



**INTERN VERTROUWELIJK**

Operationele uitwerking Informatieveiligheid  
en veilig samenwerken  
Project 27223

**TLP - GREEN**

Versienummer 1.1

Datum 3 maart 2026  
Status Definitief

Wijzigingen beheer	
Versie 1.1	datum

## Colofon

Projectnaam	Nieuwbouw cellencomplex Kavel M PI Vught
Documentkenmerk	27223
Versienummer	1.1
Projectleiders	Postbus.rvb.PIVught@rijksoverheid.nl
Contactpersoon	DG Vastgoed en Bedrijfsvoering Rijk   DGVBR-RVB- Transacties & Projecten   DGVBR-RVB-T&P-Projecten 2 Eusebiusbuitensingel 66   6828 HZ Arnhem Postbus 16169   2500 BD
Bijlage(n)	3
Auteurs	Postbus.rvb.PIVught@rijksoverheid.nl

## Inhoud

<b>1</b>	<b>Inleiding—5</b>
<b>2</b>	<b>Rollen, taken en verantwoordelijkheden—6</b>
2.1	Informatie Beveiligingsfunctionaris (IBF)—6
2.2	Interne Auditor—7
2.3	Rubriceringsambtenaar—7
2.4	Medewerkers—7
<b>3</b>	<b>Rubricering, classificatie en TLP markering—9</b>
3.1	Rubricering—9
3.2	Classificatie—10
3.3	Markering voor uitwisseling (Traffic Light Protocol)—10
3.4	Uitwerking project nieuwbouw cellencomplex Kavel M PI Vught—10
3.5	Voorwaarden TLP-markering—13
<b>4</b>	<b>Documenten en documentenbeheer—15</b>
4.1	Afspraken over informatie met TLP-markering AMBER en RED—15
4.2	Centrale opslag informatie—16
4.3	Fysieke en hardcopy informatie—16
4.4	Samenwerkingsruimte—16
4.5	Eisen toegang SWR—17
4.6	Mappenstructuur conform TLP—17
4.7	Instructies voor gebruik TLP in documenten—18
<b>5</b>	<b>Verdere Afspraken / instructies—19</b>
5.1	Fysieke beveiliging en beveiliging van de omgeving—19
5.2	Opslag informatie—19
5.3	Communicatie over het project—20
5.4	E-mail en agenda beheer—20
5.4.1	Instructies voor gebruik van TLP in berichtenverkeer, zoals e-mail—20
5.4.2	Agenda beheer—20
5.5	Gebruik sociale media—20
5.6	Divers—21
5.7	Clear screen / clear desk—21
5.8	Kantoor- thuiswerk omgeving—21
5.9	Werken op afstand (thuis of project locatie)—21
5.10	Internetverbinding—21
<b>6</b>	<b>Incidenten—22</b>
6.1	Informatie-incidenten—22
6.1.1	Meldingen—22
6.1.2	Incidenten—22
6.1.3	Handelen bij incidenten—23
6.1.4	Verantwoordelijkheid incidentmanagement—24
6.2	Veiligheidsincidenten—24
6.2.1	Melding en noodhulp buiten de PI.*—24
6.2.2	Afstemming met opdrachtgever—25
6.2.3	Gezamenlijke risicoanalyse—25
6.2.4	Evaluatie en herstel—25

## Bijlages:

- Bijlage 1 - 20250217 Algemene CAL-DJI-normaal beveiligd – def;  
Vastgesteld 3 februari 2025
- Bijlage 2 - TLP codering systematiek
- Bijlage 3 - Regels voor iedereen die bij DJI werk uitvoert, vastgesteld 26/6/2025

## 1 Inleiding

Het Rijksvastgoedbedrijf (RVB) heeft in 2025 opdracht gekregen voor de realisatie van een nieuw cellencomplex op Kavel M in PI Vught. Door de opdrachtgever, Dienst Justitiële Inrichtingen (DJI), directie Facilitaire Zaken, Huisvesting en Inkoop (FHI), is rubricering van de informatie voor dit project vastgesteld.

Naast deze rubricering is bewustwording van de omgeving waarin de werkzaamheden worden verricht in het kader van persoonlijke veiligheid van belang.

Het RVB heeft aan deze rubricering uitwerking gegeven middels het Informatieveiligheid-Beleids-Plan (IBP), de dato 4-2-2026.

De operationele kaders volgend uit dit IBP zijn vastgelegd in onderhavig document. Hierin zijn ook samenwerkingsafspraken opgenomen.

In een samenleving waarbij DJI en RVB zich bevinden is een actieve houding met betrekking tot het beschermen van informatie doorslaggevend. Alle afzonderlijke deelnemers binnen DJI-projecten moeten in het gebruik van informatie en bedrijfsmiddelen ervoor zorgen dat zij bijdragen aan de goede naam van DJI en het Rijksvastgoedbedrijf. Waken over de beschikbaarheid, integriteit en vertrouwelijkheid van informatie draagt bij aan de goede naam van DJI, Rijksvastgoedbedrijf en alle deelnemers van een specifiek DJI-project.

## 2 Rollen, taken en verantwoordelijkheden

### 2.1 Informatie Beveiligingsfunctionaris (IBF)

*Ook wel: Information Security Officer.*

De IBF van de participant houdt zich bezig met informatie veiligheid/ beveiliging voor het project op tactisch en operationeel niveau binnen haar organisatie.

De IBF is verantwoordelijk voor de dagelijkse uitvoering van het IB-beleid en het beheer van het IB-management systeem. Ook is de hij/zij degene die effectief om zal gaan met informatiebeveiligingsincidenten en het implementeren van de maatregelen om de beveiliging van informatie te waarborgen.

- Het coördineren van implementatie van het IB-beleid.
- Ondersteunen van interne en externe assessments/audits.
- Opvolging geven aan verbeteractiviteiten.
- Coördinatie bij IB gerelateerde meldingen en incidenten.
- Incident Rapportages.
- Bewaking en onderhoud van geïmplementeerde maatregelen.
- Het assisteren bij de planning en uitvoering van interne en externe audits.
- Het monitoren en begeleiden van het oplossen van bevindingen n.a.v. de interne en/of externe audit.
- Rapporteren over bovenstaande.
- Communiceert met IBF's van andere organisaties binnen het project.

Iedere organisatie binnen het project (opdrachtgever(s), opdrachtnemer(s), adviseur(s)) draagt zorg dat deze rol binnen de eigen organisatie is belegd voor het project.

## **2.2 Interne Auditor**

De controle voor de uitvoering van het IB-beleid en het IB-management systeem ligt bij de Interne Auditor. De Interne Auditor is ook verantwoordelijk voor het identificeren van mogelijke verbeterpunten in het beveiligingsbeleid.

- Controle op naleving van het IB-beleid binnen het aandachtsgebied.
- Ondersteunen van interne en externe assessments.
- Planning en uitvoering van interne audits.
- Het monitoren en begeleiden van het oplossen van bevindingen n.a.v. de interne audit.

Iedere organisatie binnen het project (opdrachtgever(s), opdrachtnemer(s), adviseur(s)) draagt zorg dat deze rol binnen de eigen organisatie is belegd voor het project.

## **2.3 Rubriceringsambtenaar**

Deze rol is juridisch vastgelegd in de VIRBI en moet door de secretaris-generaal worden toegekend. Deze rol wordt ingevuld door de projectmanager van het project.

De rubriceringsambtenaar is bevoegd tot 'het vaststellen' van de rubricering van informatie. Tevens bevoegd tot 'de-rubriceren' van (specifieke) informatie. Hierbij dient hij de rubricering en classificatie zoals die is gesteld door de DJI voor het project te borgen.

Deze rol met als scope 'het project' wordt enkel belegd binnen het RVB als eigenaar van de informatie tijdens uitvoering van project.

## **2.4 Medewerkers**

Alle medewerkers die in aanraking komen met Bijzondere Informatie:

- De naleving van het IB-beleid en daarvan afgeleide processen, procedures, richtlijnen en het IB Management systeem.
- Melden van (mogelijke) incidenten en afwijkingen.

## **Communicatie**

Het eerste aanspreekpunt voor informatiebeveiliging vormt de Informatie Beveiligingsfunctionaris (IBF) van de eigen organisatie. Hierbij heeft de IBF een

primaire rol in het toetsen of er wordt voldaan aan de informatiebeveiligingsmaatregelen zoals deze zijn opgenomen in deze informatie beveiligingsleidraad. De IBF heeft geen actieve rol in het adviseren van alle deelnemers met betrekking tot de uitvoeringsvormen van de informatiebeveiligingsmaatregelen zoals deze zijn opgenomen in deze informatie beveiligingsleidraad.



### 3 Rubricering, classificatie en TLP markering

Informatie binnen het project wordt gerubriceerd, geclassificeerd en gemarkeerd. 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 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 informatiecollectie en stapeling hiervan kan leiden tot onbedoelde kennis aggregatie verminderd. Het "Need-To-Know" principe is ook toegepast door het project/programma, waar nodig per fase, in deelprojecten op te delen die qua informatie en kennis van elkaar gescheiden zijn.

#### 3.1 Rubricering

Rubriceren is een wettelijk vastgestelde vorm van classificeren van informatie voor de Rijksoverheid. Het rubriceringsniveau wordt bepaald aan de hand van de schade die het 'leken' van deze informatie kan veroorzaken.

De rubriceringniveaus voor dit project zijn vastgesteld door de Dienst Justitiële Inrichtingen directie FHI.

Deze is vastgelegd in het volgende document, toegevoegd als bijlage:

Bijlage 1 – 20250217 Algemene CAL-DJI-normaal beveiligd – def;  
Vastgesteld 3 februari 2025

In de CAL (Classificatie Aanduiding Lijst) worden de rubriceringsniveau's aangegeven voor documenten en specifieke onderdelen van de gebouwen. Tevens bevat dit document de classificaties die niet onder de VIRBI vallen.

### 3.2 Classificatie

Welke informatie op welke wijze moet worden geclassificeerd en als zodanig worden aangeduid is vastgesteld door de Dienst Justitiële Inrichtingen directie FHI.

Deze is vastgelegd in het volgend document, toegevoegd als bijlage:

Bijlage 1 – 20250217 Algemene CAL-DJI-normaal beveiligd – def;

Vastgesteld 3 februari 2025

In de CAL worden de classificaties aangegeven voor documenten en specifieke onderdelen van de gebouwen. Tevens bevat dit document de rubriceringsniveau 's.

### 3.3 Markering voor uitwisseling (Traffic Light Protocol)

Bij uitwisseling van mogelijk gevoelige informatie moet de informatie worden voorzien van een markering volgens het Traffic Light Protocol (TLP).

De TLP-markering is aanvullend op de classificatie c.q. rubricering en markeert de wijze waarop met betreffende document mag worden omgegaan. Elk document dient voorzien te zijn van een TLP-markering.

Het Traffic Light Protocol (TLP) is ontworpen om de uitwisseling van mogelijk gevoelige informatie te bevorderen en maakt het mogelijk om effectiever samen te werken. Het uitwisselen van informatie gebeurt van een verstrekker van informatie naar één of meerdere ontvangers. TLP gebruikt vier markeringen die aangeven in hoeverre de informatie door de ontvangers verder mag worden gedeeld.

De vier TLP-markeringen zijn; RED, AMBER, GREEN en CLEAR. Binnen de CLEAR-markering gelden er geen restricties aan de verspreiding van de informatie.

Het gebruik van deze markeringen op documenten en e-mailberichten maakt de opsteller bewust van de vertrouwelijkheid en de manier waarop de informatie gedeeld kan/mag worden. De ontvanger is zich daarnaast bewust hoe met de informatie omgegaan moet/mag worden. Dit met betrekking tot doorsturen, interne verwerking/verspreiding en opslag van de informatie. De regels met betrekking tot wat wel/niet mag binnen het communiceren met de informatie moet nog nader uitgewerkt worden.

Bijlage 2 – TRAFFIC LIGHT PROTOCOL (TLP) Version 2.0;

FIRST Normdefinities en Gebruiksrichtlijnen

Vastgesteld 3 februari 2025

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

### 3.4 Uitwerking project nieuwbouw cellencomplex Kavel M PI Vught

Bij het labelen van projectinformatie dient het rubriceringsniveau of de classificatie op alle pagina's te worden vermeld en dient op alle pagina's het paginanummer en het totaal aantal pagina's en eventueel toegevoegde bijlagen te worden vermeld.

De meeste onderdelen krijgen een classificatie Intern Algemeen en Intern Vertrouwelijk. Voor een beperkt deel van de bouwonderdelen wordt de rubricering als Departementaal VERTROUWELIJK (afgekort: Dep.V) aangegeven.

De markering volgens het TLP-protocol geeft kaders en herkenbaarheid.

Voor het rubriceren en markeren van de documenten project Kavel M PI Vught wordt het volgende aangehouden.

Procesinformatie over het vastgoed – Rubricering PI Vught		
	<i>Classificatie / Rubricering</i>	<i>Markering TLP</i>
Het gehele project met alle procesinformatie over het project wordt verwerkt Intern Vertrouwelijk, met markering TLP - GREEN.	Intern Vertrouwelijk	<b>GREEN</b>
Het gehele project met alle technische vastgoed informatie over het project wordt verwerkt Intern Vertrouwelijk, met markering TLP - GREEN	Intern Vertrouwelijk	<b>GREEN</b>
Alle beveiligingsdocumenten voor PI Vught worden verwerkt Departementaal VERTROUWELIJK, met markering TLP - AMBER.	Dep.V	<b>AMBER</b>
De beveiligingsdocumenten voor beveiligingsinstallaties, zoals toegangscontrole, inbraakdetectie en cameraobservatie worden verwerkt Departementaal VERTROUWELIJK, met markering TLP – AMBER.	Dep.V	<b>AMBER</b>
De beveiligingsdocumenten voor bouwkundige beveiliging, zoals weerstandsklassen en kogelwering worden verwerkt Departementaal VERTROUWELIJK, met markering TLP - AMBER	Dep.V	<b>AMBER</b>
De beveiligingsdocumenten voor terreinvoorzieningen, zoals kabels en leidingen, omheiningen en inrichting, worden verwerkt Departementaal VERTROUWELIJK, met markering TLP - AMBER	Dep.V	<b>AMBER</b>
Specifieke beveiligingsdocumenten, geldend voor PI Vught, op aangeven van DJI	Dep.V	<b>RED</b>

Voor het benoemen van maatregelen wordt de Baseline Informatiebeveiliging Overheid, BIO, gehanteerd.

• Intern Vertrouwelijk.	Intern vertrouwelijk	<b>GREEN</b>
• Departementaal VERTROUWELIJK.	Dep.V	<b>AMBER</b>

### 3.5 Voorwaarden TLP-markering

De volgende markeringen worden toegepast met daaraan de voorwaarden gekoppeld:

**TLP: RED** Uitsluitend bestemd voor de ogen en oren van individuele ontvangers, niet voor verdere verspreiding. De volgende voorwaarden zijn hieraan gekoppeld:

- Bij een vergadering is de informatie voorbehouden aan degene die bevoegd is de informatie te ontvangen.
- De informatie wordt niet gedeeld in online besprekingen.
- De informatie wordt niet per mail verstrekt, ook niet versleuteld.
- De informatie wordt opgeslagen maar niet verwerkt binnen door het Rijksvastgoedbedrijf goedgekeurde clouddiensten. Hiervoor wordt de Samenwerkingsruimte Rijksoverheid gebruikt met een specifieke map waar een zeer beperkt aantal medewerkers binnen het project toegang toe krijgen. De informatie kan wel gecodeerd en geanonimiseerd breder opgeslagen worden in door het Rijksvastgoedbedrijf goedgekeurde clouddiensten.

**TLP: AMBER** Beperkte verspreiding, ontvangers mogen deze uitsluitend op "Need-To-Know" basis verstrekken binnen hun organisatie en ontwerpteamleden. De volgende voorwaarden zijn hieraan gekoppeld:

- Bij een vergadering is de informatie voorbehouden aan de voor het project gescreende personen die daarmee bevoegd zijn de informatie te ontvangen en bewust zijn van de voorwaarden tot delen van de informatie.
- De informatie mag gedeeld in online besprekingen, beperkt tot het gebruik van Cisco Webex.
- De informatie wordt bij voorkeur niet per e-mail verstrekt. Per e-mail is mogelijk maar enkel degelijk versleuteld (niet de standaard ZIP optie in Windows bijvoorbeeld) met gebruik van wachtwoord. Het wachtwoord wordt via een ander medium verzonden.
- De informatie kan wel binnen de Rijksoverheid via de DWR-omgeving per e-mail gedeeld worden.
- De informatie wordt of via de daartoe beschikbaar gestelde samenwerkingsruimte of wel via een secure-transfer (ODCN) gedeeld.
- De informatie mag opgeslagen of verwerkt worden binnen door het Rijksvastgoedbedrijf goedgekeurde clouddiensten zoals Samenwerkingsruimte Rijksoverheid. De informatie wordt in separate mappen opgeslagen, waarbij alleen medewerkers volgens "Need-To-Know" geautoriseerd worden. Er is een

vertegenwoordiger van het Rijksvastgoedbedrijf benoemd die de autorisaties voor de mappenstructuur goedkeurt.

**TLP: GREEN** Beperkte verspreiding, verstrekkers mogen deze informatie verspreiden binnen hun eigen organisatie en projectorganisatie. Ontvangers mogen de informatie binnen de eigen organisatie en de projectorganisatie delen, echter niet via openbaar toegankelijke kanalen. De volgende voorwaarden zijn hieraan gekoppeld:

- Bij een vergadering mag de informatie gedeeld worden met alle toehoorders mits betrokken bij het project of stakeholder organisaties.
- De informatie mag gedeeld worden in online besprekingen.
- De informatie wordt bij voorkeur niet per e-mail verstrekt. Per e-mail is mogelijk maar enkel degelijk versleuteld (niet de standaard ZIP optie in Windows bijvoorbeeld) met gebruik van wachtwoord. Het wachtwoord wordt via een ander medium verzonden.
- De informatie wordt of via de daartoe beschikbaar gestelde samenwerkingsruimte of wel via een secure-transfer (ODCN) verstrekt.
- De informatie kan wel binnen de Rijksoverheid via de DWR-omgeving per e-mail gedeeld worden.
- De informatie wordt opgeslagen of verwerkt binnen clouddiensten.

## 4 Documenten en documentenbeheer

### 4.1 Afspraken over informatie met TLP-markering AMBER en RED

- Uitgangspunt voor toegang tot de project informatie is altijd op basis van "Need-To-Know". Hiermee wordt bedoeld dat projectinformatie alleen wordt gedeeld met personen welke een actieve rol hebben binnen het project en voor hun werkzaamheden binnen het project dienen te beschikken over deze specifieke informatie.
- Binnen het project is de rol van autorisatiebeheerder aan de rubriceringsambtenaar toegewezen. De autorisatiebeheerder is verantwoordelijk voor het geven van de juiste autorisaties tot de juiste informatie en documenten. De autorisatie is gekoppeld aan het toegang beheer van de hiertoe ingerichte samenwerkingsruimte.
- Alleen die informatie wordt gedeeld die ook nodig is voor het gestelde doel. Hierbij dient de rest van de informatie verwijderd, danwel zwart gemaakt te worden in het document.
- Ook na verwijdering c.q. zwart maken van informatie blijft dezelfde classificatie, rubricering en/of TLP van kracht. Het verlagen van de rubricering (derubriceren volgens VIRBI 2025) vindt alleen plaats na goedkeuring ('vaststellen van rubricering' volgens VIRBI) door Rubriceringsambtenaar.
- Het is bekend wie welke informatie in bezit heeft en elke ontvanger van informatie is op de hoogte dat verdere verspreiding niet mag plaatsvinden. Indien iemand van mening is dat een ander deze informatie ook in zijn bezit dient te hebben dan zal dit aangevraagd moeten worden bij de Rubriceringsambtenaar. De autorisatie tot de betreffende mappen van de samenwerkingsruimte geldt als vastlegging wie welke informatie ter beschikking heeft. In de ontwerpfase is het uitgangspunt dat in verband met de integraliteit van het ontwerp de leden van het ontwerpteam over alle informatie moeten kunnen beschikken, behoudens de informatie met de markering TLP-RED.
- Opslaan van projectinformatie, ongeacht de markering, op een mobiele informatiedrager is niet wenselijk, echter indien onontkoombaar alleen toegestaan op een goedgekeurde, beveiligde USB-stick.

## **4.2 Centrale opslag informatie**

Digitale projectinformatie dient centraal te worden opgeslagen waarbij de fysieke toegankelijkheid van het opslagmedium met digitale informatie voldoende is afgeschermd en ongeautoriseerde toegang tijdig wordt gedetecteerd.

## **4.3 Fysieke en hardcopy informatie**

In eerste aanleg moet het gebruik van fysieke en hardcopy informatie zoveel mogelijk worden vermeden. Dit voorkomt onnodige blootstelling aan informatiebeveiligingsrisico's.

Het verspreiden van fysieke en hardcopy informatie zoals bijvoorbeeld rapporten, notities en tekeningen dienen tot een minimum te worden beperkt. Fysieke informatie moet altijd onder toezicht van een project werknemer worden gehouden. Hardcopy wordt zo spoedig mogelijk na verwerking op adequate wijze vernietigd (bijvoorbeeld DIN P-5 voor papier).

## **4.4 Samenwerkingsruimte**

Om informatie tussen alle afzonderlijke projectmedewerkers te delen zal het Rijksvastgoedbedrijf voorzien in een centrale opslag van informatie. Hiervoor wordt gebruik gemaakt van de Samenwerkingsruimte (SWR).

Het versturen van informatie geschiedt op twee manieren:

- Intern informatie delen via hyperlink vanuit de Samenwerkingsruimte.
- Extern informatie delen via beveiligde lokale filetransfer applicatie zoals bv Cryptshare of Secure Transfer via de Rijkscloud

Wanneer gevoelige informatie binnen het project moet worden gedeeld, is het gebruik van een hyperlink vanuit de samenwerkingsruimte de veilige manier. Hyperlinks kunnen alleen worden geopend door project werknemers welke beschikken over de juiste multi factor authentication (MFA).

Om de hoeveelheid informatie op de samenwerkingsruimte overzichtelijk te houden wordt in overleg met het ontwerpteam deze voorziening vormgegeven.



### *Gebruik Samenwerkingsruimte*

Voor het gebruik van de Samenwerkingsruimte (t/m Dep.V) worden binnen de samenwerkingsruimte sub mappen aangemaakt die alleen toegankelijk zijn voor specifiek aangewezen (externe) gebruikers. De volgende stappen zijn mogelijk;

- Unieke machtigingen;
- Unieke machtigingen binnen een map;
- Unieke machtigingen met groepen en gebruikers.

## **4.5 Eisen toegang SWR**

Om toegang te krijgen tot de SWR is een VOG-DJI verplicht.

Deze VOG mag niet ouder zijn dan 1 jaar.

Deze VOG dient aangevraagd te worden via de website van DJI.

Nadat PI Vught de echtheid van de VOG heeft vastgesteld, kan RVB de autorisatie verlenen voor de toegang.

## **4.6 Mappenstructuur conform TLP**

Binnen de mapstructuur voor informatiebeveiliging is gekozen voor een indeling op basis van het TLP. Deze structuur helpt bij het systematisch beheren en classificeren van informatie op basis van gevoeligheid en de toegestane verspreidingsgraad. De hoofdmap "Informatiebeveiliging" bevat 4 submappen, elk overeenkomstig met een TLP-classificatie:

- **TLP-RED** is gereserveerd voor de meest gevoelige informatie. Hierin bevinden zich onder andere *incidentrapportages*, *persoonsgevoelige data* en gegevens over *interne beveiligingslekken*. Deze informatie is uitsluitend bedoeld voor specifieke individuen en mag niet gedeeld worden.
- **TLP-AMBER** bevat vertrouwelijke informatie die intern binnen de organisatie gedeeld mag worden. Denk hierbij aan *projectdocumentatie*, *interne beleidsstukken* en *auditrapportages*.
- **TLP-GREEN** is bedoeld voor informatie die breed binnen de organisatie gedeeld mag worden en eventueel ook extern, mits dit functioneel is. In deze map staan onder andere *handleidingen*, *interne presentaties* en *awareness-materialen*.
- **TLP-CLEAR** bevat informatie die vrij beschikbaar is en zonder beperkingen gedeeld mag worden, ook buiten de organisatie. Hieronder vallen *persberichten*, *openbare beleidsdocumenten* en *rapporten voor extern gebruik*.

#### **4.7 Instructies voor gebruik TLP in documenten**

Alle documenten moeten de TLP-markering en de classificatie van de informatie vermelden, alsmede eventuele aanvullende beperkingen, in kop- en voettekst van iedere bladzijde. De TLP-markering dient te worden aangegeven in tenminste een 12 punts lettergrootte.

Voor tekeningen dient een stempel met TLP-markering boven de onderhoek toegepast te worden. In de onderhoek dient de classificatie opgenomen te worden.

## 5 Verdere Afspraken / instructies

### 5.1 Fysieke beveiliging en beveiliging van de omgeving

Werkzaamheden aan het project in TLP:GREEN markeringen dient plaats te vinden in een afgeschermdde omgeving, waarbij de verwerker van de informatie borgt dat informatiebeveiliging gegarandeerd is.

Werkzaamheden aan het project in TLP:AMBER markeringen kan alleen plaatsvinden in een afgeschermdde en toegang gecontroleerde omgeving, waarbij de verwerker van de informatie borgt dat er geen voor het project onbevoegden kennis kunnen nemen van de informatie.

Werkzaamheden aan het project in TLP:RED markeringen dient plaats te vinden binnen een toegang gecontroleerde en afgeschermdde ruimte waarbinnen alleen voor het project bevoegde medewerkers met toegang tot TLP RED gemarkeerde informatie aanwezig zijn. Er is geen zicht van buiten de ruimte op de TLP:RED gemarkeerde informatie mogelijk. Registratie van de medewerkers met toegang tot deze ruimte is aanwezig.

### 5.2 Opslag informatie

De opslag van informatie in ICT-systemen en hardcopy is afgeschermd voor de TLP:GREEN. Cleandesk is van toepassing en de omgeving waar informatie is opgeslagen is voorzien van inbraakdetectie met opvolging door een beveiligingsorganisatie.

De opslag van informatie in ICT-systemen en hardcopy is voor de TLP:AMBER afgeschermd in een binnen de kantooromgeving afgeschermdde ruimte. De afscherming van kantoor en separate ruimte zijn voorzien van toegangscontrole en inbraaksignalering. De opvolging na inbraakalarm wordt verzorgd door een beveiligingsorganisatie.

De opslag van informatie in ICT-systemen en in hardcopy voor TLP:RED is afgeschermd met een 'positief beveiligingsrendement'. De ruimten waar de informatie bewaard wordt zijn toegangsgecontroleerd en er vindt registratie van de toegang plaats. Gebruik wordt gemaakt van gecertificeerde afscherming.

### **5.3 Communicatie over het project**

Het is voor de organisaties in ontwerp en uitvoering verboden over het project buiten de projectorganisatie te communiceren. Dit geldt ook voor commerciële doeleinden. Indien er communicatie over het project noodzakelijk is, zal dit via de verantwoordelijken binnen DJI en Rijksvastgoedbedrijf plaatsvinden.

Het vermelden van bedrijfsnamen en project specifieke informatie (zoals adres, objectnamen etc.) op documenten met de TLP:RED is niet toegestaan.

### **5.4 E-mail en agenda beheer**

#### *5.4.1 Instructies voor gebruik van TLP in berichtenverkeer, zoals e-mail*

TLP gemarkeerde berichten moeten de classificatie gevolgd door een TLP-markering van de informatie bevatten alsmede eventuele aanvullende beperkingen, onmiddellijk voorafgaand aan de desbetreffende informatie. De classificatie en TLP-markering dient in de onderwerpregel van het e-mailbericht te staan. Zorg er waar nodig tevens voor om het einde van de tekst aan te geven waarop de TLP-markering van toepassing is.

Zowel intern als extern kan er gebruik worden gemaakt van Secure Transfer via Rijkscloud: ODCN Secure Transfer. Secure Transfer is specifiek bestemd voor het uitwisselen van Dep.V informatie, tot TLP:AMBER.

In verband met het belang van de anonimiteit vermijdt te allen tijde het gebruik van groepsverzendingen tenzij vastgesteld kan worden dat alle betrokkenen bekend zijn met elkaars betrokkenheid bij het project.

#### *5.4.2 Agenda beheer*

In verband met de anonimiteit zorg dat derden geen inzicht kunnen krijgen in de details van een afspraak door of toegang tot de agenda te blokkeren of door de afspraak privé te maken.

### **5.5 Gebruik sociale media**

Het staat alle deelnemers van een DJI-project vrij om sociale media te gebruiken. Maar ook in het gebruik van sociale media moet men waken voor de goede naam van DJI en het Rijksvastgoedbedrijf. Projecten kunnen een vertrouwelijk karakter hebben waardoor (informatie van) het project niet openbaar mag worden gemaakt. Ook kunnen uitslatingen op sociale media de integriteit van informatie, de naam van DJI en het Rijksvastgoedbedrijf ernstige schade toebrengen. Het is niet toegestaan

om op sociale media uitlatingen te doen van een DJI-project zonder schriftelijke instemming van DJI en het Rijksvastgoedbedrijf.

## **5.6 Divers**

Communicatie over het project mag niet via whatsapp plaats vinden. Indien deze vorm van communicatie noodzakelijk is, dient Signal te worden gehanteerd.

## **5.7 Clear screen / clear desk**

Dit houdt in dat bij het verlaten van de werkplek het beeldscherm wordt vergrendeld en fysieke documenten worden opgeslagen in een afsluitbare kast. De clear screen en clean desk policy geldt zowel op kantoor als voor thuiswerken als voor werken op afstand.

## **5.8 Kantoor- thuiswerk omgeving**

Ook binnen de kantooromgeving of thuiswerkplek waar werkzaamheden voor de DJI-projecten worden uitgevoerd moet men waakzaam blijven. Ook bij de aanwezigheid van facilitaire diensten zoals schoonmaak, loodgieters, liftmonteurs maar ook bezoekers enzovoorts is een extra risico aanwezig. Men moet waakzaam zijn voor de aanwezigheid van gevoelige en vertrouwelijke informatie.

## **5.9 Werken op afstand (thuis of project locatie)**

Er wordt veel op afstand gewerkt. Ook dan is de beschikbaarheid, integriteit en vertrouwelijkheid van informatie van groot belang. Let bij het werken buiten de kantooromgeving extra scherp op onveilige situaties waarbij onbevoegde toegang krijgen tot vertrouwelijke informatie.

## **5.10 Internetverbinding**

Daar waar gebruik wordt gemaakt van internetverbindingen mag men alleen gebruikmaken van VPN-verbindingen. De VPN-verbinding dient te beschikken over een adequate vorm van encryptie welke opgenomen is in het encryptie beleid van de organisatie.

## 6 Incidenten

Met het nemen van de juiste maatregelen moeten incidenten worden voorkomen. Toch blijft het een utopie om alle risico's te elimineren en alle incidenten te voorkomen.

### 6.1 Informatie-incidenten

#### 6.1.1 Meldingen

Het is van belang dat het er een laagdrempelige manier voor het doen van meldingen is. Meldingen kunnen incidenten zijn, maar dit is niet noodzakelijk. Ook een vermoeden van of juist een voorkomen incident is goed om als melding vast te leggen. Deze kunnen bijvoorbeeld inzicht geven dat een maatregel effectief is en/of mensen 'bewust' zijn.

Het is belangrijk om het (mogelijk) informatie-incident zo spoedig mogelijk te melden bij de IBF. Na de melding wordt een proces gestart voor het beoordelen en behandelen van de melding. Het doel van de registratie is om te leren van de incidenten die voorkomen en te zorgen dat passende maatregelen worden genomen om incidenten in de toekomst te voorkomen. Daarom is het van groot belang dat informatie-incidenten gemeld worden.

Binnen project wordt gebruik gemaakt van de volgende classificaties:

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

#### 6.1.2 Incidenten

Wanneer een informatie-incident is geconstateerd, moet er adequaat en effectief worden opgetreden om het incident te neutraliseren en de (gevolg)schade te beperken. Daarvoor is het belangrijk om één duidelijke definitie te stellen aan het begrip informatiebeveiligingsincident:

*Een onverwachte en ongewenste gebeurtenis waarbij de kans aanwezig is dat de beschikbaarheid, integriteit en/of vertrouwelijkheid van informatie(assets) wordt aangetast.*

Het gaat dus niet om geplande gebeurtenissen of gebeurtenissen welke een positieve impact hebben. Belangrijk om te vermelden is dat het om incidenten gaat die een ongewenst risico vormen voor de informatie(assets) en/of goede naam van DJI, Rijksvastgoedbedrijf en externe bedrijven en/of betrokken personen welke deel uit maken van het project. Wanneer een incident betrekking heeft op de informatie(assets) en/of goede naam van DJI, Rijksvastgoedbedrijf of een extern bedrijf, moet het direct worden gemeld bij de IBF.

#### 6.1.3 Handelen bij incidenten

Wanneer sprake is van een informatie-incident, is sprake van een blootstelling aan een gevaar. Ten tijde van een incident is het eerst van belang dat de blootstelling aan het gevaar wordt gestopt. Wanneer men niet zelfstandig in staat is om de blootstelling aan het risico te stoppen, moet men direct escaleren naar de persoon die de blootstelling wel kan stoppen. Bij twijfel moet geëscaleerd worden.

Bij het melden van incidenten moeten de volgende aspecten worden omschreven;

Datum en tijdstip	Wanneer het incident zich heeft voorgedaan en hoe lang het heeft geduurd tot het moment waarop de blootstelling aan het gevaar is gestopt.
Type incident	Selecteer uit de lijst met type incidenten welk type incident het gaat.
Omschrijving	Beschrijf wat er is gebeurd en aan welk risico is opgetreden.
Oorzaak	Welke (achterliggende) oorzaak ten grondslag ligt aan het risico. Tip: neem geen genoegen met de directe oorzaak maar kijk ook welke oorzaak ten grondslag ligt aan de directe oorzaak enzovoorts. Bijvoorbeeld: Collega A liet de deur open staan door te gehaast werken. Hij was te gehaast door een te strakke planning enzovoorts.
Voorstel	Indien u een voorstel heeft om dit incident op te lossen en/of in het vervolg te voorkomen.

#### 6.1.4 *Verantwoordelijkheid incidentmanagement*

Iedere projectmedewerker is verantwoordelijk om incidenten tijdig te melden bij de IBF.

De verantwoordelijke medewerker van het RVB controleert of alle relevante stakeholders incidenten correct hebben opgevolgd en afgehandeld, en of passende maatregelen en verbeteracties zijn uitgevoerd.

### 6.2 **Veiligheidsincidenten**

#### 6.2.1 *Melding en noodhulp buiten de PI.\**

- De medewerker belt bij acuut gevaar 112; de politie verleent noodhulp.
- De medewerker belt bij niet spoedeisende situaties 0900-8844 of neemt contact op met de wijkagent, de politie verzorgt administratie, eventuele escalatie en/ of opvolging.
- De werkgever wordt direct geïnformeerd en zorgt voor de coördinatie en uitvoering van directe maatregelen waaronder mede kan worden verstaan de opvang, tijdelijke werkstop en waar nodig noodhuisvesting.

\*De medewerker wordt, naast de mogelijkheid voor bevoegde instanties om dit ambtshalve te laten geschieden, te allen tijde geadviseerd aangifte te doen van strafbare feiten en kan als adres voor correspondentie opgeven het adres van organisatie.

Binnen de PI moet er altijd begeleiding zijn vanuit de PI, verantwoordelijk voor de veiligheid van betrokkenen, met de beschikking over de bijbehorende middelen.

**Bij een acuut gevaar voor personen de naam en/of continuïteit van DJI, Rijksvastgoedbedrijf of een extern bedrijf moet direct contact op worden genomen met de IBF van de eigen organisatie.**



#### *6.2.2 Afstemming met opdrachtgever*

- Binnen 24 uur informeert de werkgever de contactpersoon van de Beveiligingsautoriteit (BVA) van het RVB.
- De Beveiligingsautoriteit (BVA) van het RVB vervult hierbij de coördinerende rol namens de opdrachtgever en zorgt voor afstemming met de politie, de NCTV en andere relevante instanties binnen het stelsel Bewaken & Beveiligen.

#### *6.2.3 Gezamenlijke risicoanalyse*

- Binnen 24 uur overleg tussen werkgever, opdrachtgever, BVA, politie/wijkagent en andere belanghebbenden om risico's te analyseren en maatregelen te bepalen.
- Afspraken worden door de werkgever schriftelijk vastgelegd en gedeeld met de betrokken medewerker.
- Tijdelijke maatregelen blijven van kracht totdat structurele bescherming is gerealiseerd.

#### *6.2.4 Evaluatie en herstel*

- De werkgever blijft verantwoordelijk voor opvolging en evaluatie zolang het risico bestaat.
- Indien eerdere maatregelen niet effectief waren, worden deze beschouwd als niet adequaat, met bijbehorende verplichtingen tot coördinatie en uitvoering van herstel door de werkgever.
- De medewerker ontvangt van organisatie en opdrachtgever een schriftelijke terugkoppeling van de uitgevoerde maatregelen en beoordeelt in overleg met de politie of aanvullende stappen binnen het BBV-stelsel noodzakelijk blijven.