



INTERN VERTROUWELIJK

Informatieveiligheid Beleid Project 27223

TLP – GREEN

Rubricering / classificatie & merking

Rubricering / classificatie:

Aanvullende merking: Geen

Rubricering specifiek:

Duur (tot): Ntb

Datum vaststelling: Ntb

Vaststeller: Projectmanager RVB

Document

Titel: Informatieveiligheid Beleid Project 27223

Datum: 3 maart 2026

Status: definitief

Versienummer: 1.1

Colofon

Projectgegevens:

Projectnaam	Nieuwbouw cellencomplex Kavel M PI Vught
Projectnummer	27223
Organisatie	Rijksvastgoedbedrijf Postbus.rvb.PIVught@rijksoverheid.nl

Verantwoordelijk:

Rol:	Naam:	Functie:
Eigenaar	Postbus.rvb.PIVught@rijksoverheid.nl	IPV-er 27223
Verantwoordelijke	Postbus.rvb.PIVught@rijksoverheid.nl	BVA BZK

wijzigingen beheer:

Datum	Versie			
4-2-2026	1.0			
<u>3-3-2026</u>	<u>1.1</u>	<u>tekstueel</u>		

Akkoordverklaring:

Datum	Versie	Naam:	Functie	Paraaf
4-2-2026	1.0			

Inhoud

1	Nieuwbouw cellencomplex Kavel M PI—56
2	Uitgangspunten Informatieveiligheid—67
2.1	Eisen wet- en regelgeving—67
2.2	Scope/reikwijdte & afbakening: Project 27223—67
2.3	Uitgangspunt Informatiebeveiliging binnen het project/programma—67
3	Inrichting van informatiebeveiliging—89
3.1	Organisatorische project inrichting—89
3.1.1	Niveaus—89
3.1.2	Rollen, taken, verantwoordelijkheden en bevoegdheden—910
3.2	Rubricering van informatie binnen het project—910
3.2.1	CAL / RAL van toepassing op het project/programma—910
3.2.2	Rubriceringsverantwoordelijkheden—1011
3.2.3	Screeningvereisten per rubriceringsniveau—1011
3.3	PDCA cyclus (per niveau)—1112
3.3.1	Specifieke onderwerpen waar PDCA cyclus wordt toegepast—1112
4	Uitvoering—1213
4.1	Leveranciersmanagement—1213
4.1.1	Risicoprofielen—1213
4.1.2	IB leveranciersvoorwaarden—1314
4.1.3	Bezoek locatie en informatiebeveiliging—1314
4.2	Incidentmanagement—1314
4.2.1	Definities—1314
4.2.2	Melden van incidenten—1415
4.3	Werkbezoeken, open dagen en rondleidingen—1415
4.4	Bewustwording en on-/offboarding—1415

Bijlage 1	20250217 Algemene CAL-DJI-normaal beveiligd – def; Vastgesteld 3 februari 2025
Bijlage 2	Organisatie IB binnen project
Bijlage 3	Bouwplaats beveiliging - IB aspecten
Bijlage 4	Specifieke onderwerpen waar PDCA cyclus wordt toegepast
Bijlage 5	Operationele uitwerking Informatieveiligheid en veilig samenwerken, Project 27223

1 Nieuwbouw cellencomplex Kavel M PI

Binnen het uitvoeren van projectwerkzaamheden voor de Dienst Justitiële Inrichtingen (DJI) afdeling Facilitaire Zaken, Huisvesting en Inkoop (FHI) is werken met gevoelige informatie eerder regel dan uitzondering. Daarom is het van groot belang dat zorgvuldig wordt omgegaan met informatie, informatiesystemen en informatieprocessen. Verlies of verandering van informatie heeft binnen het werkveld van DJI grote gevolgen voor DJI, maar ook voor de maatschappij. Daarnaast draagt zorgvuldig omgaan met informatie bij aan de goede naam van de Dienst Justitiële Inrichtingen en de relatie met de uitvoerende partijen die in opdracht van DJI en het Rijksvastgoedbedrijf de projecten adviseren, begeleiden en uitvoeren.

Het Rijksvastgoedbedrijf (RVB) heeft in 2025 de opdracht gekregen middels het ondertekenen van de PID voor de realisatie van een nieuw cellencomplex op Kavel M in PI Vught. Aansluitend zijn middels de door DJI verstrekte CAL (Classificatie Aanduiding Lijst; bijlage 1) de informatieclassificaties en rubriceringen vastgesteld. Dit informatieveiligheid-Beleidsplan (IBP) is project specifiek opgesteld voor project 27223.

Het gaat hierbij met name om de bepaling welke kaders van toepassing zijn en de wijze waarop dit in de praktijk wordt toegepast.

Operationele uitwerking van de informatieveiligheid en de principes van het veilig samenwerken is uitgewerkt in:

Bijlage 5 Operationele uitwerking Informatieveiligheid en veilig samenwerken.

2 Uitgangspunten Informatiebeveiliging

In dit hoofdstuk wordt nader ingegaan op de geldende wet- en regelgeving, scope en afbakening van project 27223 en de uitgangspunten van informatiebeveiliging binnen het project 27223.

2.1 Eisen wet- en regelgeving

Dit informatiebeveiliging beleid is in lijn met het informatiebeveiliging beleid van het Rijksvastgoedbedrijf (RVB) en is vormgegeven naar de geldende wet- en regelgeving op het gebied van de beveiliging van (bijzondere) informatie, te weten:

- Voorschrift Informatiebeveiliging Rijksdienst Bijzondere Informatie 2025 (VIRBI 2025¹);
- Voorschrift Informatiebeveiliging Rijksdienst 2007 (VIR 2007²);
- Baseline Informatiebeveiliging Overheid 2 (BIO2)

Voor het beveiligen van informatie binnen het project worden verder de volgende uitgangspunten in acht genomen:

- De door de Dienst Justitiële Inrichtingen, directie FHI, opgestelde CAL is leidend in het vaststellen van de classificatie en rubricering van de gehanteerde informatie, bijlage 1
- Informatiebeveiliging is een lijnverantwoordelijkheid.
- Informatiebeveiliging is een continu verbeterproces ('Plan-do-check-act').
- De selectie van beveiligingsmaatregelen gebeurt risico gebaseerd.
- Bij uitwisseling van informatie wordt deze voorzien van Traffic Light Protocol v2.0 (TLP v2.0³) markering.

2.2 Scope/reikwijdte & afbakening: Project 27223

Dit beleid is van toepassing op het gehele project 27223. Dit betekent dat alle organisaties die projectinformatie verwerken zoals, maar niet uitsluitend, opdrachtgevers, gebruikers, opdrachtnemers, aannemers en leveranciers dit beleid moeten uitvoeren.

Het beleid geldt voor het gehele proces van informatievoorziening binnen het project, ongeacht de toegepaste technologie.

Het uitgangspunt voor het project dat alle informatie publiek is, tenzij dit betreft:

- Informatie zoals benoemd in de CAL;
- Commercieel/intern vertrouwelijke informatie;
- Persoonsvertrouwelijke informatie;
- Informatie welke van rechtswege niet geopenbaard mag worden.

Indien de informatie valt onder de uitzondering "tenzij" dan moet deze conform de BIO en, indien van toepassing de VIRBI, worden beschermd.

2.3 Uitgangspunt Informatiebeveiliging binnen het project/programma

Gezien het belang van het beveiligen van informatie in zijn algemeenheid, onafhankelijk van de gevoeligheid van individuele delen van die informatie, wordt er binnen het project/programma uitgegaan van het "Need-To-Know" principe. Het "Need-To-Know" principe houdt in dat individuen alleen toegang krijgen tot die informatie die noodzakelijk is voor het kunnen uitvoeren van de aan het individu

¹ <https://wetten.overheid.nl/BWBR0051482/2025-09-09>

² <https://wetten.overheid.nl/BWBR0022141/2007-07-01>

³ <https://www.first.org/tlp/docs/v2/tlp-v2-nl.pdf>

opgelegde rol. Dit principe is daarmee een beperking ten opzichte van het uitgangspunt dat een individu op basis van criteria zoals screeningsniveau automatisch toegang zou mogen krijgen tot informatie met een bepaalde classificatie of rubricering.

Door het "Need-To-Know" principe toe te passen wordt informatie alleen functioneel gedeeld, waardoor het risico dat informatie collectie en stapeling hiervan kan leiden tot onbedoelde kennis aggregatie verminderd.

3 Inrichting van informatiebeveiliging

In dit hoofdstuk wordt nader ingegaan op de organisatorische inrichting van het project (waaronder de governance en de PDCA), de classificatie-/rubriceringsrichtlijnen (/afspraken) en de verantwoordingslijnen.

3.1 Organisatorische project inrichting

3.1.1 Niveaus

Conform het VIR 2007 is informatiebeveiliging een lijnverantwoordelijkheid. Dat betekent dat eenieder binnen het project binnen zijn eigen verantwoordingsgebied (project c.q. (project)deel) verantwoordelijk is voor de beveiliging van informatie.

Bij de inrichting van de projectorganisatie worden 3 niveaus onderkend. Hieronder wordt per niveau de verantwoordelijkheden uiteengezet:

Niveau	Onderdeel	Verantwoordelijkheden
0	Steller rubricering; Dienst Justitiële Inrichtingen directie FHI.	- Stellen rubricering en classificatie middels CAL
1	Project; Rijksvastgoedbedrijf	- Inrichting governance. - Opstellen beleid voor het project/programma. - Opstellen vereisten aan opdrachtnemers. - Managementrapportages over het onderdeel informatieveiligheid.
2	Opdrachtnemers	- Opstellen en implementeren van Informatieveiligheid beleid om te kunnen voldoen aan de gestelde eisen. - Toezien op de correctie navolging van het beleid, zowel binnen de eigen organisatie als bij door de leverancier ingehuurde onderaannemers en leveranciers. Voor hoofdaannemers, eventueel per deelproject, tevens: - Opstellen en implementeren bouwplaatsbeveiligingsplan (BBP) specifiek voor informatiebeveiliging.

3.1.2 Rollen, taken, verantwoordelijkheden en bevoegdheden

De gedetailleerde uitwerking van de rollen, taken, verantwoordelijkheden en bevoegdheden van de niveaus is opgenomen in bijlage 2 van dit beveiligingsbeleid.

3.2 Rubricering van informatie binnen het project

Binnen het project worden uitsluitend de volgende classificaties en/of rubriceringen toegepast:

Niveau	Definitie
Openbaar	Openbaar
Intern ALGEMEEN	Alle RVB/Rijks- collega's mogen het weten, óók commerciële inhuur
Intern VERTROUWELIJK	De schade kan door het RVB, haar klanten/gebruikers beheerst worden, géén opschaling naar ministerie
Departementaal VERTROUWELIJK	Kennisname door niet geautoriseerde kan schade toebrengen aan de belangen van <u>één of meerdere ministeries</u> .

Middels classificatie aanduiding lijsten (CAL) en/of rubricering aanduiding lijsten (RAL) wordt de juiste classificatie of rubricering vastgesteld. In volgende paragrafen wordt dit nader uitgewerkt.

Noot: terminologie vanuit de wet- en regelgeving wordt gehanteerd. De maatregelen verbonden aan deze rubricering zijn weergegeven in onderhavig document.

3.2.1 CAL / RAL van toepassing op het project/programma

Het Rijksvastgoedbedrijf (RVB) heeft de rol van uitvoerende partij bij het project voor de opdrachtgever, de Dienst Justitiële Inrichtingen (DJI) afdeling Huisvesting, Facilitaire zaken en Inkoop (FHI). Bij de uitvoering van dit project houdt het RVB tijdens de projectuitvoering rekening met de te beschermen belangen en ziet er ook op toe dat de betrokken participanten bij de werkzaamheden zich hieraan houden.

De opdrachtgever heeft een CAL vastgesteld, in deze CAL wordt per type informatie het niveau van classificeren, rubriceren en eventueel merken aangegeven wat gehanteerd dient te worden.

Een CAL c.q. RAL is gebaseerd op het actueel ondervonden dreigingsniveau. Wijziging in het dreigingsniveau kan aanleiding zijn om de respectievelijke aanduiding lijst daarop aan te passen.

3.2.2 Rubriceringsverantwoordelijkheden

De verantwoordelijkheden voor opstellen, vaststellen en nakomen van rubriceringsvereisten is weergegeven in onderstaande schema:

Onderdeel	Verantwoordelijkheden
BVA / IBF van de opdrachtgever (DJI)	<ul style="list-style-type: none"> Opstellen van een CAL
Project (RVB)	<ul style="list-style-type: none"> Aanwijzing en mandatering van rubriceringsambtenaren⁴. Vertaling CAL naar praktisch gebruik. Toezen op correcte rubriceringsvoorstellen. Vaststellen rubricering. Afstemmen met BVA bij specifieke vraagpunten qua toepassing.
Opdrachtnemers/participanten	<ul style="list-style-type: none"> Toepassing van classificaties en/of voorstellen van rubricering bij het maken van documenten als opsteller volgens VIRBI 2025. Voorstellen doen op het gebied van het de-rubriceren van informatie. Organiseren wijze van gebruik/opslag en delen van informatie (inclusief de ketenpartijen).

3.2.3 Screeningvereisten per rubriceringsniveau

Voorwaarden om toegang tot bijzondere informatie te verkrijgen zijn als volgt:

Niveau	Definitie
Intern VERTROUWELIJK en hoger	<ul style="list-style-type: none"> Verklaring omtrent gedrag (VOG) bij aanvang werkzaamheden niet langer dan 1 jaar eerder afgegeven. Jaarlijks dient nieuwe VOG te worden overlegd. Medewerker van de projectorganisatie dient te beschikken over een VOG met het screeningsprofiel; 'medewerker hoofdkantoor met specifieke informatie'. Medewerker die uitvoeringswerkzaamheden op de justitiële locatie gaat verrichten dient te beschikken over een VOG met het screeningsprofiel; 'medewerker inrichting'. Ondertekende geheimhoudingsverklaring. Een model geheimhoudingsverklaring wordt beschikbaar gesteld door de project/programmamanager van het RVB.

⁴ Projectmanager en diens plaatsvervanger zijn gemandateerd als rubriceringsambtenaar. Aanwijzing geschiedt middels nota "Aanwijzing Rubriceringsambtenaar" welke op voorspraak van de BVC/BVA door de SG wordt vastgesteld.

3.3 PDCA cyclus (per niveau)

Informatiebeveiliging is een continu verbeterproces ('Plan-Do-Check-Act'), alle niveaus zijn binnen het project primair zelf verantwoordelijk voor het opzetten en doorlopen van een PDCA-cyclus. Hieronder wordt per cyclusonderdeel, per niveau, de activiteiten beschreven:

Cyclus	Niveau	Activiteit
Plan	Niveau 1: Project	Opstellen beleid: <ul style="list-style-type: none"> • Informatieveiligheid beleid project (incl. governance) • Autorisatie systeemtoegang • Classificatie / Rubricering • Onboarding/ offboarding • Bewustwordingsprogramma • Incidentmanagement • Auditprogramma
	Niveau 2: Opdrachtnemers	<ul style="list-style-type: none"> • Informatieveiligheid beleid per leverancier voortvloeiend uit ketenverantwoordelijkheid (leveranciersvoorwaarden) + presentatie IB voor nieuwe leveranciers • Risico-profiel (definiëring + toepassing) leveranciers • Statement of Compliancy (SoC) • Onderwerpen maandelijks overleg aannemers • Auditprogramma
Do	Niveau 1: Project	<ul style="list-style-type: none"> • Onboarding nieuwe medewerkers • Risico-analyse IB per complexdeel + programma • Handreiking: rubricering + workshop • Melden en afhandelen van incidenten • Uitvoeren bewustwordingsacties (kalender)
	Niveau 2: Opdrachtnemers	<ul style="list-style-type: none"> • IBP documenten beoordeling/ acceptatie projectmanager • Maandelijks overleg met participanten per complexdeel (vaste onderwerpen) • Handreiking: rubricering voor aannemers, architecten, adviseurs en overige participanten. • Bewustwordingsacties naar leveranciers
Check	Niveau 1: Project	<ul style="list-style-type: none"> • Toetsen: inrichting/autorisaties, uitvoeren screening, toepassen juiste rubricering
	Niveau 2: Opdrachtnemers	<ul style="list-style-type: none"> • Audits bij leveranciers + verslaglegging verbeteringen • Statement of Compliancy (SoC)
Act	Niveau 1: Project	<ul style="list-style-type: none"> • Bijstellen van beleid en verbeteringen voorstellen na uitvoeren cyclus
	Niveau 2: Opdrachtnemers	<ul style="list-style-type: none"> • Verbeteringen voorstellen na uitvoeren van cyclus

3.3.1 Specifieke onderwerpen waar PDCA cyclus wordt toegepast

Voor de verschillende onderwerpen die van toepassing zijn voor het project is er per onderwerp een PDCA cyclus gedefinieerd. Deze cycli zijn in bijlage 4 opgenomen.

4 Uitvoering

In dit hoofdstuk worden de onderwerpen die relevant zijn bij de uitvoering van project/programma toegelicht.

4.1 Leveranciersmanagement

4.1.1 Risicoprofielen

De toepassing van informatiebeveiliging is risico gebaseerd. Voor de opdrachtnemers wordt gewerkt met verschillende risicoprofielen die in de onderstaande tabel staan opgesomd.

Per opdrachtnemer wordt op basis van de gevoeligheid van de informatie waar opdrachtnemer mee werkt en/of de werkzaamheden die zij uitvoert, een risicoprofiel toegekend. Het risicoprofiel dat van toepassing is bepaald daarmee de impact en de mate van de maatregelen van het project/programma op deze opdrachtnemers.

Mag toegang krijgen tot / gebruiken van			
Risico profiel	Openbare informatie	Intern VERTROUWELIJK	Dep.V informatie
Top	Ja	Ja	Ja
Midden	Ja	Ja	Nee
Geen	Ja	Nee	Nee

Overzicht van de 'maatregelen van het project/programma' die worden uitgevoerd per risicoprofiel:

	Top	Midden	Geen
Naleving IB maatregelen toetsing in het jaar	Maandelijkse bespreking: incidentmanagement; risico's, uitgevoerde audits door IBF; awareness activiteiten	Jaarlijkse bespreking: Review van alle activiteiten die in IBP zijn opgenomen.	n.v.t.
SoC (Statement of compliancy)	Jaarlijks SoC opleveren	Jaarlijks SoC opleveren.	n.v.t.
Meeting groep (betrokken IBF-en)	Gemeenschappelijk overleg organiseren – uitwisseling van ervaringen	n.v.t.	n.v.t.
Awareness activiteiten RVB - leveranciers	Deelname medewerkers aan bewustwordingsbijeenkomsten.	Deelname medewerkers aan bewustwordingsbijeenkomsten.	n.v.t.

4.1.2 *IB leveranciersvoorwaarden*

Opdrachtnemers die Dep.V informatie in hun eigen werkomgeving verwerken (downloaden, opslaan etc.) moeten een informatieveiligheid beleidsplan (IBP) opstellen dat wordt beoordeeld en geaccepteerd door de projectmanager als eindverantwoordelijke.

Periodiek wordt er een toets (al dan niet audit) uitgevoerd om te zien of de partij inderdaad de geformuleerde beheersmaatregelen heeft geïmplementeerd.

Onderdeel	Inhoud
Opleveren van (IBP)	IBP moet inzicht geven op welke wijze aan wet- en regelgeving wordt voldaan. Aspecten die cruciaal zijn is: risicomanagement, beheer van autorisaties, screening, awareness activiteiten en incidentmanagement.
Acceptatie IBP door projectmanager RVB	Bevestiging acceptatie door vastlegging in samenwerkruimte.
Informatiebeveiligingsfunctionaris (IBF) organisatie leverancier/opdrachtnemer	Binnen de organisatie van de leverancier/opdrachtnemer is IBF verantwoordelijk voor alle activiteiten op het gebied van informatiebeveiliging bij de leverancier.
Statement of Compliancy (SoC)	Jaarlijks wordt verantwoording afgelegd door de leverancier op het gebied informatiebeveiliging ten aanzien van naleving van de voorschriften.
Audit	Het RVB heeft een 'right to audit' en kan onderzoeken (laten) uitvoeren.

4.1.3 *Bezoek locatie en informatiebeveiliging*

Op het moment dat er bouwactiviteiten gaan plaatsvinden dient er een bouwplaatsbeveiligingsplan (BBP) te zijn opgesteld door de opdrachtnemer(s) en geaccepteerd door het project.

Om richting te geven aan de uitwerking van een BBP zijn in Bijlage 3 IB-gerelateerde zaken opgenomen die hierin aan de orde zouden moeten komen. Hierbij is het uitgangspunt dat in het BBP de adequate maatregelen worden getroffen op het niveau van de individuele bouwlocatie.

Mocht er op specifieke onderdelen sprake zijn van verhoogde risico's dan worden deze en passende maatregelen in het desbetreffende BBP opgenomen en geëffectueerd.

4.2 **Incidentmanagement**

4.2.1 *Definities*

Een "incident" is een gebeurtenis die de bedrijfsvoering van het RVB negatief kan beïnvloeden. Van een "informatiebeveiligingsincident" is sprake als er inbreuken zijn op de Beschikbaarheid (B), Integriteit (I) of de Vertrouwelijkheid (V).

Indien het bovenstaande van toepassing is op persoonsgegevens dan is er sprake van een "privacy incident".

Een "Near miss" is de constatering van een gebeurtenis of omstandigheid waardoor potentieel een incident zou kunnen optreden, wanneer hier geen actie op wordt ondernomen.

Het is van belang om alle gesignaleerde mogelijke incidenten tijdig te melden. Binnen project wordt gebruik gemaakt van de volgende classificaties:

Classificatie	Omschrijving	Incident	Near Miss
RC1	Ernstige impact	Incident waarbij Dep.V informatie gelekt is	Risico met potentie tot het lekken van Dep.V informatie
RC2	Beperkte impact	Incident waarbij geclassificeerde informatie gelekt is	Risico met potentie tot het lekken van geclassificeerde informatie niet zijnde Dep.V informatie
RC3	Matige impact	Overige incidenten met IB aspect	Overige risico's met IB aspect

4.2.2 *Melden van incidenten*

Uitgangspunt: Opdrachtnemer dient beveiligingsincidenten met betrekking tot de beschikbaarheid, integriteit en/of vertrouwelijkheid van (bijzondere) informatie per ommegaande, maar uiterlijk binnen 24 uur na kennis te hebben genomen van het incident, te melden bij de opdrachtgever en verleent daarbij alle medewerking aan het mogelijk onderzoeken en oplossen van deze incidenten.

Processtappen voor incidentmelder:

- Bij het constateren van een Informatiebeveiligingsincident is het eerste belang het beperken van de gevolgen. Denk hierbij aan het blokkeren van bestanden, het onklaar maken van verdwenen apparatuur of het afsluiten van inlog mogelijkheden.
- Maak melding van het incident.
- Betreft het een incident met een risico classificatie RC1, neem dan altijd direct telefonisch contact op met de IBF en eventueel projectmanager.

Escalatielijnen

Incidenten met een risico classificatie RC1 worden gemeld aan de BVC (BeveiligingsCoördinator) RVB.

4.3 **Werkbezoeken, open dagen en rondleidingen**

De principes 'Need-To-Know' en 'need to be' vormen hier de basis. Waarbij werkbezoeken voor gekenden zijn. Open dagen en rondleidingen zijn met derden (niet gekenden).

Voor werkbezoeken met gekenden krijgt iemand alleen de informatie die nodig is om een bepaalde taak uit te voeren. Ook als degene(n) vanuit zijn functie meer informatie zou mogen zien. Dit dient verder uitgewerkt te worden in het Bouwplaats BeveiligingsPlan

4.4 **Bewustwording en on-/offboarding**

Door alle nieuwe medewerkers, zowel RVB personeel als extern ingehuurd, die binnen het project/programma komen te werken wordt een verplichte onboarding doorlopen. Hierbij wordt ingegaan op o.a. de onderwerpen: informatie veiligheid en beveiliging, gebruik social media, classificatie, rubricering, TLP protocol en praktische toepassing en persoonlijk veiligheid t.a.v. delen van informatie.

Bij de offboarding worden alle accounts met toegang tot informatiesystemen geblokkeerd. Van de vertrekkende medewerkers wordt verwacht dat zij de informatie archiveren



Rijksvastgoedbedrijf
Ministerie van Volkshuisvesting en
Ruimtelijke Ordening

INTERN VERTROUWELIJK

Informatieveiligheid Beleid Project 27223

TLP – GREEN

Rubricering / classificatie & merking

Rubricering / classificatie:

Aanvullende merking: Geen

Rubricering specifiek:

Duur (tot): Ntb

Datum vaststelling: Ntb

Vaststeller: Projectmanager RVB

Document

Titel: Informatieveiligheid Beleid Project 27223

Datum: 3 maart 2026

Status: definitief

Versienummer: 1.1

Bijlage 2: *Organisatie IB binnen project/programma*

Niveau	Rol	Activiteiten
1	Project / programma manager	<ul style="list-style-type: none"> - Opstellen IB Beleid voor het project/programma Screeningsbeleid, Autorisatiebeleid Systeemtoegang en Rubriceringsbeleid. - Uitvoeren IB Risicomanagement, waaronder toezicht op het uitvoeren van een RA (Risico Analyse) op programma. - Opstellen van Managementrapportages over het onderdeel IB (per kwartaal, i.o.m. de stakeholders CISO en BVC). - Opstellen van IB vereisten aan opdrachtnemers. - Onderhouden van contacten met de BVA van de gebruiker(via de BVC RVB). - Onderhouden van contacten met de BVC RVB en CISO RVB. - Aansturen van IBF op het gebied van IB. - Toezicht houden op de autorisaties toegang tot informatiesystemen. - Uitvoeren van het onboardings- en offboardingsproces. - Toezien op correcte toepassing van rubricering en classificering informatie op basis van de CAL/RAL.
2	IBF	<ul style="list-style-type: none"> - Verantwoordelijk voor de operationele uitvoering van Risicomanagement, waaronder een halfjaarlijkse RA specifiek op het gebied van informatiebeveiliging binnen het complexdeel. - Verantwoordelijk voor het bepalen van prioritering inzake de uit te voeren audits en toezien op voldoen aan compliancy op gebied van de relevante wet- en regelgeving bij leveranciers. - Opvolgen van de auditbevindingen. - Toezien dat alle leveranciers die daartoe verplicht zijn een IB beleid opleveren (op basis van de BIO + indien van toepassing VIRBI) dat voldoet aan de gestelde voorwaarden. - Toezien op juiste autorisaties toegang tot informatiesystemen voor complexdeel. - Toezien dat de screening juist wordt uitgevoerd (VOG, GHV en indien noodzakelijk VGB). - Verantwoordelijk voor de operationele uitvoering van incidentmanagement, waaronder maandelijks doornemen incidenten + Prio 1 en 2 bespreken. - Uitvoeren van de rol van de rubriceringsambtenaar binnen het complexdeel en toezien dat de juiste rubricering wordt toegepast.

	Contractmanager	<ul style="list-style-type: none"> - Zorgdragen dat in de contractvoorwaarden van alle leveranciers is opgenomen dat ze aan de vereiste IB moeten voldoen (IBP opleveren, goedkeuren, audits). - Leveranciersselectie en afsluiten van contracten namens het RVB met opdrachtnemers.
	Project assistent (PA)	<ul style="list-style-type: none"> - Toekennen en intrekken van autorisaties toegang tot informatiesystemen (met ondersteuning van functioneel beheer) per complexdeel voor leveranciers en andere betrokken partijen. - Screening: verzamelen en bijhouden de screeninggegevens van alle medewerkers van een complexdeel. - Opvragen van SoC bij opdrachtnemers (jaarlijks). - Periodiek toetsen informatie geplaatst in Samenwerkingsruimte / Document Management System (DMS). Filenet / archivering. - Coördineren / toetsen van de autorisaties in, registratie van screeninggegevens.
3	Leveranciers	<p><i>In de ontwerpfase, in de onderzoeksfase en in de realisatiefase zijn dat met name architecten, betrokken adviseurs enerzijds en hoofd- en onderaannemers.</i></p> <ul style="list-style-type: none"> - Opstellen Informatie Beveiligingsplan (IBP) - Acceptatie verkrijgen van IBP door Opdrachtgever - Toepassen van informatiebeveiliging op basis van geaccepteerd IBP; - Aanwijzen IB Functionaris (IBF); - Faciliteren van IB audits door RVB <p>Voor (hoofd)aannemers per (complex/bouw)deel tevens:</p> <ul style="list-style-type: none"> - Opstellen en implementeren BBP (specifiek voor informatiebeveiliging)

Bijlage 3: *Bouwplaatsbeveiliging – IB aspecten*

Categorie middelen	Onderwerp	Beheersmaatregel	Type maatregel	Korte beschrijving
Fysieke toegang tot bouwlocatie/ zone op bouwlocatie	Toegang tot de bouwlocatie (fysieke toegangsbeveiliging) – afgeschermdde omgeving	Toegangspasbeheer	Preventief	Alleen medewerkers die gescreend zijn (VOG en GHV) krijgen een toegangspas tot de bouwlocatie. Daarnaast moeten ze ook nog de nodige beveiligingscertificaten in het bezit hebben
	Zonering op de bouwplaats en toegang tot deze plekken	Aparte toegang (alleen VGB gescreende medewerkers) - beveiligger checkt toegang tot deze bijzondere ruimte	Detectief	Op de bouwlocatie is bekend in welke zone alleen VGB gescreende medewerkers mogen komen voor hun werkzaamheden (installaties in de bijzondere ruimte waarbij locatie bekend is); Ook installeren van gebouwelementen met Stg C informatie op specifieke locatie in het gebouw (o.a. kozijnen, beglazing, deuren etc.)
Medewerkers	Medewerkers op de bouwplaats	Onboarding nieuwe medewerkers	Preventief	Onboarding (pasbeheer, screening, instructie/ gedragsregels, werkplek toewijzing etc.) Offboarding (bij vertrek rechten intrekken + inleveren van passen) Instructies op bouwplaats inzake na te leven gedragsregels
Bouwmaterialen	Bouwmaterialen en installaties in RAL als Dep.V aangeduid worden afgeleverd en moeten geplaatst worden	Installatie door gescreende medewerkers	Preventief	Installatie werkzaamheden door gescreende medewerkers die enerzijds de Dep.V informatie weten maar ook de locatie in het gebouw
Werkplek op bouwlocatie	Gebruik van middelen op de bouwplaats	Specifieke locatie voor inzien van informatie	Detectief	Georganiseerd dat er bepaalde werkplekken zijn waar informatie kan worden ingezien op de bouwlocatie. Informatie – maximaal dep V kan ook in afgesloten kasten worden opgeborgen (ook clean desk toepassing).
IT middelen gebruik	IT middelen mogen worden gebruikt (BIM Look) om digitale tekeningen te kunnen raadplegen (zo min mogelijk papier gebruiken)	Digitaal benaderen van tekeningen/ informatie	Preventief	Mogelijk gebruik van mobiele telefoon maar geen autorisatie om foto's te maken
Informatie	Gebruik/ opslag van informatie op de bouwplaats	Opslag kast documenten	Preventief	Documenten die naderhand alsnog gebruikt kunnen worden worden opgeslagen in een kast in de buurt van de werkplek (bouwkeet)

Bijlage 4: *Specifieke onderwerpen waar PDCA cyclus wordt toegepast*

Onderwerp	PDCA – cyclus	
Onboarding/ offboarding	Plan	Beleid op het gebied van het Onboarden en offboarden van medewerkers (inclusief proces met screening + autorisaties toegang tot informatiesystemen)
	Do	Geven van presentaties voor nieuwe medewerkers; medewerkers uit dienst exit stappen doornemen
	Check	Toetsen of alle nieuwe medewerkers per periode introductie project/programma hebben doorlopen. Dit geldt ook voor de vertrekkende medewerkers m.b.t afsluiten autorisaties + opschonen/ archiveren mail en documenten
	Act	Aanpassen van beleid c.q. proces n.a.v. ervaringen
Risicomanagement informatieveiligheid	Plan	Risicomanagement beleid
	Do	Uitvoering van een risico analyse + definiëring/ uitvoeren beheersmaatregelen
	Check	Toetsen management rapportage op juiste weergave en wel of geen toprisico
	Act	Verbeteren van analyse/ samenwerking

TLP - GREEN

Intern vertrouwelijk | Definitief | Informatieveiligheid Beleid Project 27223 | 3 maart 2026

Screening – VOG, GHV en VGB-B	Plan	Screeningbeleid project/programma, proces van aanvraag GHV, VOG en indien van toepassing aanvraag VGB
	Do	Uitvoeren door Project assistenten (PA) registratie + bijhouden van actualiteit
	Check	Toetsen actualiteit qua screening van de medewerkers per complexdeel
	Act	Indien noodzakelijk bijstellen proces
Classificeren / Rubriceren	Plan	Classificatie- / rubriceringsbeleid; bewustwordingssessie / workshop
	Do	Toepassen van classificatie / rubricering van informatie in de praktijk; advisering bij specifieke problemen
	Check	Toetsing op juiste rubricering informatie
	Act	Bijstellen classificatie- / rubriceringsbeleid
Autorisaties toegang tot informatiesystemen	Plan	Autorisatiebeleid voor toegang tot informatiesystemen (op basis van 'Need-To-Know'); proces aanvraag/toekennen en intrekken autorisaties
	Do	Inregelen van autorisaties door Project assistent bij Onboarding/ offboarding
	Check	Toetsing toegang tot informatiesystemen
	Act	Bijstellen van autorisatiebeleid of proces

Incidenten	Plan	Incidentmanagement beleid/ proces + wijze van registreren en rapporteren
	Do	Registreren en prioriteren van incidenten en zorgdragen voor afhandeling (inclusief afstemming correctieve maatregelen). Rapportage van de incidenten per maand per complexdeel en ook voor het programma
	Check	Toetsen van de registratie van incidenten bij de opdrachtnemers
	Act	Aanpassen van beleid c.q. proces
Bewustwordingsacties	Plan	Bewustwordingsplan definiëren met een kalender van alle activiteiten op dit gebied gedurende het jaar
	Do	Uitvoeren van bewustwordingsactiviteiten
	Check	Toetsen op opdrachtnemers ook voldoende bewustwordingsacties uitvoeren in hun organisatie + onderaannemers
	Act	Aanpassen beleid/acties + kalender op basis van ervaringen