.93	09-05-2022	Arold Sonke	Concept	Redactionele verbeteringen
0.94	11-05-2022	Arold Sonke	Concept	Aanpassingen n.a.v. projectoverleg.
0.95	26-07-2022	Martin van Loveren, Jasper Zweers en Yara van der Laan	Concept	Interne review, inhoudelijke en redactionele aanpassingen
0.96	12-09-2022	Jasper Zweers, Arold Sonke	Concept	Verwerken reviews, aanvulling uitwerking IB Beleid.
1.0	18-10-2022	Martin van Loveren, Arold Sonke	Concept	Aanpassingen door Martin en n.a.v. bespreking projectoverleg. Versie voorgelegd aan het GMT ter meningsvorming.
1.1	01-11-2022	Arold Sonke	Concept	Commentaar GMT i.s.m. het projectoverleg verwerkt.
1.2	28-11-2022	Jasper Zweers	Concept	Versie na aanbieding document als ‘voorgenomen besluit’ aan de Veiligheidsdirectie.
1.22	09-12-2022	Arold Sonke	Concept	Privacy vervangen door persoonsgegevens
1.30	24-05-2023	Jasper Zweers	Concept	Tekstuele wijzigingen n.a.v. commentaar dagelijks bestuur.

Autorisatie

Door	Datum	
GMT	25 oktober 2022	Meningsvormend
Veiligheidsdirectie	16 november 2022	Meningsvormend
OR		Advisering / Instemming
Algemeen Bestuur		Besluitvormend

Classificatie en herzieningsdatum

Dit document is alleen voor intern gebruik binnen de Veiligheidsregio Gooi en Vechtstreek en de Veiligheidsregio Flevoland.

Het document heeft een geldigheidsduur van 5 jaar vanaf het moment van definitief vaststellen.

Inhoudsopgave

1 Inleiding

Het voorliggende informatiebeveiligingsbeleid is een invulling van de Baseline Informatiebeveiliging Overheid (BIO). Het beleid biedt kaders voor het organiseren van de beveiliging en zorgt ervoor dat we wendbaar blijven om op basis van de beleidsuitgangspunten in te spelen op de actuele maatschappelijke ontwikkelingen. Daarnaast sluit het aan bij het versnellingsplan informatiebeveiliging van het NIPV (voorheen IFV) om te komen tot het borgen van het vereiste basisniveau voor informatiebeveiliging in alle 25 veiligheidsregio's en bij het NIPV.

De scope van het informatieveiligheidsbeleid omvat de bedrijfsonderdelen van de Veiligheidsregio Gooi en Vechtstreek en de Veiligheidsregio Flevoland. Daarbij gaat het in eerste instantie om de onderdelen Brandweerzorg, Bedrijfsvoering, Veiligheidsbureau, Bevolkingszorg, Meldkamer Brandweer, O&HR en overige onderdelen die conform de Wet op de veiligheidsregio en de Gemeenschappelijke Regeling onder de verantwoordelijkheid van de veiligheidsregio vallen.
De GHOR valt conform de Gemeenschappelijke Regeling onder de veiligheidsregio. Daarmee is het informatiebeveiligingsbeleid van toepassing voor de GHOR. Echter qua uitvoering zijn de 'beheerswerkzaamheden' t.b.v. de GHOR ondergebracht bij de GGD. De GGD hanteert de normering van ISO 27001 en NEN-7510. Daarmee is het informatiebeveiligingsbeleid van de GGD gelijkwaardig aan het beleid van de samenwerkende Veiligheidsregio Flevoland en Veiligheidsregio Gooi en Vechtstreek en ook van toepassing op de GHOR.

In het verlengde daarvan geldt hetzelfde voor de bestuurders van de veiligheidsregio's.
Alhoewel zij een wettelijke verantwoordelijkheid hebben conform de Wet op de veiligheidsregio zijn zij door de Kroon benoemd als burgermeester van de (aangesloten) gemeenten. Ook de gemeenten moeten voldoen aan de BIO. Daarmee is het informatiebeveiligingsbeleid van de gemeenten van toepassing voor de bestuurders.

In de ketenverantwoordelijkheid werken Politie, GGD, Defensie, Waterschap enz. intensief samen met de veiligheidsregio's, maar ook zij hebben hun eigen verantwoordelijkheid ten aanzien van informatiebeveiliging. Daar waar het de samenwerking raakt met of via de (technische) systemen van de veiligheidsregio wordt van hen verwacht zich te houden aan het beleid van de veiligheidsregio voor zo ver dat niet in gedrang komt met hun eigen stringentere beveiligingsnormeringen.

1.1 Achtergrond

We leven in een kennismaatschappij, waarin informatie- en communicatietechnologie een belangrijke rol speelt in het delen van informatie.
Informatie is niet alleen cruciaal voor onze kantooromgeving, maar ook voor de operationele incidentbestrijding en crisisbeheersing zoals op voertuigen, in de crisisruimtes en meldkamer.

Veiligheidsregio Flevoland en Veiligheidsregio Gooi en Vechtstreek lopen een reëel risico op (im)materiële schade door verstoring van de informatie- en communicatietechnologie van de organisatie (of van één van de ketenpartners), waardoor onze interne organisatie dan wel onze hulpverleningstaken in gevaar komen.

Dit kan door zowel gerichte criminele activiteiten, zoals een cyberaanval, zoals bij de VNOG en Hof van Twente is gebleken, maar kunnen ook door andere oorzaken worden veroorzaakt.

1.2 Visie op informatiebeveiliging

In het belang van de burgers, de bedrijven, de overheid, de crisispartners en de eigen organisatie zien de Veiligheidsregio Gooi en Vechtstreek en de Veiligheidsregio Flevoland informatie als één van de kritische bedrijfsmiddelen om de ambitie van de organisatie te realiseren.
Het optimaal functioneren van de informatie- en communicatietechnologie is noodzakelijk voor het goed coördineren en samenwerken bij het voorkomen en bestrijden van crises met een mono- of multidisciplinaire aanpak. Ook is betrouwbare informatie noodzakelijk bij de ondersteunende, versterkende processen, die leiden tot onder andere aannemen en trainen van medewerkers en autoriseren van medewerkers voor informatiesystemen en fysieke ruimten. De noodzakelijke beschikbaarheid, integriteit en vertrouwelijkheid van de informatie in al haar vormen is vastgelegd en leidend voor uitvoeren van een samenhangend stelsel aan organisatorische en technische risico beheersende maatregelen.
We organiseren een continu regieproces om blijvend een optimale betrouwbaarheid van de informatie in al haar vormen te realiseren. Hiervoor stellen we normen op en we nemen maatregelen op basis van de risico's. We beperken de financiële en personele consequenties van de in het beleid vertaalde wet- en regelgeving door het zo goed mogelijk bieden van oplossingen, opdat medewerkers hun werkzaamheden kunnen uitvoeren. Het veilig omgaan met informatie verankeren we in de bedrijfsprocessen van de organisatie en dit komt tot uiting in onze organisatiecultuur. Dit betekent dat we betrouwbare informatie met de juiste personen via het juiste middel voor het juiste doel delen. Ook mogen we elkaar aanspreken om onjuist handelen te voorkomen.

Informatie

Informatie is één van de kritieke bedrijfsmiddelen om de ambitie van de organisatie te realiseren. Het optimaal functioneren van de informatie- en communicatietechnologie is noodzakelijk voor het goed coördineren en samenwerken bij het voorkomen en bestrijden van crises met een mono- of multidisciplinaire aanpak.

Borging

We organiseren een continu regieproces om blijvend een optimale informatievoorziening in al haar vormen te realiseren. Hiervoor stellen we normen op en we nemen maatregelen op basis van de risico's. Het veilig omgaan met informatie verankeren we in de bedrijfsprocessen van de organisatie.

BIV

De noodzakelijke beschikbaarheid, integriteit en vertrouwelijkheid van de informatie in al haar vormen is vastgelegd en leidend voor uitvoeren van een samenhangend stelsel aan organisatorische en technische risicobeheersende maatregelen

1.3 Doel

Het doel van het informatiebeveiligingsbeleid is de kaders en voorwaarden te scheppen om de risico's te beheersen en accepteren t.a.v. de informatievoorziening. De beschikbaarheid, integriteit en vertrouwelijkheid van digitale en niet-digitale informatie dient te worden geoptimaliseerd en te worden geborgd in de bedrijfsprocessen van de organisatie. Daarnaast dient de (cyber)weerbaarheid bij een informatiebeveiligingsincident te worden vergroot. De belangrijkste voorwaarden om hieraan te kunnen voldoen, zijn voldoende bewustzijn van de medewerkers over veilig omgaan met informatie en management commitment.

1.4 Reikwijdte

Het informatiebeveiligingsbeleid heeft betrekking op de veiligheidsregio Flevoland en de veiligheidsregio Gooi en Vechtstreek en alle vormen van informatie, alle mogelijke informatiedragers en alle informatie- en netwerksystemen. In onze risicobeheersing prioriteren we organisatorische en technische beheersmaatregelen op basis van risico's (kans x impact). Het beleid richt zich op medewerkers welke in dienst zijn of een overeenkomst hebben met de Veiligheidsregio Gooi en Vechtstreek en de Veiligheidsregio Flevoland.

1.5 Periodieke herziening / evaluatie

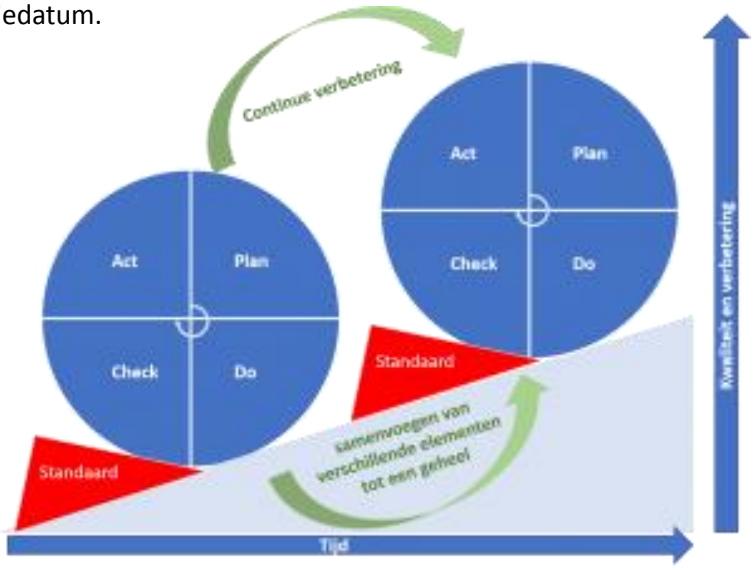
Het informatiebeveiligingsbeleid wordt ieder jaar als onderdeel van de directiebeoordeling geëvalueerd en zo nodig aangepast. Minimaal eenmaal per drie jaar wordt het beleid geactualiseerd.

2 Stappen van informatiebeveiliging, inrichting ISMS

Een ISMS is een informatiebeveiligingsbeheersystemen en een belangrijk managementinstrument om veiligheidsrisico's in kaart te brengen en te beheersen. Beleid, taken en verantwoordelijkheden, normenkaders, beheersmaatregelen en inzicht in risico's komen in dit systeem bijeen.

Om het management systeem van informatiebeveiliging (ISMS) te borgen zal een plan-do-check-act cyclus worden gehanteerd, waarmee stelselmatig aan continue verbetering wordt gewerkt. Het ISMS is een kwaliteitszorgsysteem dat gebaseerd wordt op ISO 27001.

- In de plan-fase wordt besloten welke verbeteringen van informatiebeveiliging in de komende cyclus worden meegenomen. De gekozen verbeteringen worden concreet gemaakt en aan een verantwoordelijke toegewezen, samen met een oplosrichting, benodigd budget en realisatiedatum.



- In de do-fase ontwerpt elke aangewezen verantwoordelijke de oplossing voor de verbetering en implementeert deze. Daarbij moet de business-as-usual gewoon zonder verstoring doorlopen.
- In de check-fase worden de resultaten van de verbetering gemeten, om te beoordelen of de beoogde effecten ook worden bereikt. Elke afwijking wordt geanalyseerd op oorzaken, zodat er effectief gereageerd kan worden. De oorzaken van de afwijking zijn namelijk bepalend voor de wijze waarop bijgestuurd moet worden.
- In de act-fase worden op basis van de analyses uit de check-fase maatregelen bepaald en doorgevoerd, om binnen de lopende plan-do-check-act cyclus de effecten te verbeteren. Verantwoordelijk hiervoor zijn de personen die in de planfase zijn aangewezen om de verbeteringen te realiseren.

Als uit analyse blijkt dat beoogde doelen niet behaald kunnen worden omdat de oplossingsrichting, het budget of de streefdatum niet realistisch blijken, dan wordt geëscaleerd naar de Veiligheidsdirectie. De Veiligheidsdirectie besluit dan of de plan-fase per direct bijgesteld moet worden, of dat gewacht kan worden op de plan-fase in de volgende cyclus.

De plan-do-check-act activiteiten voor de informatiebeveiliging worden binnen de Veiligheidsregio Gooi en Vechtstreek en de Veiligheidsregio Flevoland geïntegreerd in het kwaliteitszorgsysteem.

2.1 Bewustwording

Vanuit de BIO/ISO27001 wordt verwacht dat organisaties voldoende middelen bieden om medewerkers bewust te maken van het belang van informatiebeveiliging. Door middel van opleiden en periodiek bijscholen moet het informatiebeveiliging bewustzijnsniveau van de Veiligheidsregio Gooi en Vechtstreek en de Veiligheidsregio Flevoland op peil blijven. Beveiligingsbewustzijn gaat voor een groot deel over de bedrijfscultuur binnen de organisaties. Er kunnen namelijk voldoende technische en organisatorische maatregelen zijn geïmplementeerd om informatiebeveiligingsrisico's te beheersen, maar de medewerkers moeten wel correct omgaan met deze maatregelen. Binnen de organisatie moet duidelijk worden dat informatiebeveiliging geen ICT-feestje is, maar dat juist iedereen individueel verantwoordelijk is voor de informatierisico's die zij mede veroorzaken. Hierdoor is het stuk bewustwording uit de BIO/ISO27001 één van de belangrijkste aspecten die de Veiligheidsregio Gooi en Vechtstreek en de Veiligheidsregio Flevoland goed ingeregeld moeten hebben.

2.2 Risicobeheer

Beveiligen gebeurt met een duidelijk beeld voor ogen van de waarde van datgene dat beveiligd wordt. Hoe meer waarde iets heeft voor de organisatie, des te beter moet de bescherming zijn. Dit uitgangspunt is leidend bij het nemen van maatregelen.

2.2.1 Risico analyse

Een belangrijk onderdeel van het managementsysteem voor informatiebeveiliging bestaat uit een risicoanalyse van de bestaande situatie. Het analyseren van de risico's heeft tot doel:

Figuur 1: Bewuste risicoacceptatie

- Inzicht te krijgen in de risico's die de realisatie van het gewenste beveiligingsniveau in gevaar kunnen brengen.
- Keuzes te kunnen maken voor het beheersen van risico's.
- Prioriteiten te bepalen voor de verbetering van de bestaande situatie.
- Het prioriteren van het monitoren van de effectiviteit van de getroffen maatregelen.

De risicoanalyse wordt, in beginsel, elke drie jaar herhaald, of tussentijds in het geval van substantiële wijzigingen.

2.2.2 Classificatie van informatie

Volgens de BIO moet informatie verwerkt door de veiligheidsregio's worden geclassificeerd. Classificatie van informatie is gebaseerd op het criteria vertrouwelijkheid, één van de componenten van de BIV-classificatie. Hiermee kan worden bepaald welke beheersmaatregelen nodig zijn. De te nemen maatregelen moeten worden afgestemd op de risico's, waarbij rekening dient te worden gehouden met technische mogelijkheden en de kosten van maatregelen. Dit is vaak situatie afhankelijk. Naarmate de gegevens een gevoeliger karakter hebben, of gezien de context waarin ze gebruikt worden een groter risico inhouden, dienen zwaardere eisen te worden gesteld aan de beveiliging van die gegevens. Kort gezegd: risico's en tegenmaatregelen dienen in balans te zijn. De basis voor de bescherming van persoonsinformatie is dat alle informatie over medewerkers en andere personen alleen wordt verwerkt in de daarvoor toegewezen systemen, zoals bv het personeelsinformatiesysteem. In bijlage II is de classificatie van informatie verder uitgewerkt.

2.2.3 Continuïteit

Informatiebeveiliging heeft als doel om risico's met betrekking tot informatiebeveiligingsincidenten te reduceren tot een, door het dagelijks bestuur vastgesteld, acceptabel niveau. Ondanks goede beheersmaatregelen kan een incident zich voordoen.
Voor kritieke ICT-diensten en informatiesystemen is een continuïteitsplan aanwezig. Hierin is opgenomen hoe de getroffen ICT-dienst of het getroffen informatiesysteem in geval van calamiteiten weer operationeel gemaakt kan worden. Een continuïteitsplan kan variëren van een goede back-upvoorziening of het geografisch spreiden van de ICT-dienst tot een complete uitwijklocatie. Continuïteitsplannen worden minimaal één keer per jaar op actualiteit geëvalueerd.

3 Randvoorwaarden informatiebeveiliging

3.1 Informatiebeveiligingsbeleid

1. Het Veiligheidsberaad heeft de gehele Baseline Informatiebeveiliging Overheid (BIO) van toepassing verklaard voor de veiligheidsregio's. De BIO is het uitgangspunt voor de door de veiligheidsregio's te treffen beheersmaatregelen.
2. Het beleid wordt conform BIO (en daarmee ISO27001/2) opgesteld en de onderliggende procedures en uitwerkingen worden in lijn met het beleid en de normen uit de BIO opgesteld.
3. Het informatiebeveiligingsbeleid mag niet belemmerend zijn voor de transparante manier van werken en het gebruikersgemak, daartoe:
    a. wordt ruimte gegeven voor de afweging en de prioritering van risico beheersende maatregelen op basis van het principe 'pas toe of leg uit'.
    b. wordt informatiebeveiliging als een continu integraal verbeterproces benaderd.
    c. kan aan het bestrijden van een crises of incident een hogere prioriteit worden gegeven dan aan bescherming van persoonsgegevens en security, mits noodzakelijk, onderbouwd en passend binnen de kaders van de wet.
4. De risico's worden geclassificeerd op basis van de kans en impact. De risicoclassificatie is leidend voor de prioriteit van het nemen van beheersmaatregelen van organisatorische en/of technische aard.

3.2 Organisatorisch

1. De Veiligheidsdirectie bied het informatiebeveiligingsbeleid voor vaststelling aan de besturen aan, waarbij de voorzitter van de Veiligheidsdirectie de opdrachtgever van het informatiebeveiligingsbeleid is. De plaatsvervangend directeur bedrijfsvoering (tevens Chief Information Officer) is de opdrachtnemer (en zorgt voor uitvoering en verantwoording richting de Veiligheidsdirectie) van het informatiebeveiligingsbeleid. De directie bedrijfsvoering bespreekt jaarlijkse herijking van het beleid en de daarbij behorende uitwerkingen.
2. De basis van informatiebeveiliging moet worden verankerd in de bedrijfsprocessen, waarbij de organisatie ervan uitgaat dat medewerkers, ketenpartners en anderen afspraken nakomen in relatie tot beschikbaarheid, integriteit en vertrouwelijkheid van de informatievoorziening.
3. In de reguliere (team)overleggen dient informatiebeveiliging een terugkerend agendapunt te zijn. Hierdoor stelt de organisatie zichzelf in staat om te kunnen sturen op prioriteitstelling van risico's en uitvoeren van reducerende maatregelen. Het lijnmanagement is verantwoordelijk voor de uitvoering van informatiebeveiliging in de eigen lijn
4. De voorzitter van de Veiligheidsdirectie voert een actief beleid om het beveiligingsbewustzijn van management en medewerkers te stimuleren. Hiertoe stelt de Chief Information Officer (CIO), in samenwerking met de teamleider I&A en FG, een bewustwordingsprogramma op en werkt dit samen met betrokken afdelingen uit in een activiteitenkalender.
5. De veiligheidsregio's beschikken over gedragsregels voor het gebruik van digitale werkomgeving. Deze zijn uitgewerkt in de 'gedragscode voor gebruikers van de digitale werkomgeving'. Op de naleving van deze gedragsregels wordt toegezien.
6. Bij overtreding van de regelgeving voor informatiebeveiliging en/of relevante wettelijke bepalingen kan een sanctie wordt opleggen conform wat hierover met betrekking tot op

non-actiefstelling, disciplinaire straffen, en beëindiging van het dienstverband is vastgelegd in de CAR-UWO.

7. Rollen en verantwoordelijkheden met betrekking tot informatiebeveiliging zijn uitgewerkt in het document 'rollen en verantwoordelijkheden IB'. De beschrijvingen zijn opgesteld aan de hand van een afgestemde RACI-matrix die tevens te vinden is in het hierboven genoemde document.

3.3 Persoonsgegevens

1. Verwerking van persoonsgegevens is aantoonbaar gebonden aan een duidelijke doel.
2. Bij de selectie, aanschaf en implementatie van informatiesystemen waarin persoonsgegevens worden verwerkt, wordt het principe van *privacy by design* en *dataminimalisatie* toegepast.
3. Het verwerken van persoonsgegevens en bijzondere persoonsgegevens, zoals bijvoorbeeld gegevens die inzicht gegeven in iemands ras, geloof, gezondheid, seksuele voorkeur of geaardheid, lid van een vakbond, genetische of biometrische gegevens is slechts toegestaan als daarvoor een grondslag is.
4. Bij verwerking van persoonsgegevens wordt toegang tot deze gegevens beperkt tot degenen die hiervoor formeel bevoegd zijn.
5. De veiligheidsregio's dragen zorgvuldige omgang met persoonsgegevens uit, zowel binnen als buiten de organisatie, door een privacy statement dat op de publieke website raadpleegbaar is.

4 Uitgangspunten informatiebeveiliging

Onderstaande uitgangspunten geven richting bij het inrichtingen of wijzigingen die effect hebben op de informatiebeveiliging. In het document 'Uitwerkingen van het informatiebeveiligingsbeleid' wordt nadere invulling gegeven aan het informatiebeveiligingsbeleid en de te treffen beheersmaatregelen.

4.1 Informatiebeveiliging is verantwoordelijkheid van iedereen

Kernaspecten van informatiebeveiliging zijn Beschikbaarheid, Integriteit en Vertrouwelijkheid (BIV). Het niveau van informatiebeveiliging van de Veiligheidsregio Gooi en Vechtstreek en de Veiligheidsregio Flevoland vraagt nu specifieke aandacht gezien externe ontwikkelingen (zoals hacks die plaatsvinden bij andere veiligheidsregio's), de inzet van vrijwilligers binnen de Veiligheidsregio Gooi en Vechtstreek en de Veiligheidsregio Flevoland en de samenwerkingen die bestaan met andere organisaties. We werken daarom aan het expliciteren van de risico's en bewustzijn van informatiebeveiliging binnen Veiligheidsregio Gooi en Vechtstreek en de Veiligheidsregio Flevoland.

4.2 Toegang

- Binnen de Veiligheidsregio Gooi en Vechtstreek en de Veiligheidsregio Flevoland wordt niet meer toegang verleend aan medewerkers, samenwerkingspartners of vrijwilligers dan noodzakelijk. Hierbij gebruikt de veiligheidsregio het "need-to-know" principe.
- Bij uitdiensttreding wordt het account z.s.m. maar uiterlijk binnen 5 werkdagen op inactief gezet op basis van informatie van O&HR (of de leidinggevende bij spoed) over beëindiging van het contract.
- Er wordt zo veel mogelijk gebruik gemaakt van Single Sign On (SSO) met twee factor authenticatie (2FA) om in te loggen op applicaties/systemen.
- Op aangeven en in samenwerking met het team Informatisering & Automatisering (I&A) controleren leidinggevenden periodiek[1] of toegangsrechten van iedere medewerker onder hem/haar nog overeenkomen met de functie die hij/zij vervult. Het initiatief ligt hier bij het team I&A.

4.3 Verspreiden van informatie

- Medewerkers en vrijwilligers worden op de hoogte gesteld welke informatie wel of niet mag worden verspreid en hoe zij omgaan met versturen of opslaan van informatie.
- Bij transport van vertrouwelijke informatie over openbare netwerken, zoals het internet, dient geschikte encryptie te worden toegepast. Hierbij dient te worden aangehaakt bij de dataclassificatie (zie bijlage II 'informatieclassificatie' bij het Informatiebeveiligingsbeleid).
- Er zijn gedragsregels opgesteld voor opslag van vertrouwelijke informatie op verwijderbare media.
- Het meenemen van vertrouwelijke informatie buiten de EU vindt uitsluitend plaats indien dit voor de uitoefening van de functie noodzakelijk is en in overleg met de leidinggevende. Dit geldt dus ook voor devices zoals een telefoon, tablet en laptop van de VR waarop vertrouwelijke informatie staat.
- Fysieke verzending van bijzondere persoonsgegevens mag alleen geschieden met goedgekeurde middelen, waardoor de inhoud niet zichtbaar, niet kenbaar en inbreuk detecteerbaar is.

[1] Voor de frequenties zie BIO Norm A.9.2.3.1 en A.9.2.5.3

4.4 Leveranciersrelaties

- Bij de selectie van ICT dienstverleners wordt een pakket van eisen gehanteerd, waarin de IB en privacy eisen nadrukkelijk worden meegenomen. Tevens moet het pakket van eisen waarborgen dat de nieuwe oplossing past binnen de ICT omgeving van de Veiligheidsregio Gooi en Vechtstreek en de Veiligheidsregio Flevoland en geen nieuwe risico's introduceert in de organisatie.
- Van ICT dienstverleners die de ICT van de veiligheidsregio's beheren, wordt verwacht dat zij ISO 27001 gecertificeerd zijn en voldoen aan de BIO dan wel de faciliteiten bieden aan de veiligheidsregio's om te voldoen aan de BIO.

Bijlagen

Bijlage I – Gerelateerde documenten

In de volgende documenten is of wordt nader invulling gegeven aan het informatiebeveiligingsbeleid:

1. Rollen en verantwoordelijkheden IB Veiligheidsregio Gooi en Vechtstreek en de Veiligheidsregio Flevoland
2. Gedragscode voor gebruikers van de digitale werkomgeving
3. Uitwerkingen van het informatiebeveiligingsbeleid
4. Autorisatiebeleid Veiligheidsregio Gooi en Vechtstreek en de Veiligheidsregio Flevoland
5. Informatie Management Systeem Veiligheidsregio Gooi en Vechtstreek en de Veiligheidsregio Flevoland
6. Bewustwordingsprogramma IB
7. Proces risicobeheer
8. Continuïteitsplan Veiligheidsregio Gooi en Vechtstreek en de Veiligheidsregio Flevoland

Bijlage II - Informatieclassificatie

Vertrouwelijkheid	Belangrijkste beheersmaatregelen
1. Openbaar Informatie mag door iedereen worden ingezien (bijv.: algemene informatie op de externe website van de veiligheidsregio's)	• Deze informatie kent veelal lage eisen ten aanzien van de vertrouwelijkheid en is daardoor voor **iedereen** binnen en buiten de Veiligheidsregio Gooi en Vechtstreek en de Veiligheidsregio Flevoland beschikbaar en toegankelijk. • Geen specifieke bescherming noodzakelijk. • Integriteit is relevant, gegevens mogen niet kunnen worden gemuteerd door derden.
2. Intern gebruik Dit betreft de informatie die toegankelijk mag of moet zijn voor alle **medewerkers** van de veiligheidsregio. Voorbeelden: Procedures, werkinstructies, checklijsten.	• Logische toegangsbeveiliging op basis van een autorisatiematrix. • Worden niet gedeeld buiten de organisatie.
3. Vertrouwelijk Dit betreft informatie die alleen toegankelijk mag zijn voor een **beperkte** groep gebruikers waaronder informatie die persoonsgegevens bevat en daardoor extra beveiligd moet worden. Hieronder worden ook documenten of informatie verstaan die vanwege geldende wetgeving of opgelegde geheimhouding niet openbaargemaakt mogen worden. Voorbeelden: gegevens van medewerkers, geheime gegevens van bedrijven, contract informatie.	Aanvullend op intern[2]: • De informatie wordt beschikbaar gesteld op basis van het "*need to know*" principe. • De data is alleen toegankelijk met ten minste twee factor authenticatie. • Data wordt encrypted opgeslagen en getransporteerd (ten minste AES-256). • Bij verwerking van de data door een leverancier, wordt een verwerkersovereenkomst afgesloten met leveranciers die NEN-7510 / ISO 27001 gecertificeerd zijn.
4. Zeer vertrouwelijk Dit betreft informatie zoals bijzondere persoonsgegevens. Dit zijn gegevens die inzicht gegeven in iemands ras, geloof, gezondheid, seksuele voorkeur of geaardheid, lid van een vakbond, genetische of biometrische gegevens.	Aanvullend op vertrouwelijk: • Het raadplegen van de data wordt gelogd. • De toegang tot deze gegevens is beperkt tot degenen die hiervoor formeel bevoegd zijn.

Tabel 1: Classificatie van informatie

Deze classificatie van gegevens is als volgt herkenbaar:

1. Informatie die met toestemming gedeeld wordt op internet, is openbaar.

[2] Het is mede afhankelijk van de leveranciers of deze beheersmaatregelen worden aangeboden. Vanaf 2022 zal hiermee in de leverancierselectie expliciet rekening worden gehouden.

2. Voor alle documenten en gegevens die geen persoonsgegevens bevatten en alleen bedoeld zijn voor medewerkers van de veiligheidsregio, geldt de classificatie Intern. Op Interne documenten / gegevens die ten behoeve van een specifieke doelgroep worden verzameld, wordt aangegeven – indien relevant - binnen welke groep het document gedeeld mag worden.
3. Bestanden en documenten met persoonsgegevens in de zin van de AVG en behoren tot de categorie 3 en 4 zijn herkenbaar doordat de persoon identificeerbaar is.
4. Gegevens die inzicht gegeven in iemands ras, geloof, gezondheid, seksuele voorkeur of geaardheid, lid van een vakbond, genetische of biometrische gegevens behoren tot categorie 4, zeer vertrouwelijk.

Bijlage III - Begrippenlijst

Begrip	Toelichting
BIO (Baseline Informatiebeveiliging Overheid)	De Baseline informatiebeveiliging Overheid (BIO) is het basisnormenkader voor informatiebeveiliging binnen alle overheidslagen (Rijk, gemeenten, provincies en waterschappen). De BIO is gebaseerd op ISO 27002 met aanvullende beheersmaatregelen die specifiek zijn voor de overheid.
BIV-classificatie	Aan de hand van een BIV-classificatie wordt binnen de informatiebeveiliging, de beschikbaarheid (continuïteit), de integriteit (betrouwbaarheid) en de vertrouwelijkheid (exclusiviteit) van informatie en systemen aangegeven.
Informatie	Met informatie bedoelen we alle vormen van digitale en niet digitale informatie, alle mogelijke informatiedragers (zoals papier, elektronisch en USB stick) en alle informatie en netwerksystemen.
ISMS (Information Security Management System)	Een ISMS is een informatiebeveiligingsbeheersystemen en een belangrijk managementinstrument om veiligheidsrisico's in kaart te brengen en te beheersen. Beleid, taken en verantwoordelijkheden, normenkaders, beheersmaatregelen en inzicht in risico's komen in dit systeem bijeen.
ISO (International Standardization Organization)	ISO is een internationale organisatie die zich focust op het opstellen, beheren en verbeteren van normen voor organisaties, processen en keuringen.
ISO27001	ISO 27001 is een wereldwijd erkende norm voor informatiebeveiliging en risk management. De norm beschrijft hoe er procesmatig met het beveiligen van informatie wordt omgegaan. Met het uiteindelijke doel om de vertrouwelijkheid, beschikbaarheid en integriteit van informatie van een organisatie zeker te stellen.
NIPV (Nederlands Instituut Publieke Veiligheid)	Het Nederlands Instituut Publieke Veiligheid (NIPV) verbindt en versterkt de veiligheidsregio's, Rijksoverheid en crisispartners met onderzoek, onderwijs, ondersteuning en informatie.
Security	Het voorkomen of verminderen van het moedwillig toebrengen van schade aan medewerkers en bezittingen van de onderneming.

Zie voor een uitgebreide toelichting op gehanteerde begrippen in de informatiebeveiliging en cybersecurity: https://hetccv.nl/fileadmin/Bestanden/Onderwerpen/Cybercrime/Woordenboek-Cyberveilig-Nederland-2019.pdf.