Informatiebeveiligingsbeleid

Reclassering Nederland

Versie: 1.0 – definitief
Auteur: Fred van Tol
Datum goedkeuring Directie RN: 03-04-2023

Inhoud

1. Inleiding

Dit beleidsdocument beschrijft het beleid dat Reclassering Nederland voert ten aanzien van de beveiliging van informatie en de informatievoorziening. Het stelt kaders en geeft aan hoe Reclassering Nederland informatiebeveiliging invult als onderdeel van de uitvoering van haar taken.

Het informatiebeveiligingsbeleid als beschreven in dit document heeft de goedkeuring van de RN Directie. Het heeft daarmee een normstellend en verplichtend karakter.

Reclassering Nederland verwacht van alle medewerkers dat zij kennis hebben genomen van het informatiebeveiligingsbeleid en dat leidinggevenden sturing geven aan de uitvoering binnen de kaders van dit beleid.

Voor het vervullen van onze wettelijke taken werken wij met zeer veel informatie van onszelf, van cliënten en van relaties. De aard van deze informatie noodzaakt tot beveiliging. Informatie moet bij ons in goede, vertrouwde handen zijn!

Het vereiste betrouwbaarheidsniveau kan alleen worden bereikt als iedereen weet waarom informatiebeveiliging voor Reclassering Nederland noodzakelijk is, zijn steentje bijdraagt en zijn eigen verantwoordelijkheid serieus neemt. Het is daarom belangrijk dat iedere gebruiker op de hoogte is van regels en richtlijnen die specifiek voor hem van toepassing zijn en deze naleeft. Alleen dan is de betrouwbaarheid van de informatie en informatievoorziening, die nodig is voor de continuïteit van onze werkprocessen en activiteiten, gewaarborgd op het niveau dat wij ons ten doel stellen en de samenleving van ons mag verwachten.

Reclassering Nederland geeft via dit beleidsdocument aan dat Reclassering Nederland:
1. Waarde hecht aan informatiebeveiliging als integraal onderdeel van de algehele bedrijfsvoering.
2. Een heldere, bewust gekozen basis hanteert voor de invulling van informatiebeveiliging op alle niveaus.

Voor vragen, opmerkingen of verbetervoorstellen inzake dit beleid kan je je wenden tot de Chief Information Security Officer (CISO).

1.1 Versie beheer en geldigheid

Versie	Datum	Auteur	Wijzigingen
0.2	14-09-22	F. van Tol	
0.3	30-11-22	F. van Tol	
0.4	13-02-23	F. van Tol	
1.0 Definitief	03-04-23	F. van Tol	Goedgekeurd Directie Reclassering Nederland

De Directie Reclassering Nederland is eigenaar van dit document. De Chief Information Security Officer (CISO) van Reclassering Nederland is auteur van dit document en verantwoordelijk voor beheer, periodieke evaluatie en bijstelling. Herijking vind iedere drie jaar plaats, tenzij grote veranderingen eerdere herijking noodzakelijk maken.

1.2 Definitie

Informatiebeveiliging is het proces van vaststellen van de vereiste betrouwbaarheid van informatie en informatiesystemen, alsmede het treffen en in standhouden van een samenhangend, weloverwogen pakket van organisatorische-, procedurele-, technische- en bewustwordingsmaatregelen ten aanzien van toegankelijkheid en gebruik van informatie.

1.3 Belang

De voornaamste redenen voor Reclassering Nederland om informatiebeveiliging op orde te hebben zijn:

- De verantwoordelijkheid voor de bescherming van de informatie die aan Reclassering Nederland is toevertrouwd
- De verplichtingen die voortkomen uit wet- en regelgeving
- De verplichtingen en verantwoordelijkheid die Reclassering Nederland heeft richting de Nederlandse samenleving
- De grote bedrijfsafhankelijkheid van informatievoorzieningen en informatie.

1.4 Werkingsgebied

Het Informatiebeveiligingsbeleid van Reclassering Nederland geldt voor:

- alle informatie (elektronisch, papier en mondeling) en IT systemen die gebruikt worden voor de uitvoering van de primaire en bedrijfsondersteunende processen van Reclassering Nederland. Hieronder vallen ook applicaties en portalen die extern gehost worden of als SaaS-dienst worden afgenomen
- de uitwisseling van informatie (elektronisch, papier en mondeling) tussen Reclassering Nederland en andere partijen zoals cliënten, opdrachtgevers, ketenpartners en leveranciers
- alle medewerkers, in dienst van dan wel ingehuurd door Reclassering Nederland.

1.5 Doel beleidsdocument

Dit beleidsdocument is primair bedoeld voor gebruik binnen Reclassering Nederland, als:

- Richtinggevend kader voor het beheersen van informatiebeveiligingsrisico's en implementeren en borgen van informatiebeveiliging binnen Reclassering Nederland.
- Basis voor communicatie-instrumenten voor het onder de aandacht brengen van het IB-beleid bij leidinggevenden en medewerkers.

1.6 Leeswijzer

Het eerste hoofdstuk behandelt een aantal aspecten van het informatiebeveiligingsbeleid, zoals doel, werkingsgebied en geldigheid. Hoofdstuk 2 beschrijft het informatiebeveiligingsbeleid zelf, met een onderverdeling naar medewerkers, toegang tot informatie en IT systemen. Hoofdstuk 3 gaat over de processen voor het tot stand brengen van informatiebeveiliging en de beheersing daarvan.

Bijlage 1 *Relevante wet- en regelgeving* geeft een overzicht van wet- en regelgeving die belangrijk is voor Reclassering Nederland in het kader van informatiebeveiliging. Bijlage 2 *Definities* geeft een overzicht en definitie van een aantal belangrijke gehanteerde begrippen. Bijlage 3 geeft een opsomming van de gouden regels op het gebied van gedrag. Bijlage 4 *strategische risicoanalyse* geeft inzicht in het risicoprofiel van Reclassering Nederland en is input geweest voor dit beleidsstuk. Bijlage 5 bevat een tabel met een overzicht van de classificaties en de gegevens die daarbij horen.

Daar waar dit informatiebeveiligingsbeleid taken, verantwoordelijkheden en/of bevoegdheden aan personen toewijst, hanteert het document omwille van de leesbaarheid de 'hij'-vorm (en is de 'zij'- of "hen" vorm eveneens van toepassing).

2. Informatiebeveiligingsbeleid

Dit hoofdstuk beschrijft het informatiebeveiligingsbeleid. Het beleid is uitgewerkt in regels en richtlijnen. Achtereenvolgens komen aan bod:

- Doelstellingen
- Taken en verantwoordelijkheden
- Beleid voor medewerkers
- Beleid voor toegang tot informatie
- Beleid voor applicaties en IT infrastructuur
- Beleid voor Ketenpartners en leveranciers
- Continuïteitsbeleid
- Beleid voor clouddiensten
- Beleid voor logging en monitoring.

2.1 Doelstellingen

De informatiebeveiliging van Reclassering Nederland heeft als doel:

- **Te voorkomen dat niet-openbare informatie van/over Reclassering Nederland, medewerkers, cliënten en relaties, zonder nadrukkelijke toestemming van de eigenaar van de informatie of zonder een andere gegronde reden, in verkeerde handen komt.** informatie – van wie dan ook - moet bij Reclassering Nederland in goede handen zijn. Het uitlekken van informatie kan schadelijk uitpakken voor Reclassering Nederland, haar medewerkers, cliënten en/of de mensen en partijen met wie Reclassering Nederland samenwerkt. Het kan resulteren in inbreuk op de persoonlijke levenssfeer van medewerkers of cliënten, reputatieschade, financiële schade door claims, een afname van zaken en subsidie, afname van mogelijkheden tot samenwerking, et cetera.

- **Te voorkomen middels maatregelen in IT systemen en applicaties dat informatie bedoeld of onbedoeld wijzigt en onjuist is.**[1] Voor het nemen van de juiste stappen en beslissingen op alle niveaus van het werk is het noodzakelijk dat informatie niet veranderd tijdens opslag of verzending van het werk door storingen, fouten of opzettelijke wijzingen. Fouten en afwijkingen kunnen leiden tot onjuiste adviezen, interventies en toezicht.

- **Het voorkomen en terugdringen van de gevolgen door verstoring van de primaire reclasseringsprocessen van Reclassering Nederland door verstoring van IT-infrastructuur en applicaties.** Voor het verwezenlijken van de missie van Reclassering Nederland is de continuïteit van de primaire reclasseringsprocessen belangrijk. Verstoring of uitval van de (al dan niet digitale) informatievoorziening en onjuiste of het ontbreken van informatie mag niet leiden tot onwenselijke gevolgen voor opdrachtgevers, ketenpartners en/of cliënten.

- **Het voldoen aan 1) wet- en regelgeving op het gebied van informatiebeveiliging en 2) formeel gemaakte afspraken waar derden Reclassering Nederland aan kunnen houden.** Reclassering Nederland dient zich te houden aan wet- en regelgeving. Daarnaast heeft Reclassering Nederland te maken met voorwaarden en bepalingen die voortkomen uit overeenkomsten en andere formeel met andere partijen gemaakte afspraken.

- **Reclassering Nederland volgt de Baseline Informatiebeveiliging Overheid (BIO).** Voor het inrichten van haar informatiebeveiliging laat Reclassering Nederland zich leiden door de BIO van het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties. Uitgangspunt voor alle informatie en informatiesystemen van Reclassering Nederland is **Basis BeveiligingsNiveau 2 (BBN2) van de BIO.**

[1] Het beleid en processen op het gebied van Datamanagement, gericht op beheer, juistheid en validatie van gegevens valt niet binnen de scope van dit beleid

2.2 Taken en verantwoordelijkheden

Naast verantwoordelijkheden en taken voor informatiebeveiliging die algemeen van aard zijn, kent Reclassering Nederland een aantal bijzondere rollen met taken, verantwoordelijkheden en bevoegdheden die specifiek zijn. Hieronder zijn algemene en specifieke taken en verantwoordelijkheden opgesomd.

Rol	Verantwoordelijkheid
Directie	• Goedkeuring van het informatiebeveiligingsbeleid, • Het uitdragen van het belang van informatiebeveiliging en het geven van het goede voorbeeld.
LMT	• Het aansturen en houden toezicht op naleving van informatiebeveiliging. • Het uitdragen van het belang van informatiebeveiliging en het geven van het goede voorbeeld.
Directeur P&O en Bedrijfsvoering	• Aanspreekpunt op bestuurlijk niveau • Eindverantwoordelijk dragen voor informatiebeveiliging
Medewerkers	• Zijn zelf verantwoordelijk voor het naleven van de regels en het gebruik van middelen om veilig te werken.
Leidinggevenden	• Houden toezicht op naleving van de regels door hun medewerkers en hebben een voorbeeldfunctie. • Leidinggevenden zijn verantwoordelijk voor het controleren van raadplegingen van clientdossiers • Het juist doorlopen van het P&O proces (o.a. VOG aanvragen, toekennen van de juiste rechten en inkoopproces (stellen van security eisen aan de in te kopen dienst) • Het bewust maken van medewerkers van informatiebeveiliging maakt integraal deel uit van de managementtaak van leidinggevenden. • De leidinggevende realiseert bewustwording door informatiebeveiliging aan bod te laten komen in werkoverleg en via tweegesprekken met de medewerker
Projectleider	• Is verantwoordelijk voor het bepalen en implementeren van de securitymaatregelen in de op te leveren dienst, applicatie of product.
Applicatie eigenaar	• Is verantwoordelijk voor implementeren en up to date houden van security maatregelen in de applicatie.
Hoofd afdeling I&A & huisvesting en inkoop	• Is verantwoordelijk voor het implementeren en testen van de security maatregelen binnen de IT infrastructuur en applicaties, gebouwen, kantoor- en technische ruimtes. • Is verantwoordelijk dat het inkoop proces voldoet aan de betreffende maatregelen uit de BIO (Hoofd afdeling inkoop is niet verantwoordelijk voor de uitvoering van de maatregelen)
Hoofd afdeling P&O	• Is verantwoordelijk dat het P&O proces voldoet aan de betreffende maatregelen uit de BIO. (Hoofd afdeling P&O is niet verantwoordelijk voor de uitvoering van de maatregelen).
Hoofd afdeling Control & Auditing	• Is verantwoordelijk voor het periodiek uitvoeren van audits op het gebied van informatiebeveiliging. Hierover heeft hij afstemming met de CISO.
Hoofd afdeling Beleid	• Is verantwoordelijk dat informatiebeveiliging is geborgd in nieuw beleid en projecten
Chief Information Security Officer (CISO)	• Ondersteunt het primaire proces op het gebied van informatiebeveiliging

	• Hij stelt de regels op voor informatiebeveiliging, houdt toezicht en toetst BIO processen en maatregelen • Hij adviseert op het gebied van informatiebeveiliging aan de Raad van Bestuur.
Information security officer (ISO)	• Is verantwoordelijk voor het implementeren en testen van de security regels en maatregelen binnen de IT infrastructuur en applicaties.
Privacy Coordinator	• Zorgt voor de beleidsvorming en beleidsbewaking op het thema privacy en is binnen Reclassering Nederland adviseur op het gebied van privacyvraagstukken.
Functionaris voor de Gegevensbescherming	• Heeft een spilfunctie vanwege haar wettelijke taak als onafhankelijk toezichthouder op de naleving van de privacy wet- en regelgeving binnen RN en is adviseur van de Raad van Bestuur.

2.3 Beleid voor medewerkers

Medewerkers hebben een belangrijke rol in de beveiliging van informatie. Hieronder wordt beschreven welke principes voor medewerkers gelden.

Medewerkers gedragen zich professioneel en verantwoordelijk. Iedere medewerker moet op de hoogte zijn van regels en richtlijnen op het gebied van informatiebeveiliging en is verantwoordelijk voor het toepassen hiervan in het dagelijks werk. Leidinggevenden zien toe op de naleving hiervan. Misbruik van bevoegdheden en het niet dragen van verantwoordelijkheid kan leiden tot disciplinaire maatregelen. Zie de gedragscode.

Reclassering Nederland heeft een programma voor beveiligingsbewustzijn. Gezien de belangrijke rol van de medewerkers heeft Reclassering Nederland een doorlopend programma voor het trainen van medewerkers en op peil houden van de kennis van informatiebeveiliging. Doelstelling van het programma is veiliger gedrag en goede naleving van de regels. De verwachting is dat zich dit vertaald in minder datalekken, een hogere alertheid van alle medewerkers en een beter meldgedrag van verdachte situaties.
Het Programma valt onder de verantwoordelijkheid van de CISO. Uitgangspunten van het programma zijn:

- Het programma is meetbaar
- Alle medewerkers volgen het programma
- Het programma bevat in ieder geval de onderdelen: meting, e-learning en phishing simulatie.

Ook 'bijzondere' medewerkers zoals ingehuurde personen, tijdelijke krachten, promovendi, afstudeerders en stagiaires moeten bekend zijn met wat Reclassering Nederland van hen verwacht en welke taken en verantwoordelijkheden zij hebben.

Bovenstaande is verder uitgewerkt in de gouden regels voor informatiebeveiliging welke te vinden zijn in bijlage 3. Het Digiplein is de belangrijkste bron van informatie rond informatiebeveiliging. Het bevat o.a. het informatiebeveiligingsbeleid van Reclassering Nederland en de gouden regels voor informatiebeveiliging (hiervan is de laatste versie op het intranet beschikbaar,)

2.4 Beleid voor toegang tot informatie

Het beheersen van toegang is een belangrijke pijler in het beveiligen van informatie en systemen. Het classificeren van informatie zorgt mede voor de criteria op basis waarvan toegang wordt toegekend

Classificatie
Classificeren is het systematisch indelen in categorieën van de waarde van informatie, om te kunnen bepalen welk niveau van beveiliging de informatie nodig heeft. **Reclassering Nederland classificeert gegevens om daarmee het beveiligingsniveau en gepaste toegangsrechten**

te kunnen toekennen. Het beveiligingsniveau wordt uitgedrukt aan de hand van de Basis beveiligingsniveaus (BBN) uit de BIO[2]. De BIO bevat een set aan technische en organisatorische normen en maatregelen die gebaseerd is op het ISO 27002 normenkader. De BIO bestaat uit 3 basisniveaus en ieder niveau bevat een uitbreiding ten opzichte van het niveau daaronder.

Reclassering Nederland hanteert de volgende 3 classificaties[3]:

1 **Openbaar**: alle informatie die openbaar gemaakt (mag) worden. Voorbeeld is een jaarverslag en andere onderwerpen die op de externe website staan.
2 **Niet openbaar**: Hieronder valt alle bedrijfs- en management informatie die niet openbaar gemaakt worden.
3 **Reclassering Vertrouwelijk** : hieronder vallen persoonsgegevens van cliënten zoals strafrechtelijke persoonsgegevens en bijzondere persoonsgegevens. Ook vallen hieronder de (bijzondere) persoonsgegevens van medewerkers en andere personen waarmee RN samenwerkt. Specifieke bedrijfs- en management informatie die extra gevoelig zijn en afscherming nodig hebben vallen hier ook onder.

Toegang tot informatie
Hierbij wordt onderscheid gemaakt in de validatie (identificatie en authenticatie) van rechtmatige toegang en het verstrekken van de rechten (autorisatie).

Ten behoeve van het identificeren en authentiseren heeft een gebruiker een persoonlijke en exclusieve gebruikersnaam en is een veilig(sterk) wachtwoord vereist, en in geval wanneer een grotere zekerheid omtrent de identiteit vereist is, 2 factor authenticatie.

Rechten dienen te worden verstrekt nadat identificatie en authenticatie heeft plaatsgevonden. In iedere regio is een door de Regiodirecteur gemandateerde aanvrager aangewezen die aanvragen autoriseert. Hierbij geldt het noodzakelijkheidsbeginsel : **Reclassering Nederland kent alleen de rechten toe die noodzakelijk zijn voor het uitvoeren van de werkzaamheden ("need to know").** De rechten zijn vastgelegd in profielen die afgestemd zijn op de functie**.** De classificatie van de informatie speelt hierbij als volgt een rol**:**

1. Openbare gegevens: Uitgangspunt hierbij is dat de informatie wordt gedeeld met de buitenwereld.
2. Niet openbare gegevens: Uitgangspunt is dat de toegang wordt beperkt tot de afdeling of unit. Ook delen met de gehele organisatie (bijv op intranet) is een mogelijkheid indien noodzakelijk.
3. Reclassering Vertrouwelijke gegevens. Uitgangspunt hierbij dat deze alleen toegankelijk zijn voor gebruikers die de gegevens nodig hebben voor de uitoefening van hun functie.

Voor het beheersen van autorisaties heeft Reclassering Nederland een autorisatiebeheer proces ingericht. Dit proces zorgt ervoor dat rechten conform beleid worden toegekend en zo snel mogelijk worden ingetrokken na functiewisseling of uitdiensttreding.

Toegang door leveranciers
Wanneer leveranciers op locatie of op afstand beheerwerkzaamheden verrichten aan systemen van Reclassering Nederland **is het noodzakelijk dat begeleiding of monitoring plaatsvindt. Tevens dienen de medewerkers van de leverancier in bezit te zijn van een Verklaring Omtrent het Gedrag (VOG) en een geheimhoudingsverklaring te ondertekenen**.

---

[2] De gehele ICT infrastructuur (netwerk, werkplek, shares, email) is ingedeeld **op BBN2 niveau,** afzonderlijke applicaties kunnen beveiligd worden op BBN 1 niveau afhankelijk van de classificatie. BBN3 is niet van toepassing binnen Reclassering Nederland

[3] Staatsgeheim geclassificeerde informatie ontbreekt in het overzicht omdat deze niet voorkomen bij Reclassering Nederland en het begrip "Reclassering vertrouwelijk" komt overeen met "departementaal vertrouwelijk" niet goed past. Voorgeschreven in de BIO is het labelen van geclassificeerde informatie (voorzien van een kenmerk). Dit gebeurt nog niet binnen reclassering en is voorzien om in de toekomst in te voeren.

Archivering (bewaartermijnen)
Papieren stukken van de afdeling Bestuursondersteuning worden bewaard in het historisch archief in Den Bosch. Het historisch archief bevat geen cliëntendossiers noch digitale informatie.

De Huidige informatievoorziening is volledig digitaal en deze gegevens (o.a. netwerkmappen, email en IRIS) worden opgeslagen in het datacenter. Hiervan worden periodiek back-ups gemaakt welke 7 jaar bewaard en daarna vernietigd worden.

In tabel in bijlage 5 is de relatie tussen de classificaties, toegang en beveiligingsmaatregelen en bewaartermijnen weergegeven.

2.5 Beleid en regels voor applicaties en infrastructuur

Informatiebeveiliging wordt vanaf het begin meegenomen (Security by design)
Informatiebeveiliging begint al bij het bedenken en uitwerken van plannen en projecten. Al in een vroeg stadium moet rekening gehouden worden met informatiebeveiliging (Security by design), of het nu gaat om nieuwe samenwerkingsverbanden met derden, het wijzigen van bedrijfsprocessen of het ontwikkelen van nieuwe informatiesystemen.

Het interne netwerk wordt niet vertrouwd. Bij werkplekconcepten binnen Reclassering Nederland wordt geen onderscheid (meer) gemaakt naar netwerkvertrouwensniveau. Dit betekent dat devices op een zelfde niveau worden beveiligd wanneer gebruikt op beveiligde interne netwerken als daarbuiten.

Segmentatie. Reclassering Nederland past (virtuele) netwerksegmentatie toe om impact van een hack of verstoring te beperken en te vertragen. Hierbij worden minimaal de volgende segmenten aangebracht:

- Een desktopomgeving voor gebruikers
- Een desktopomgeving voor beheerders
- Back end omgeving voor servers (onderverdeeld in diverse afzonderlijke virtuele omgevingen)

Versleuteling. Verkeer naar applicaties of portalen (data in transport) die zich buiten het RN datacentrum bevinden dient end tot end encrypt te zijn met minimaal met TLS 1.2. Verkeer van interne webapplicaties wordt ook standaard versleuteld.

Voor data in rust gelden geen specifieke eisen t.a.v. de encryptie, alleen dat wachtwoorden, active directory en private keys versleuteld dienen te zijn te zijn.

Ten aanzien van data opgeslagen bij een cloudprovider geldt dat deze data versleuteld dienen te zijn en bij voorkeur de private keys in beheer bij Reclassering Nederland. Indien dit niet het geval is dient de cloudprovider technische en logische maatregelen te treffen voor beveiliging van de private keys van Reclassering Nederland.

Evenwichtige balans tussen preventieve en repressieve maatregelen Niet alles valt te voorkomen. Reclassering Nederland streeft naar een gezonde balans tussen het voorkomen dat incidenten plaatsvinden en het adequaat reageren op verschillende soorten incidenten.

Kwetsbaarhedenmanagement
Informatiebeveiliging begint bij een actueel overzicht van de primaire en ondersteunende bedrijfsprocessen. Hiervan afgeleid is een actueel overzicht beschikbaar van alle IT componenten die ingezet worden in de bedrijfsprocessen. Reclassering Nederland heeft een proces om een actueel overzicht van alle IT componenten te behouden. Tevens wordt periodiek gescand of deze componenten kwetsbaarheden bevatten.

2.6 Beleid voor Ketenpartners en leveranciers

Reclassering Nederland komt in aanraking en werkt samen met een veelheid aan partijen: de andere reclasseringsorganisaties, opdrachtgevers, ketenpartners, leveranciers, enzovoorts. Bij het samenwerken dient voldoende aandacht uit te gaan naar beveiligingsaspecten. Meer en meer blijkt dat leveranciers via de systemen die zij leveren door hackers gebruikt worden als springplank voor een cyberaanval. Dit wordt het "supply chain" risico genoemd.
Om beveiligd te zijn tegen dit risico maakt Reclassering Nederland afspraken op het gebied van informatiebeveiliging met deze partijen.

De reclasseringsorganisaties
Iedere reclasseringsorganisatie is verantwoordelijk voor de beveiliging van de informatie behorend bij het eigen primaire proces en cliëntenbestand. Op het gebied van IT wordt een deel van IT infrastructuur en applicaties gedeeld, waarbij Reclassering Nederland verantwoordelijk is voor het beheer en beveiliging van dit gezamenlijke deel. Het betreft o.a. justitienetwerk, JUBIT opgang, IRIS, back-end servers, leeromgeving).

Reclassering Nederland levert deze gemeenschappelijke IT infrastructuur en applicaties als dienst aan de andere reclasseringsorganisaties en sluit hier een overeenkomst over af. De beveiligingseisen die gesteld worden aan deze dienst zijn gebaseerd op dit informatiebeveiligingsbeleid en hierbij is rekening gehouden met het belang van de andere reclasseringsorganisaties. De exacte scope van de diensten kan variëren en wordt nader omschreven in de overeenkomst. SVG en LDHJ&R zien toe op een juiste uitvoering en beveiliging van de door Reclassering Nederland geleverde diensten.
Reclassering Nederland ziet op haar beurt toe op een juiste uitvoering en beveiliging van de infrastructuur en applicatie die als dienst worden afgenomen (oa. justitienetwerk, Jubit internetopgang en LAN verbindingen).

De Veiligheidsketen
Reclassering Nederland is een zelfstandige stichting en legt formeel geen verantwoording af aan het ministerie van Justitie en Veiligheid op het gebied van informatiebeveiliging. Echter omdat er een grote ketenafhankelijkheid is en Reclassering Nederland diensten afneemt van MinJ&V en taakorganisaties volgt Reclassering Nederland zo veel mogelijk centraal beleid en stemt hierover af. O.a. door deelname aan de CISO-Board van MinJ&V en afstemming bij specifieke samenwerking met taakorganisaties en door periodiek J&V hierover te informeren (via VMR en jaarrapport).

Inkoop
Bij inkoop van diensten dient informatiebeveiliging afdoende aandacht te krijgen en altijd in de overeenkomst tussen Reclassering Nederland en de wederpartij te worden afgedekt. Indien sprake is van verwerking van persoonsgegevens wordt ook een verwerkingsovereenkomst gesloten (en dient een DPIA uitgevoerd te worden). Het aandacht geven dient te gebeuren bij de aanbestedingsuitvraag of offertevergelijking. Het is de bedoeling de beveiligingseisen in (Programma van Eisen) op te nemen, maar dient ook plaats te vinden in de fase van onderhandeling en contractvorming. Er is vanuit de CISO een lijst met standaardeisen en maatregelen voor leveranciers beschikbaar gesteld, tevens is een selectietool beschikbaar voor het bepalen van de eisen in maatwerk situaties. Diegene, onder wiens verantwoordelijkheid Reclassering Nederland een overeenkomst met een derde partij aan gaat, ziet hier op toe. Bovenstaande is meer in detail beschreven in het inkoopproces.

Tijdens levering
De (gedelegeerd) opdrachtgever voor de dienst (contracthouder) controleert en beoordeelt het niveau van de dienstverlening periodiek. Hij ziet er op toe dat de derde partij formeel gemaakte afspraken die betrekking hebben op informatiebeveiliging naleeft en dat de derde partij informatiebeveiligingsincidenten en problemen goed afhandelt. Hiertoe draagt hij zorg voor een goede relatie met de dienstverlenende partij en verifieert hij steekproefsgewijs of de andere partij afspraken nakomt. De (gedelegeerd) opdrachtgever onderneemt terstond passende actie wanneer door Reclassering Nederland manco's in de dienstverlening worden waargenomen. Als hiertoe aanleiding is initieert de opdrachtgever een onafhankelijke audit of pentest.

2.7 Beleid ten aanzien van clouddiensten

Clouddiensten zijn een bijzondere vorm van IT dienstverlening en zorgen voor specifieke risico's op het gebied van informatiebeveiliging. Reclassering Nederland verwacht in 2023 een cloudstrategie te hebben opgesteld, maar maakt in de praktijk reeds gebruik van enkele publieke clouddiensten (o.a. het P&O systeem). Gezien ontwikkelingen zoals cloud only is het te verwachten dat Reclassering in de toekomst meer gebruik gaat maken van publieke clouddiensten. Recent voorbeeld is de kantoorautomatisering van Microsoft (o.a. Office365 en Teams) die alleen als clouddienst beschikbaar is.

Een eventueel private Cloud initiatief van Reclassering Nederland volgt dezelfde regels en voorwaarden als een publieke clouddienst aangevuld met specifieke eisen.

Publieke Clouddiensten. Kenmerken van publieke clouddiensten zijn:

- commerciële partij is eigenaar
- klanten delen de diensten
- kosten worden per gebruikseenheid in rekening gebracht
- hoge schaalbaarheid en toepassing van cloudtechnologie
- dataopslag buiten het eigen datacenter.

Rijkscloudbeleid

Reclassering volgt het Rijkscloud beleid dat in juni 2022 is gepubliceerd. Hierin wordt in principe toegestaan departementaal vertrouwelijk gerubriceerde informatie ("vertrouwelijk" volgens de classificatie van Reclassering Nederland) in een Publieke clouddienst onder te brengen. Voor bijzondere persoonsgegevens geldt echter een zwaardere beleidsverplichting. Voor deze gegevens wordt **in principe géén** gebruik gemaakt van publieke clouddiensten, tenzij aantoonbaar aan eisen en voorwaarden is voldaan.

Voorwaarden

Wanneer Reclassering gebruik maakt van een publieke clouddienst dient aan de volgende voorwaarden voldaan te worden:

- Er dient een relevante risico afweging gemaakt te worden en het besluit dient te passen binnen de risico bereidheid van reclassering en getoetst te worden door de FG van reclassering
- Wanneer strafrechtelijke en bijzondere persoonsgegevens verwerkt worden dient een DPIA uitgevoerd te worden
- Er dient een actueel overzicht te zijn van alle public clouddiensten
- Het derden beleid voor inkoop en tijdens levering dient gevolgd te worden. Dit houdt in dat een quickscan informatiebeveiliging uitgevoerd dient te worden of de selectietool toegepast dient te worden voor het bepalen van informatiebeveiligingseisen
- Alle opslag en verwerking van persoonsgegevens vindt verantwoord plaats conform geldende privacy vereisten, waaronder:
  o opslag en verwerking binnen de Europese Economische Ruimte (EER), of
  o in landen waarvoor een adequaatheidsbesluit bestaat
- Er dient altijd een 'exit strategie' opgenomen te zijn in de overeenkomst met de Cloud leverancier. Hierin staat hoe, bij beëindiging van de overeenkomst, data wordt overgedragen en hoe wordt geregeld dat data bij de leverancier vernietigd wordt
- Indien mogelijk wordt gebruik gemaakt van de Trusted Cloud van J&V.

Laagdrempelige public clouddiensten en apps

Reclassering Nederland volgt het beleid voor Rijksambtenaren om apps afkomstig van landen met een offensieve cyberstrategie niet toe te staan op werk mobiele devices en prive devices die voor werk gebruikt worden.
Laagdrempelige clouddiensten zijn goedkope (of gratis) publieke clouddiensten die zonder de inkoopprocedures te volgen door medewerkers zijn aan te schaffen. Voorbeelden zijn We transfer, Datumprikker en Dropox. Deze diensten niet toegestaan, maar in bepaalde gevallen wordt uitzondering verstrekt door CISO en FG, nadat beoordeling en toetsing heeft plaatsgevonden (o.a Trello en Mural en what's app zijn goedgekeurd. Gebruik is alleen toegestaan onder de uitdrukkelijke voorwaarde dat geen cliëntgegevens en persoonsgegevens van medewerkers of overige vertouwelijke informatie worden verwerkt.

2.8 Continuïteitsbeleid

Het tijdig kunnen herstellen van een calamiteit zoals een cyberaanval of grote verstoring is cruciaal voor de continuïteit van Reclassering Nederland. Om hier op voorbereid te zijn treft Reclassering Nederland maatregelen zoals herstelplannen en continuïteitsoefeningen. Reclassering Nederland volgt het IT continuïteitsbeleid van MinJ&V en gebruikt de templates van het ministerie van JenV. Business Continuïteit in breder verband zoals ontruimingsplannen valt buiten de scope van het IB-beleid.

Continuïteitseisen
Als startpunt voor het bepalen van het niveau van de continuitsmaatregelen voert Reclassering Nederland Business Impact Analyses (BIA's) uit voor de primaire processen. De uitkomst van de BIA's worden beschreven aan de hand van de Recovery Time Objective (RTO) en Recovery Point Objective (RPO). Bij de BIAs worden vertegenwoordigers uit het operationele proces betrokken en worden de uitkomsten ter goedkeuring aan de Directie voorgelegd.

Herstelplannen
In het IT herstelplan worden de maatregelen en processen beschreven waarmee de continuïteit hersteld wordt in geval van een calamiteit.
In de plannen staat dat Reclassering Nederland beschikt over twee locaties met centrale IT-infrastructuur: het primaire datacentrum en de "uitwijkomgeving" Reclassering Nederland heeft gekozen voor een zogenaamde "passive standby" waarbij eerst aanvullende handelingen verricht moeten worden om de systemen over te kunnen schakelen. Daarnaast heeft Reclassering Nederland restoreplannen om data te kunnen herstellen.

Oefening
Om de werking van de herstelplannen te kunnen evalueren wordt jaarlijks een uitwijk oefening, restore oefening en crisismanagement oefening gedaan. In de oefening wordt getest of aan de RTO en RPO voldaan kan worden.

2.9 Beleid voor Logging en Monitoring

Systeemeigenaren houden toezicht op het veilig gebruik van informatie en informatiemiddelen. Het niet naleven van informatiebeveiligingsregels, -richtlijnen en/of -maatregelen kan resulteren in het opleggen van sancties door het daartoe bevoegde management.

Logging en monitoring
Reclassering Nederland registreert (logt) en monitort het gebruik van haar informatiesystemen, waaronder IRIS en de e-mailvoorziening, en de internetaansluiting. (zie het juridisch kader controle logging voor verdere uitwerking). Hierin is aangegeven welke gebeurtenissen minimaal gelogd dienen te worden.

Door de logbestanden regelmatig te (laten) controleren of automatisch te analyseren, kunnen inbreuken op de beveiliging worden ontdekt. Ook datalekken worden gesignaleerd of juist uitgesloten dat er een datalek is geweest. Het controleren van logging is zowel een verplichting uit de BIO als ook de AVG.

Controle van loggings kan geautomatiseerd door middel van SOC (Security Operating Center) functionaliteit of handmatige controle plaatsvinden. Reclassering beschikt op dit moment niet over SOC functionaliteit maar streeft er naar gefaseerd de infrastructuur en kritieke applicaties aan te sluiten op de SOC dienst van Min J&V.

Vanuit de verantwoordingsplicht in de AVG is het noodzakelijk een proces in te richten voor het controleren van logbestanden van systemen die persoonsgegevens bevatten. Voor IRIS is een proces voor het handmatig controleren van logbestanden geimplementeerd , voor andere systemen nog niet. De logbestanden in Iris worden net zo lang bewaard als de cliëntinformatie zelf.

Voor logging van Internet en email-gebruik is een protocol vastgesteld. [4]

3. Proces en beheersing

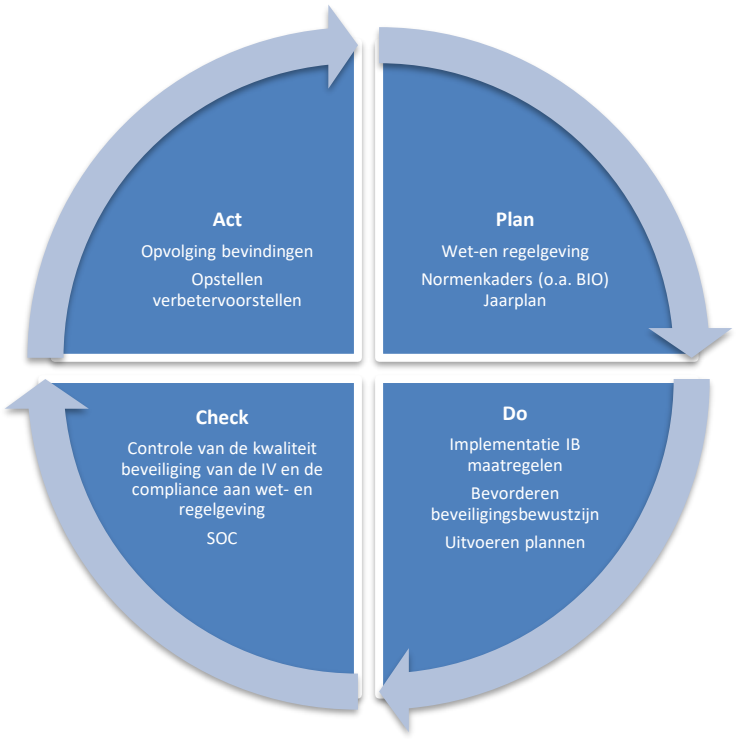
Informatiebeveiliging is geen eenmalige activiteit maar een continue verbeterproces. Het proces voor het beheersen van (de inrichting van) informatiebeveiliging is opgezet conform de BIO

De risico bereidheid van Reclassering Nederland is "Voorzichtig". Dit houdt in dat Reclassering Nederland in beperkte mate risico wil nemen, waarbij als randvoorwaarde geldt dat Reclassering Nederland aan wet- en regelgeving voldoet. Elke beveiligingsmaatregel moet in een proportionele verhouding staan tot (de omvang van) het te beheersen risico. De beheersing van risico's wordt methodisch in kaart gebracht en vastgelegd. De verantwoordelijk voor risicomanagement ligt bij eigenaren van primaire processen en systemen.

Reclassering Nederland heeft de ambitie om NBA volwassenheidsniveau 3 te bereiken en behouden. Hiervoor volgt Reclassering Nederland een groeimodel en heeft een IB-beheerproces ingericht met een Plan-Do-Check-Act cyclus. Dit houdt o.a. in dat processen en werkinstructies worden vastgelegd en de werking wordt getoetst. De uitvoering van de PCDA cyclus wordt vastgelegd (bij voorkeur in een GRC Tool)

3.1 Continue proces

Het doel van dit proces is middels een kwaliteitscyclus (Plan-Do-Check-Act) de ontwikkeling en positie van informatiebeveiliging in de organisatie te borgen.



Figuur 2 PDCA-cyclus informatiebeveiliging Reclassering Nederland

- **Plan**: De cyclus start met het informatiebeveiligingsbeleid, gebaseerd op wet- en

[4] Zie protocol Internet en email

regelgeving, landelijke normen zoals de Baseline Informatiebeveiliging Overheid (BIO) en 'best practices', uitgewerkt in regels voor onder meer informatiegebruik, bedrijfscontinuïteit en naleving. Planning geschiedt op jaarlijkse basis en wordt indien nodig tussentijds bijgesteld.

Jaarlijks stelt de CISO samen met het team Privacy een privacy- en informatiebeveiligingsplan (jaarplan) op. Het privacy- en informatiebeveiligingsplan bevat in elk geval een opsomming van de beveiligingsactiviteiten die het afgelopen jaar zijn uitgevoerd en die in het betreffende jaar zullen worden uitgevoerd.

Naast maatregelen die voorkomen uit de BIO bestaat het informatiebeveiligingsplan uit activiteiten die voortkomen uit:

- Verbeteracties die volgen uit incidenten (datalekken, beveiligingsincidenten)
- Verbeteracties die volgen uit audits
- Verbeteracties die volgen uit anderszins gesignaleerde risico's.

- **Do**: Het informatiebeveiligingsbeleid en de informatiebeveiligingsplannen uitvoeren. Er is nadrukkelijk aandacht voor beveiligingsbewustzijn. Aan het begin van een project worden de security eisen voor ontwikkeling of de in te kopen dienst opgesteld. Tevens wordt aan het begin van een project een risicoanalyse uitgevoerd en een project start architectuur inclusief een informatiebeveiligingsparagraaf opgesteld. Dit zorgt er voor dat beveiligingsmaatregelen goed passen in het ontwerp en een afgewogen niveau van beveiliging wordt gerealiseerd (door security by design en risicomanagement). **Pas toe of leg uit ("Comply or explain")** Alleen om gegronde redenen en voor zover dat wettelijk mogelijk is, is het toegestaan af te wijken van door Reclassering Nederland vastgestelde regels en richtlijnen. De argumentatie voor deze afwijking wordt schriftelijk vastgelegd en **vraagt altijd goedkeuring van de Directie**.
- **Check**: Door middel van testen en audits wordt gecontroleerd of de beveiligingsmaatregelen de beoogde doelstellingen behalen, door:
  - het laten uitvoeren van pentesten
  - controle door een externe auditor
  - uit uitvoeren van technische scans (ISO) en het toetsen van BIO maatregelen (CISO)
- **Act**: De cyclus is rond met de uitvoering van verbeteracties die afkomstig zijn uit de controles. De cyclus is een continu proces; de bevindingen van controles zijn input voor de jaarplanning en beveiligingsplannen en het evalueren van het IB-beleid. De bevindingen worden in beginsel gerapporteerd aan het en vastgelegd (bij voorkeur in een GRC tool) en gerapporteerd aan de Directie. Voor ingrijpende verbeteracties wordt een project gestart.

3.2 Risicobeheersing

Strategische niveau
Het informatiebeveiligingsbeleid van Reclassering Nederland is mede gericht op het beheersen van risico's die Reclassering Nederland loopt door het lekken van (gevoelige) cliënt- en medewerkersinformatie en door verstoringen als gevolg van een cyberaanval. Dit soort incidenten kunnen leiden tot grote operationele verstoringen, reputatieschade, financiële schade en overtredingen van wet- en regelgeving.

Voor het opstellen en updaten van dit informatiebeveiligingsbeleid wordt periodiek een strategische risicoanalyse uitgevoerd (zie bijlage 4).

Operationeel niveau

Reclassering Nederland heeft een proces en methode (afkomstig van MinJ&V) om op operationeel niveau risico's te beheersen. Hierin zijn eigenaren van processen en systemen verantwoordelijk voor het beheersen van informatiebeveiligingsrisico's die zich voordoen in systemen en processen. Tools die hiervoor gebruikt worden zijn de Quickscan Informatiebeveiliging en overzicht restrisico's en maatregelen (IRAM2). Indien sprake is van verwerking van (bijzondere) persoonsgegevens dient een DPIA uitgevoerd te worden voor een (nieuw) proces, systeem of applicatie.

Tevens wordt een project start architectuur document opgesteld welke een informatiebeveiligingsparagraaf bevat (security by design). Het is aan de eigenaar van een informatiesysteem en/of gegevensverzameling en om te beslissen welk rest-risico acceptabel is, mits passend binnen de risicobereidheid van Reclassering Nederland. Eventuele substantiële restrisico's worden vastgelegd (bij voorkeur in een GRC tool) en ter goedkeuring voorgelegd aan de Directie. Het beheersen van risico's dient te voldoen aan de risico bereidheid van reclassering Nederland

3.3 Beveiligingsincidenten

Definitie
Onder beveiligingsincidenten verstaat Reclassering Nederland geconstateerde dan wel vermoede aantasting van de vertrouwelijkheid, integriteit en/of de beschikbaarheid van informatie of informatievoorzieningen alsmede situaties die het ontstaan van een aantasting in de hand werken.

Reclassering Nederland merkt de volgende gebeurtenissen aan als beveiligingsincident:

1. Een datalek op grond van de AVG (zoals gedefinieerd in het informatieblad meldplicht datalekken). Ook interne datalekken (die hoeven vanwege de mindere ernst niet gemeld te worden bij de AP) worden aangemerkt als beveiligingsincident.
2. Het lekken van overige vertrouwelijke gegevens.
3. Ongeautoriseerde toegang of misbruik van:
    a. (Informatie) systemen (ook niet geslaagde pogingen zijn een incident)
    b. Bevoegdheden en/of rechten
    c. Voorzieningen zoals e-mail, internet en accounts (wachtwoorden)
    d. Bedrijfsmiddelen zoals computers, laptops en informatiedragers
    e. Beveiligde ruimten
4. SOC JenV meldingen over CVE kwetsbaarheden.
5. Cyberaanvallen in de vorm van o.a. phising, DDOS, ransomware.
6. Verlies of diefstal van informatiedragers of mobiele apparatuur.
7. Alle vormen van fraude inclusief identiteitsfraude.
8. Het niet naleven van de regels op het gebied van informatiebeveiliging.

Melding, registratie en afhandeling
Het is van belang dat medewerkers informatiebeveiligingsincidenten melden. In de bewustwordingscampagne worden medewerkers gewezen op het belang van het melden van incidenten of verdachte situaties. Melding maakt het mogelijk te reageren en kwetsbaarheden die tot het incident geleid hebben te verhelpen.

Melding is afhankelijk van het soort incident bij:

- Datalekken zoals bedoeld in artikel 33AVG worden gemeld bij De Autoriteit Persoonsgegevens (door tussenkomst van de Regiodirecteur en in afschrift aan de Functionaris Gegevensbescherming). Zie het Informatieblad Meldplicht Datalekken op Digiplein. Interne datalekken dienen te worden gemeld bij de Functionaris Gegevensbescherming.
- Overige informatiebeveiligingsincidenten worden gemeld bij de Servicedesk en of CISO. Zie de gouden regels voor informatiebeveiliging op Digiplein.

Registratie

Datalekken worden vastgelegd in het register datalekken. De Overige informatiebeveiligingsincidenten worden vastgelegd in het servicedesk systeem. Alle beveiligingsincidenten worden op periodieke basis gerapporteerd aan de Directie.

Afhandeling
IT gerelateerde beveiligingsincidenten worden bij de servicedesk gemeld en afgehandeld volgens het reguliere incidentenproces. Datalekken worden afgehandeld door het betreffende organisatie onderdeel, bijgestaan door de Functionaris gegevensbescherming en of ander lid van het privacy team.

Ernstige IT gerelateerde informatiebeveiligingsincidenten (bijv. een acute kwetsbaarheid met hoog risico) worden afgehandeld volgens de P1 procedure. De coördinatie van een P1 security incident ligt bij de CISO.

Wanneer een informatiebeveiligings incident (ook een datalek) leidt tot een calamiteit of crisis wordt het crisismanagement team van Reclassering Nederland geactiveerd. Indien de crisis of calamiteit impact heeft op 1 of meer onderdelen uit de JenV keten wordt dit gemeld aan het SOC JenV en de CISO JenV.

3.5 Overlegstructuur en verantwoording

Er is geen specifieke overlegstructuur voor IV of IT security onderwerpen binnen Reclassering Nederland of in 3RO verband. Afhankelijk van context (ter afstemming/besluitvorming) en scope (RN/3RO) worden IT security onderwerpen ter besluitvorming geagendeerd in 1 van de volgende overleggen:

RN overleggen
- Het Directieoverleg (tactische onderwerpen, Besluitvormend)
- Het Landelijk operationeel overleg: Operationeel directeur, regiodirecteuren, bestuurssecretaris (operationele/tactische onderwerpen, regio overstijgend)

3RO overleggen
- Het 3RO Directie Overleg (3RO directeuren, 3RO Bestuurssecretaris ->strategische onderwerpen, besluitvormend)

3.6 Relatie met andere documenten

Dit document is gebaseerd op de Baseline Informatie Beveiliging Overheid (BIO 2019) en de Algemene Verordening Gegevensbescherming (AVG). Reclassering Nederland hanteert de BIO als een baseline voor informatiebeveiliging.

Daarnaast volgt Reclassering Nederland het geldende beleid op het gebied van informatiebeveiliging dat afkomstig is van het ministerie van Justitie en Veiligheid. Afwijking hiervan is mogelijk mits dit onderbouwd wordt (Comply or Explain).
Het informatiebeveiligingsbeleid is uitgewerkt in onderliggende documenten met concrete richtlijnen en maatregelen zie *figuur 1*. , zoals (niet uitputtend):

- Gedragscode Reclassering Nederland
- Privacybeleidskader 2017
- Jaarplan Informatiebeveiliging en Privacy
- Gouden regels informatiebeveiliging
- Gebruiksvoorwaarden ICT-middelen.
- Werkinstructies.
- Dienstverleningsafspraken met derden.
- Herstel plannen.
- Wachtwoordbeleid J&V.

- Continuïteits- en herstelmaatregelen J&V.
- Pentestbeleid

Bijlage 1: Relevante wet- en regelgeving

De volgende wet- en regelgeving en besluiten zijn met oog op informatiebeveiliging relevant voor reclasseringsinstellingen:

- Nederlandse Grondwet (artikel 10)
- Europees Verdrag voor de Rechten van de Mens (artikel 8)
- Reclasseringsregeling 1995
- Uitvoeringsregeling Reclassering Nederland 2005
- Algemene Verordening Gegevensbescherming (AVG)
- CAO Reclassering Nederland
- Wet Justitiële en Strafvorderlijke Gegevens en het daaruit voortvloeiende Besluit Justitiële gegevens
- Wet identiteitsvaststelling verdachten, veroordeelden en getuigen
- Auteursrecht (Burgerlijk Wetboek)
- Aansluitbeleid Justitienet3 / JN DepV (maart 2013)
- eIDAS Uitvoeringswet 2018

Bijlage 2: Definities

Authenticatie: Het verifiëren van de identiteit van een persoon of zaak, aan de hand van met de identiteit verbonden kenmerken, zoals een wachtwoord en/of fysieke kenmerken.

Beschikbaarheid: Het waarborgen dat vanuit hun functie geautoriseerde gebruikers op de juiste momenten tijdig toegang hebben tot informatie en aanverwante bedrijfsmiddelen (informatiesystemen).

Betrouwbaarheid: De mate waarin de organisatie zich kan verlaten op een informatiesysteem voor zijn informatievoorziening, ter ondersteuning van een of meer afhankelijke bedrijfsprocessen.

Calamiteitenplan: opsomming van alle maatregelen welke tot uitvoering moeten komen als zich een situatie voordoet waarbij de beschikbaarheid, integriteit en/of vertrouwelijkheid van een informatiesysteem in beduidende mate niet aan de eisen voldoen.

(Beveiligings)Incident: Geconstateerde dan wel vermoede aantasting van de vertrouwelijkheid, integriteit en/of de beschikbaarheid van informatie of informatievoorzieningen alsmede situaties die het ontstaan van een aantasting in de hand werken.

Derde: Een andere organisatie, niet Reclassering Nederland zelf.

Externe: Persoon die ten behoeve van Reclassering Nederland werkzaamheden verricht zonder persoonlijke arbeidsovereenkomst (zoals medewerkers in dienst bij leveranciers en (keten)partners, uitzendkrachten, freelancers en ZZP'ers) en overige personen die formeel met toestemming gebruik maken van faciliteiten van Reclassering Nederland.

Gebruiker: Elk persoon die voor de uitvoering van zijn taken werkt met middelen van Reclassering Nederland - waaronder informatie en informatiesystemen - en hiertoe bevoegd is. Denk aan vaste en tijdelijke medewerkers, externen, medewerkers Leger des Heils en SVG, stagiaires/ afstudeerders, enzovoorts.

Informatiebeveiliging: Het proces van vaststellen van de vereiste betrouwbaarheid van informatiesystemen in termen van vertrouwelijkheid, beschikbaarheid en integriteit alsmede het treffen, onderhouden en controleren van een samenhangend pakket van bijbehorende maatregelen.

Informatiesysteem: Een samenhangend geheel van gegevensverzamelingen, en de daarbij behorende personen, procedures, processen en programmatuur alsmede de voor het informatiesysteem getroffen voorzieningen voor opslag, verwerking en communicatie.

Integriteit: Het waarborgen van de juistheid, volledigheid en tijdigheid van informatie en de verwerking ervan.

Leidinggevende: Iemand die door formeel daartoe te zijn aangesteld in haar of zijn werk leiding geeft aan een of meer anderen.

Medewerker: Persoon die ten behoeve van een organisatie werkzaamheden verricht via een arbeidsovereenkomst voor bepaalde of onbepaalde duur.

Organisatie: Instelling, instantie, orgaan, bedrijf, onderneming, vereniging, stichting of ander samenwerkingsverband gericht op het via middelen, activiteiten en processen realiseren van een of meer doelstellingen.

Risico: De kans (waarschijnlijkheid) dat een onzekere gebeurtenis zich in een gegeven periode en situatie zal voordoen vermenigvuldigd met de directe en indirecte gevolgen van die gebeurtenis.

Risicobeheer: Het systematisch inventariseren, beoordelen en door het treffen van maatregelen beheersbaar maken van risico's en kansen die het bereiken van de doelstellingen van een organisatie bedreigen dan wel bevorderen.

Samenwerkingsverband: Geheel van onderlinge afspraken met betrekking tot samenwerking tussen organisaties en/of personen.

Vertrouwelijkheid: Het waarborgen dat informatie alleen toegankelijk is voor degenen die hiertoe zijn geautoriseerd. Het gaat hier onder meer om het beveiligen van de toegang tot de gebouwen, informatiesystemen en de ICT-infrastructuur tegen onbevoegden (hackers en andere indringers) en malafide software (virussen, Trojan horses e.d.). Maar ook om maatregelen om te voorkomen dat medewerkers van Reclassering Nederland toegang krijgen tot informatie die niet voor hen is bedoeld.

Bijlage 3: Gouden regels voor informatiebeveiliging

Gouden regels
Dit zijn de gouden (gedrags) regels voor informatiebeveiliging die voor alle medewerkers gelden:

1 **– Gebruik de door de werkgever verstrekte en voorgeschreven middelen voor het uitvoeren van je werk**
De (Thuis) werkplek van Reclassering en het Justitienetwerk bieden een solide beveiligingsniveau. Dit geldt ook voor de verstrekte mobiele apparatuur in combinatie met mobile iron. Maak in aanvulling daarop gebruik van de ICT middelen zoals **Zivver** en Webex (op termijn Teams) wanneer dat vereist is om Reclasserings informatie te versturen naar je prive- email of op te slaan op prive apparatuur.

2 – Sla informatie veilig op
Sla clientgegevens alleen op in IRIS. Overleg met je leidinggevende wat het beste alternatief is wanneer dit niet mogelijk is. Het is niet toegestaan om informatie van Reclassering op te slaan in publieke clouddiensten zoals dropbox bijvoorbeeld.

3 – Raadpleeg alleen clientgegevens die noodzakelijk zijn voor de uitvoering van je werkzaamheden
Het feit dat je clientgegevens kunt raadplegen, betekent niet automatisch dat dit in alle gevallen toegestaan is. Leidend is of je de gegevens nodig hebt voor de uitvoering van je taak. Wees je hier zelf van bewust en vul de reden van raadpleging in wanneer je wel noodzaak hebt maar geen autorisatie.

4 - Neem zo weinig mogelijk informatie(dragers) mee
Weeg de noodzaak tegen de risico's af voordat documenten worden meegenomen buiten kantoor. Neem uitsluitend de informatie mee die noodzakelijk is voor het bezoek en houd de documenten binnen handbereik. Houd de periode dat de informatie buiten kantoor verblijft zo kort mogelijk.

5 **- Wachtwoorden en pincodes zijn strikt persoonlijk**
Het wachtwoord en pincode dient uitsluitend om persoonlijk toegang te krijgen tot systemen. Geef het niet aan collega's (dus ook niet aan een medewerker van de ICT afdeling of aan een collega die jouw taken overneemt tijdens je vakantie) en bewaar ze gescheiden van elkaar op een veilige plek, dus niet in een agenda of op een geel briefje. Gebruik eventueel een wachtwoordtool (zie voor meer uitleg onder de ICT maatregelen en tips)

6 **- Houd rekening met wie meeluistert of meekijkt**
Werken gebeurt op kantoor, thuis en in openbare gelegenheden. Houd er in alle situaties rekening mee dat anderen kunnen meeluisteren met telefoongesprekken of kunnen meelezen op beeldschermen.

7 **- Wees alert op misleiding**
Wees ervan bewust dat mensen kunnen proberen met verkeerde bedoelingen informatie af handig te maken. Bijvoorbeeld via de telefoon of door middel van een phishing mail. (zie meer uitleg hierover bij de ICT maatregelen en tips)

8 **- Vergrendel de pc**
Zet, bij het voor korte tijd verlaten van de werkplek, de scherm vergrendeling aan (Windows + L), berg vertrouwelijke informatie op in een afsluitbare kast of locker en meld je af van de systemen. Laat ook geen documenten achter en laat geen aantekeningen achter op het whiteboard of flipover.

9 **- Begeleid bezoek en spreek onbekende personen aan**
Bezoekers worden opgehaald en weer teruggebracht naar de receptie. Laat bezoekers niet onbegeleid door het pand lopen. Spreek onbekende personen aan, stel jezelf voor en vraag of hij of zij hulp kan gebruiken.

***10* – Je toegangspas is strikt persoonlijk**
Als medewerker van Reclassering Nederland ontvang je een toegangspas. Deze is strikt persoonlijk Leen hem niet uit en laat hem niet onbeheerd achter. Vermeld vermissing direct .

***11* - Meld beveiligingsincidenten**
Meld een datalek zoals verlies of diefstal van vertrouwelijke persoonsgegevens direct bij je leidinggevende (zie de pagina incidenten en datalekken op Digiplein). Meld verlies van iPad, laptop of smartphone direct bij de leidinggevende. . Meld ICT gerelateerde zaken zoals verdachte mails, sms'jes of telefoontjes, waarschuwingsmeldingen op je scherm, verlies van wachtwoorden direct bij de Servicedesk.

***12* - Houd je aan de regels en spreek elkaar aan op onveilig gedrag**.
Als medewerkers van Reclassering Nederland zijn wij er met elkaar verantwoordelijk voor dat wij zorgvuldig en integer werken. Neem daarom je eigen verantwoordelijkheid op het gebied van (informatie)beveiliging. Het is ook belangrijk dat je je collega's durft aan te spreken op onveilig gedrag.

Bijlage 4: Strategische risicoanalyse

Totaal inherent cyber risk	**51**
Risicoscore	Medium risico

	Dashboard – Uitkomsten cyberrisico's		
	Naam organisatie:	**Reclassering**	**Nederland dd 23-03-2023**
	Categorie:	**Score:**	**Waardevolle standaarden:**
1	Organisatie & Governance	**6**	U lijkt zicht te hebben op uw governance en organisatie risico's en de beheersing daarvan.
2	Gedrag & Cultuur	**4**	U lijkt uw risico's t.a.v. gedrag en cultuur niet volledig te kennen en te beheersen. De normen van NIST v1.1 04.2018, ISACA Cybercrime Audit/ Assurance Program 2016 en Cloud Security Alliance v3.0.1 03.2019 bieden hier handvatten voor.
3	Waardeketen (stakeholders) versus risico's	**7**	U lijkt uw risico's t.a.v. waardeketen en stakeholders niet volledig te kennen en te beheersen. De normen van ISO/IEC 27032, DNB 58 Controls en PCI/DSS V3.2.1 bieden hier handvatten voor.
4	Inzicht in technologielandschap	**4**	U lijkt uw risico's t.a.v. technologielandschap niet volledig te kennen en te beheersen. De normen van NIST v1.1 04.2018, ISO/IEC 27032, ISACA Cybercrime Audit/ Assurance Program 2016 en DNB 58 Controls bieden hier handvatten voor.
5	Wet- en regelgeving	**8**	U lijkt zicht te hebben op uw wet- en regelgeving risico's en de beheersing daarvan.
6	Detectie	**6**	U lijkt uw risico's t.a.v. detectie niet volledig te kennen en te beheersen. De normen van PAS 555, NIST v1.1 04.2018, ISO/IEC 27032, ISACA Cybercrime Audit/ Assurance Program 2016, DNB 58 Controls,PCI/DSS V3.2.1 en CIS v7.1 04.2019 bieden hier handvatten voor.
7	Reactie	**5**	U lijkt uw risico's t.a.v. reactie niet volledig te kennen en te beheersen. De normen van NIST v1.1 04.2018, ISACA Cybercrime Audit/ Assurance Program 2016 en PCI/DSS V3.2.1 bieden hier handvatten voor.
	Overall cyber risico score (1 – 10)	**6**	

Bijlage 5: Tabel Classificatie en maatregelen

Classificatie	Toegang (in applicaties en shares)	BBN	Maatregelen	Bewaartermijn
Niet openbaar -Gevoelige Management en Stafinformatie -Gewone persoonsgegevens van medewerkers die in bepaalde gevallen breder gedeeld moeten worden (calamiteitenlijst)	de toegang wordt beperkt tot de afdeling of unit. Indien noodzakelijk is delen met de hele organisatie (bijv op intranet) toegestaan	BBN2/BBN1	-Bij voorkeur Zivver	7 jaar
Openbaar Overige informatie, zoals nieuwsberichten of algemene regelingen en kennis en instructies	Informatie is zo veel mogelijk toegankelijk en wordt gedeeld met de gehele organisatie	BBN1		5 jaar
Reclassering Vertrouwelijk Dit betreft persoonsgegevens zoals beschreven in de AVG: - **strafrechtelijke gegevens** - **bijzondere persoonsgegevens** van cliënten en medewerkers (zoals gezondheidsgegevens en gegevens m.b.t. ras of religie) en - **gewone persoonsgegevens** (naam, adres , telefoonnummer, emailadres)	alleen toegankelijk voor gebruikers die de gegevens nodig hebben voor de uitoefening van hun functie	BBN2 (departem taal vertrouwelijk)	- Veilige email (justitienetwerk en Zivver) -moet voldoen aan de AVG Leveranciers: VOG Begeleiding	7 jaar