VEILIGHEIDSREGIO UTRECHT

Beleid Informatiebeveiliging

Inhoudsopgave

Versienr	Datum	Auteur(s)	Status	Opmerking
0.1	6-10-2016	J. Meulendijks	Concept	**Initiële versie**
0.2	7-11-2016	J. Meulendijks	Concept	**Aanpassing huisstijl / doelstelling**
0.3	30-11-2016	O. Huizenga	Concept	**Review gehele document**
1.0	5-12-2016	J. Meulendijks	Definitief	**Aanbieding MT**
2.0	12-3-2018	M. van der Rijt	Definitief	**Aanbieding MT/DT**
3.0	22-4-2018	M. van der Rijt	Definitief	**Aanbieding DB**
3.0	14-5-2018	M. van der Rijt	Definitief	**Vastgesteld in DB**

1 Managementsamenvatting

1.1 Samenvatting

Voor u ligt het informatieveiligheidsbeleid van de VRU. Het beschrijft het te voeren beveiligingsbeleid binnen de VRU. Hieraan gerelateerd zijn de meer gedetailleerde procedures, maatregelen en richtlijnen die voor het uitvoeren van het beleid van toepassing zijn. Dit beleid beschrijft de richting en ondersteuning zoals deze door het dagelijks bestuur van de VRU (DB) is bepaald voor informatiebeveiliging in overeenstemming met de bedrijfsmatige eisen voor effectieve en efficiënte bedrijfsprocessen, betrouwbare financiële verslaggeving en naleving van wet- en regelgeving.

Het DB stelt daarom het volgende informatiebeveiligingsbeleid vast:

- Het informatiebeveiligingsnormenkader Baseline Informatiebeveiliging Gemeente (BIG) wordt beschouwd als uitgangspunt voor het ontwikkelen van richtlijnen die specifiek op de organisatie zijn toegesneden. Op sommige punten kan -gemotiveerd - worden afgeweken van de voorgestelde maatregelen en/of zijn er wellicht aanvullende maatregelen nodig.
- Het uit te dragen informatiebeveiligingsbeleid is vastgelegd in dit document.

- In het informatiebeveiligingsplan is het beleid vertaald in concrete maatregelen.
- De in het informatiebeveiligingsplan beschreven maatregelen geven het ambitieniveau van VRU weer.
- Alle medewerkers van de VRU conformeren zich aan het Informatiebeveiligingsbeleid.
- Alle medewerkers zijn gehouden gegevens en informatiesystemen te beschermen tegen ongeautoriseerde toegang, gebruik, verandering, openbaring, vernietiging, verlies of overdracht.
- De VRU bevordert actief het beveiligingsbewustzijn van haar medewerkers.
- Daartoe worden alle onderdelen van dit beleid uitgewerkt in concrete richtlijnen en maatregelen, toegesneden op de taken en verantwoordelijkheden van de betrokken medewerkers.
- Periodiek wordt beoordeeld of voor specifieke gegevens of informatiesystemen aanvullende maatregelen noodzakelijk zijn. De frequentie van de beoordeling is gerelateerd aan de planning & control cyclus van de VRU. De naleving van genomen maatregelen wordt periodiek getoetst.
- Het beleid wordt eens per drie jaar herzien en indien nodig tussentijds aangepast.

Vastgesteld tijdens de vergadering van het DB van 14 mei 2018.

1.2 Leeswijzer

In *Hoofdstuk 1* wordt het **beveiligingsbeleid** van VRU beschreven in doelstellingen en uitgangspunten.

Hoofdstuk 2 beschrijft de **verantwoordelijkheden en bevoegdheden** van de verschillende functies en rollen voor beveiliging.

In *Hoofdstuk 3* is de **Beheersing** van beveiliging opgezet.

Voor de leesbaarheid van dit document is ervoor gekozen om de wijze waarop de invulling van dit beleid plaatsvindt te verwerken in separate documenten. Deze documenten zijn onderdeel van het ISMS (Information Security Management System).

ISMS

Het ISMS is het Information Security Management System. Door het inrichten van een ISMS behoud de organisatie grip op het onderwerp Informatiebeveiliging.

Dit document geeft invulling aan de volgende normenelementen

ISO 27001	BIG
5.1.1	5.1.1

2 Beveiligingsbeleid

De informatiebeveiligingsdoelstelling is afgeleid van de missie van de VRU. Deze luidt:

"*We zijn de drijvende en bindende kracht achter een goede hulpverlening, rampenbestrijding en crisisbeheersing in de regio Utrecht. Dit doen wij binnen onze wettelijke kaders*"[1].

Op basis van deze missie is het mogelijk een (strategische) doelstelling voor Informatiebeveiliging te definiëren.

Alle medewerkers van de VRU zijn zich bewust van hun handelen (professionaliteit) ten aanzien van de informatiebeveiligingsaspecten en op welke wijze dit bijdraagt om als VRU een betrouwbare taakuitvoerder te zijn die met vakmanschap en passie, continu kan anticiperen en inspelen op ontwikkelingen in het fysieke veiligheidsdomein.

Deze doelstelling heeft betrekking op de organisatie-, technische- en mensaspecten.

2.1 Doel van het beleid

Beschikken over juiste en betrouwbare informatie, maar ook het delen ervan met ketenpartners, is essentieel voor het succes van de VRU. De VRU heeft haar beleidsplan daarom als titel "verbinden voor veiligheid" gegeven. Hierbij is het belangrijk dat vanuit een strategisch oogpunt wordt bepaald, vastgelegd en gecommuniceerd hoe de VRU informatie ontvangt, gebruikt en uitwisselt. Voor een effectieve beveiliging is het noodzakelijk dat gegevens, die aan de basis liggen van informatie, voldoen aan de gestelde eisen ten aanzien van vertrouwelijkheid, integriteit en beschikbaarheid. Effectieve beveiliging wordt ook bereikt door te werken met gepaste gedragsregels, in overeenstemming met de wetgeving, navolgen van het vastgesteld beleid en de gewenste richtlijnen uit de praktijk.

Dit beleid beschrijft het te voeren beveiligingsbeleid en geeft richting aan de meer gedetailleerde maatregelen en richtlijnen die van toepassing zijn binnen VRU. Het beschrijft de fysieke- en informatiebeveiliging voor wat betreft de organisatorische aspecten en de uitvoering. Voor de leesbaarheid van dit document is ervoor gekozen om verdere invulling van dit beleid te verwerken in separate documenten en/of procesbeschrijvingen.

[1] Bron (intranet): VRU Directiemanifest, *april 2013*

Doelstellingen

De doelstellingen van dit beleid zijn:

- Het voldoen (compliant zijn) aan geldende wet- en regelgeving
- Het beschermen van alle fysieke en digitale informatiesystemen binnen VRU (met inbegrip van, maar niet beperkt tot, alle computers, netwerkapparatuur, software en data) en het beperken van de risico's van diefstal, verlies, misbruik, of beschadiging van deze systemen.
- De bewustwording creëren met betrekking tot de bekendheid en naleving van alle huidige en relevante interne procedures en richtlijnen, alsmede van wetgeving op het gebied van informatieveiligheid. Met het doel te zorgen dat alle gebruikers hun eigen verantwoordelijkheden begrijpen voor de bescherming van de vertrouwelijkheid en integriteit van de gegevens die zij behandelen.
- Het zorgen voor een veilige en betrouwbare werking van de informatiesystemen voor het personeel en andere geautoriseerde gebruikers.
- De borging ten aanzien van het beheer (exploitatie) van informatiesystemen om onbedoelde wijzigingen, met mogelijke nieuwe risico's, te voorkomen.
- De VRU te beschermen tegen aansprakelijkheid of schade door het misbruik van haar informatiesystemen en faciliteiten.
- Zorgen voor een systematiek van incidentenregistratie, analyse en selecteren van gepaste maatregelen om informatieveiligheid te vergroten.
- Het bieden van kader voor een adequate continuïteitstrategie om onderbrekingen van activiteiten tegen te gaan en kritieke processen te beschermen tegen de gevolgen van omvangrijke storingen in informatiesystemen of rampen en om tijdig herstel te bewerkstelligen.

Reikwijdte

Het beleid heeft betrekking op alle door VRU gebruikte gegevens en hieraan gerelateerde informatiesystemen, de fysieke aspecten met betrekking tot deze gegevens, privé-systemen welke zijn aangesloten op het netwerk van VRU (bijvoorbeeld laptops van medewerkers) én op software in eigendom van de VRU of via licentie verkregen.

Uitgangspunten

- De inhoud van dit beleid dient bekend te zijn bij alle geautoriseerde gebruikers van de VRU en de oplegging tot naleving ervan. Om dit te bereiken zal het onderwerp 'informatiebeveiliging' deel uitmaken van het inwerkprogramma van nieuwe medewerkers. Daarnaast wordt periodiek,

maar minimaal één keer per **vier** maanden, het onderwerp op het (werk-)overleg geagendeerd en besproken.

- Informatiebeveiliging is een continu proces. Daarom is het nodig periodiek het vastgestelde beleid te herijken. Technologische en organisatorische ontwikkelingen binnen en buiten de VRU maken het noodzakelijk om periodiek te beoordelen of de organisatie op adequate wijze de (informatie-)beveiliging weet te waarborgen. Audits maken het mogelijk het beleid en de genomen maatregelen te controleren op effectiviteit.
- De VRU is eigenaar van de informatie die onder haar verantwoordelijkheid wordt geproduceerd, tenzij dit op basis van wettelijke gronden anders is overeengekomen.
- Elke medewerker van de VRU behoort de waarde van informatie te kennen en daarnaar te handelen. Deze waarde wordt bepaald door de schade als gevolg van verlies van beschikbaarheid, integriteit en vertrouwelijkheid. Het classificeren van gegevens kan hierbij behulpzaam zijn. Zie ook paragraaf 0.
- Bij veranderingen, zoals infrastructurele wijzigingen of de aanschaf van nieuwe systemen, wordt het onderwerp informatiebeveiliging zowel in de voorbereidingen als in de uitvoering meegenomen.
- Door de VRU wordt de BIG als normenkader gehanteerd, waartegen toetsing van de uitvoering van het beleid en genomen maatregelen mogelijk is.

2.2 Risicoanalyse en continuïteit

Beveiligen gebeurt met een duidelijk beeld voor ogen van de waarde van datgene wat beveiligd wordt. Dat betekent dat bewustzijn van die waarde en van de risico's van mogelijke schade, de grondslag is van dit beleid en daarmee sturend moet zijn in het nemen van maatregelen. Het is de taak van de verantwoordelijke bestuurder(s) en lijnmanagement om ervoor te zorgen dat dit bewustzijn aanwezig is.

Risicoanalyse

Om reproduceerbaar en eenduidig de waarde van informatie(-systemen) en gepaste beheersmaatregelen te kunnen bepalen wordt er gebruik gemaakt van een kwalitatieve risicoanalyse om onderbouwd de belangrijkste risico's te identificeren. De risicoanalyse wordt, in beginsel, elke drie jaar herhaald, of tussentijds in het geval van substantiële wijzigingen.

Classificatie informatiesystemen

Elk informatiesystemen heeft een eigenaar[2]. De waarde van de informatiesystemen wordt vastgesteld door de eigenaar o.b.v. een uniforme methodiek voor classificatie van beveiligingsniveaus voor informatiesystemen, zie tabel 1. De waarde wordt bepaald door de schade die verlies van beschikbaarheid, integriteit en vertrouwelijkheid toebrengt aan de mogelijkheid tot het kunnen organiseren van de risicobeheersing, rampenbestrijding en crisisbeheersing binnen de regio.

Strategie voor Continuïteit

Informatiebeveiliging heeft als doel om risico's met betrekking tot informatiebeveiligingsincidenten te reduceren tot een, door management 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, in geval van calamiteiten, de getroffen ICT-dienst of het getroffen informatiesysteem, binnen de door de VRU vastgestelde tijd, operationeel gemaakt kan worden. Een continuïteitsplan kan variëren van een goede back-upvoorziening of het geografisch spreiden van de ICT-dienst tot een complete uitwijk. Continuïteitsplannen worden minimaal **één** keer per jaar op actualiteit geëvalueerd.

[2] Met eigenaar wordt bedoeld de persoon/functionaris, doorgaans de proceseigenaar, die verantwoordelijk is voor alle aspecten ten aanzien de exploitatie, aanpassingen en toekomstige vervangingen van het systeem.

2.3 Informatieclassificatie

Alle informatie binnen de VRU wordt geclassificeerd naar één van de drie niveaus van vertrouwelijkheid, zoals hieronder vermeld.

Gegevens-classificatie	Kenmerken van informatie
Publiek	Deze informatie kent veelal lage eisen ten aanzien van de vertrouwelijkheid en beschikbaarheid en is daardoor voor **iedereen** binnen en buiten de VRU beschikbaar en toegankelijk.
Intern	Dit betreft de informatie die toegankelijk mag of moet zijn voor alle **medewerkers** van de VRU. De eisen ten aanzien van vertrouwelijkheid zijn beperkt maar aanwezig.
Vertrouwelijk	Dit betreft informatie die alleen toegankelijk mag zijn voor een **beperkte** groep gebruikers. Hieronder worden ook documenten of informatie verstaan die vanwege geldende wetgeving of opgelegde geheimhouding niet openbaargemaakt mogen worden. De informatie wordt beschikbaar gesteld op basis van het "*need to know*" principe[3]. Schending van deze classificatie kan direct of indirecte schade toebrengen aan de VRU, onderdelen van de VRU of personen binnen en buiten de VRU.

Voor informatie geclassificeerd als 'Intern' of 'Vertrouwelijk' dienen, additioneel aan het basis beveiligingsniveau, extra beschermende maatregelen te worden getroffen.

2.4 Naleving van wet- en regelgeving

De VRU dient zich te houden aan alle relevante wet- en regelgeving die van toepassing zijn op het uitvoeren van de dagelijkse werkzaamheden. De relevante wet- en regelgeving is vertaald naar richtlijnen en gedragscodes die van toepassing zijn op alle medewerkers van de VRU en voor het overige van toepassing zijn op inhuurpersoneel, stagiaires van de VRU of derden (zoals leveranciers) die gebruik maken van informatievoorzieningen van de VRU. In het bijzonder gelden in dit verband de volgende richtlijnen en codes:

- Gedragscode telefonie-, e-mail- en internetgebruik.

Wettelijke voorschriften welke opgevolgd dienen te worden:

- Wet op computercriminaliteit.
- Wet Bescherming Persoonsgegevens.
- Algemene Verordening Gegevensbescherming[4] (AVG)

[3] Need to know principe. Dit principe houdt in dat functionarissen slechts toegang hebben tot die informatie die zij nodig hebben voor het uitoefenen van hun functie.

[4] De AVG is de Europese privacy verordening die per24 mei 2016 in werking is getreden. De Verordening is pas vanaf 25 mei 2018 van toepassing.

- Auteurswet.
- Archiefwet.
- Beleidsregels Informatiebeveiligingsbeleid C2000.
- Meldplicht datalekken.

Daarnaast gelden de afspraken die contractueel gelden met leveranciers waarmee de VRU afspraken heeft gemaakt.

Indien de VRU schade ondervindt door nalatigheid bij het gebruik of het opzettelijke misbruik van informatievoorzieningen (plichtsverzuim) zullen de vigerende wet- en regelgeving worden toegepast en op basis daarvan maatregelen worden genomen door of namens de directie van de VRU.

3 Verantwoordelijkheden

Informatiebeveiliging dient als proces[5] te worden ingericht. Het onderwerp moet tevens een duidelijk benoemd onderdeel zijn van alle processen van de VRU[6]. Informatiebeveiliging is onderdeel van de planning- en control cyclus. Aansluitend hierbij worden jaarplannen opgesteld, belegd in de organisatie en uitgevoerd. De resultaten ervan worden geëvalueerd en vertaald naar nieuwe jaarplannen (Plan, Do, Check, Act).

3.1 Actoren

Verschillende actoren binnen de VRU verrichten gezamenlijk de activiteiten binnen het beveiligingsproces. Elke actor heeft een bepaalde rol[7] binnen het proces. Een goede verdeling van de *taken, bevoegdheden en verantwoordelijkheden* (TBV's) tussen de verschillende actoren is cruciaal voor een effectief en efficiënt procesverloop.

Voor beveiliging worden binnen de VRU de volgende actoren onderkend:

- De directie heeft strategische verantwoordelijkheid - besturing.
- Het lijnmanagement heeft een tactische verantwoordelijkheid - aansturing.
- De CISO[8] (informatiebeveiligingscoördinator) - beheersing en naleving.
- De kwaliteitsadviseur bewakende en adviserende verantwoordelijkheid.
- De medewerker (iedereen) hebben een operationele verantwoordelijkheid - uitvoering.
- De externe partijen, onafhankelijk toetsen en beoordelen.

Het DB is verantwoordelijk voor het vaststellen van het beleid en de directie voor het vaststellen van de richtlijnen die ten grondslag liggen aan een adequaat systeem van informatiebeveiliging en voor het beoordelen van de efficiëntie en effectiviteit hiervan. Als verantwoordelijke voor het onderwerp informatiebeveiliging is een portefeuillehouder informatiebeveiliging aangewezen.

Vanuit de rol van CISO is de functionaris verantwoordelijk voor beleidsvorming, controle en registratie, communicatie en voorlichting en stelt verbetervoorstellen op voor de informatiebeveiliging. Dit gebeurt in nauw overleg met de kwaliteitsadviseur.

---

[5] Voor de inrichting van het proces is het Information Security Management System (ISMS) als uitgangspunt te nemen.
[6] Of in contracten ondergebracht indien er sprake is van uitbestede (ICT-)diensten.
[7] Voor een beschrijving van de verschillende rollen zie het document: "6.1.1_Rollen Informatiebeveiliging"
[8] Chief Information Security Officer.

De kwaliteitsadviseur bewaakt de samenhang met het kwaliteitssysteem van de VRU. Belangrijke taken vanuit de kwaliteitsmedewerker VRU zijn informeren, borging van de integrale kwaliteit en doelmatigheid van de VRU activiteiten, naleving van wet- en regelgeving en het eigen beleid en het uitvoeren van audits om van daaruit te komen tot verbetervoorstellen.

De dagelijkse verantwoordelijkheid berust bij het lijnmanagent van de VRU die voortdurend toezien op naleving van de vastgestelde richtlijnen. Daarnaast wordt van hen verwacht om de risico's beoordelen waarmee hun afdeling wordt geconfronteerd.

Elke medewerker (al dan niet in vaste dienst) van de VRU is gehouden mee te werken aan de informatiebeveiliging. Zij zijn op individueel niveau verantwoordelijk voor een effectieve informatiebeveiliging van de aan hen toevertrouwde gegevens. Ook wordt van alle medewerkers verwacht dat zij eventuele beveiligingsincidenten direct melden bij hun leidinggevende (of hiervan een melding maken in het registratiesysteem).

Voor sommige (werk-)processen geldt dat deze (deels) worden *uitgevoerd* door externe partijen. Met de externe dienstverleners worden concrete en toetsbare afspraken gemaakt over de door hen te treffen beveiligingsmaatregelen. Deze afspraken worden vastgelegd in externe dienstverleningsovereenkomsten. In elke dienstverleningsovereenkomst worden de door de dienstverlener te treffen beveiligingsmaatregelen beschreven. De VRU controleert periodiek de correcte naleving van de gemaakte afspraken.

3.2 Evaluatie & Controle

Onder controle wordt verstaan zowel interne controle door de eigen organisatie als toetsing door een onafhankelijke derde. De toetsing richt zich zowel op het beveiligingsbeleid als op de maatregelen die uit dit beleid voortvloeien. Dit betekent dat de toetsing zich richt op de volgende drie punten:

1. Juiste naleving van het beleid en de interne werkafspraken;
2. Correcte werking van de beveiligingsorganisatie;
3. Toereikendheid van de vastgestelde beveiligingsmaatregelen gedurende een bepaalde periode.

Onder evaluatie wordt verstaan het nagaan of de kaders van de beveiliging inhoudelijk nog toereikend zijn. Hierbij worden twee niveaus onderscheiden: de evaluatie van het beleid en de evaluatie van het beheer.

De evaluatie van het beleid is een heroriëntatie op de beleidsuitgangspunten. Bij de evaluatie van het beheer wordt nagegaan of het vastgestelde beleid nog toereikend is.

De periodieke controle (opgenomen in het jaarplan) op beveiliging bestaat uit drie onderdelen:

1. Toetsing beveiligingsmaatregelen
   Om ervoor te zorgen dat geïmplementeerde beveiligingsmaatregelen worden nageleefd dient er periodiek worden gemeten, naast de dagelijkse controle door teamleiders. De interne auditors (eventueel kwaliteitsmedewerkers) zullen op basis van een nader vast te stellen werkprogramma (inclusief uitgewerkte kwaliteitseisen) een audit uitvoeren.

2. Functiescheiding bij audits
   Om ervoor te zorgen dat de beveiligingsorganisatie (actoren, rollen, TBV's) correct werkt, wordt dit opgenomen in de interne auditstructuur. Er moet hierbij rekening gehouden worden met noodzakelijke functiescheiding. De functionarissen die zelf deel uitmaken van de beveiligingsorganisatie mogen geen deel uitmaken van het auditteam. Dit om belangenverstrengeling te voorkomen.

3. Evaluatie van het beleid
   Driejaarlijks wordt het vastgestelde beleid (inclusief maatregelen) op de toereikendheid beoordeeld. Concreet betekent dit dat beoordeeld wordt of het beleid en de maatregelen zorgen voor een afdoende beveiliging van de processen en de informatiestromen van de VRU.

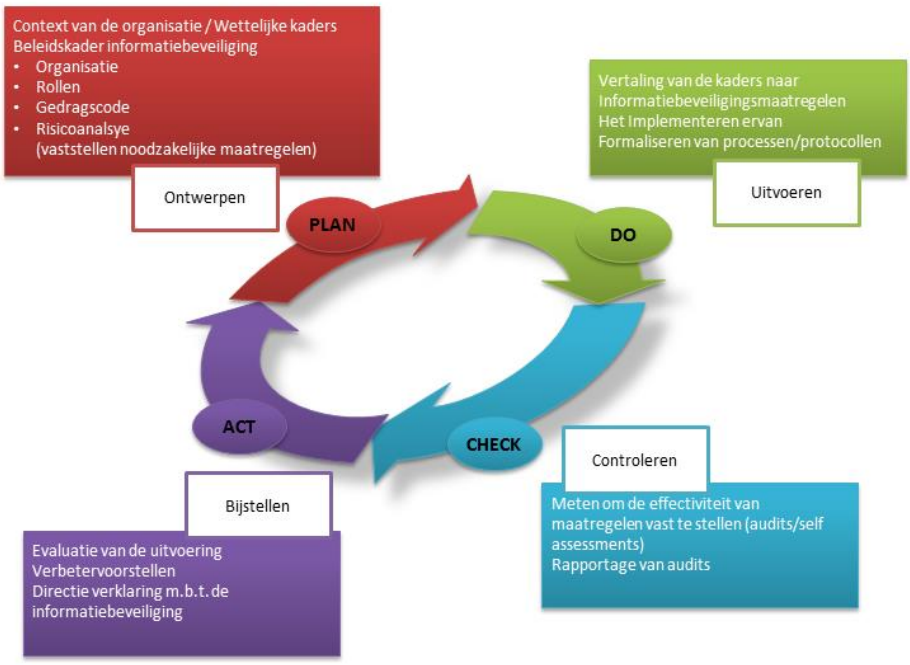
3.3 Sancties bij inbreuken op het informatiebeveiligingsbeleid

Het beleid is uitgewerkt in verschillende processen, procedures en richtlijnen die van toepassing zijn binnen de VRU. Bij inbreuk op het informatiebeveiligingsbeleid zullen door of namens de directie (passende) maatregelen worden getroffen.

Indien de VRU wordt aangesproken op de overtreding van eigendomsrechten, auteursrechten of overtreding van andere wettelijke bepalingen, zijn de wettelijke en binnen de VRU geldende regelingen van toepassing. In geval er door het onrechtmatig handelen schade ontstaat, wordt of kan de overtreder daarvoor aansprakelijk gesteld.

4 Beheersing van informatiebeveiliging

De informatiebeveiliging van de VRU is een cyclisch proces. Via de zogenaamde Plan-Do-Check-Act cyclus wordt gestreefd naar een adequaat niveau van informatiebeveiliging. De tussentijdse controles of constateringen kunnen aanleiding zijn bij te sturen op de bestaande maatregelen.



De cyclus wordt jaarlijks minimaal één keer doorlopen. Het procesonderdeel toetsing wordt jaarlijks uitgevoerd wat betreft de toetsing van de opzet en het bestaan, en **twee-**jaarlijks wat betreft de toetsing van de werking (het bestaan gedurende een vastgestelde periode).

Bijlage 1 - Definities

In deze bijlage worden enkele definities nader toegelicht.

Algemene Verordening Gegevensbescherming

De AVG is de Europese privacy verordening die per24 mei 2016 in werking is getreden. De Verordening is pas vanaf 25 mei 2018 van toepassing. De AVG vervangt de huidige privacy wetten van de verschillende EU-lidstaten.

Chief Information Security Officer

De functionaris binnen de VRU welke is belast met het coördineren van de informatiebeveiligingsactiviteiten.

Continuïteitsplan

Een plan om bij (ernstige) verstoringen de informatievoorziening gericht op het primaire proces, binnen de door de VRU aangegeven tijd, weer beschikbaar te hebben.

Compliant

Compliance betekent dat de organisatie moet (en wil) voldoen aan de wet- en regelgeving. Het niet voldoen aan compliancy-eisen brengt risico's met zich mee zoals:

- imagoschade die kan worden opgelopen;
- financiële schade in de vorm van boetes of claims.

Fysieke en digitale informatiesystemen

Informatiesystemen met het doel vanuit gegevensbronnen voor een gebruiker relevantie informatie te generen. Dit kan een digitaal systeem (bijvoorbeeld: een applicatie) zijn of een fysiek systeem (bijvoorbeeld: het HRM-dossier in een kast)

Incidentenregistratie

Een systeem, bij voorkeur digitaal, waar meldingen over de informatiebeveiliging in worden geregistreerd zodat de organisatie adequaat kan reageren en de opvolging kan worden gemonitord.

ISMS

Het Information Security Management System. Door het inrichten van een ISMS behoud de organisatie grip op het onderwerp Informatiebeveiliging.