Autoriteit Nucleaire Veiligheid en
Stralingsbescherming

# Handreiking **beveiliging nucleaire inrichtingen**

# Inhoud

# 1 Inleiding

In Nederland is regelgeving rondom nucleaire beveiliging doelgericht: diefstal en sabotage moeten voorkomen worden, maar de regelgeving schrijft niet voor hoe dat juist moet gebeuren. Hierdoor heeft een vergunninghouder de ruimte - maar ook de verantwoordelijkheid - om keuzes te maken over beveiligingsmaatregelen en aan te tonen dat doeltreffend zijn.

Soms is het voor vergunninghouders moeilijk om in te schatten wanneer de ANVS iets als “goed genoeg” beschouwd, en welke criteria worden gehanteerd bij de beoordeling. De wettelijke basis bevindt zich in het Besluit kerninstallaties, splijtstoffen en ertsen, in de ANVS-Verordening nucleaire drukapparatuur, beveiliging en ontmanteling en het Geheimhoudingsbesluit Kernenergiewet. Om verwachtingen betreffende nucleaire beveiliging uit die documenten beter te duiden en inzicht te verschaffen in de door de ANVS gebruikte criteria, heeft de ANVS deze handreiking opgesteld.

Handreikingen zijn informatieve documenten, die de ANVS ten behoeve van vergunninghouders en initiatiefnemers publiceert en waarin staat beschreven hoe de ANVS tegen een bepaald onderwerp aankijkt. De vergunninghouder of initiatiefnemer kan de handreiking vervolgens als uitgangspunt nemen bij het opstellen van zijn documenten en bij zijn handelen. Handreikingen zijn niet aan een vergunning of de wet verbonden en hebben geen verplichtend karakter.

# 2 Voor wie is deze handreiking bedoeld

Deze handreiking is bedoeld voor alle vergunninghouders van inrichtingen, in de zin van artikel 15, onder b, van de Kernenergiewet (verder: nucleaire inrichtingen).

Merk op dat deze handreiking focust op de beveiliging van kernmateriaal in nucleaire inrichtingen. Wanneer in dezelfde inrichting ook radioactieve stoffen aanwezig zijn, kan voor de beveiliging daarvan de “Handreiking BRAS” geraadpleegd worden.

Een deel van deze handreiking is ook van toepassing op inrichtingen die beschikken over gegevens, hulpmiddelen of materialen, dan wel onderzoekingen verrichten of werkmethoden toepassen, ten aanzien waarvan het Geheimhoudingsbesluit Kernenergiewet geldt.

# 3 Toetsingskader

De regelgeving voor de beveiliging van nucleaire inrichtingen in Nederland is beschreven in het Besluit kerninstallaties, splijtstoffen en ertsen, in de ANVS-Verordening nucleaire drukapparatuur, beveiliging en ontmanteling en het Geheimhoudingsbesluit Kernenergiewet.

Naast de regelgeving geeft ook de referentiedreiging (ook wel Design Basis Threat of DBT genoemd) een kader waartegen de vergunninghouder weerstand moet bieden. Deze DBT wordt elke paar jaar herzien. Voor beoordelingen van de nucleaire beveiliging bij een inrichting, wordt steeds de meest recente versie van de DBT gehanteerd, zoals vastgesteld door de bewindspersoon.

Zowel in deze handreiking als in de DBT wordt verwezen naar URC en HRC waarden. Dit staat voor respectievelijk “Unacceptable Radiological Consequences” en “High Radiological Consequences”, dit zijn drempelwaardes van radiologische consequenties. Deze waarden worden beschreven in de ANVS handreiking toepassing URC en HRC.

# 4 Referentiekader

De ANVS ziet graag dat beveiligingsmaatregelen zo veel mogelijk in lijn met relevante nationale en internationale referenties worden geïmplementeerd. Als relevante documenten in deze context wordt onder meer bedoeld:

De IAEA Nuclear Security Series, met in het bijzonder NSS No. 13; Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5).

Merk op dat NSS No. 13 al grotendeels geïmplementeerd is in Nederlandse regelgeving. Verder zijn de Nuclear Security Series niet specifiek opgesteld voor nucleaire inrichtingen. Veel van de IAEA guidance is geschreven voor de nationale toezichthouders zoals de ANVS, en andere hebben een focus op thema's zoals radioactieve stoffen of transport. Toch is veel van de inhoud relevant en bruikbaar als referentiekader. Daarom is het voldoen aan de eisen in de NSS No. 13 die gericht zijn op vergunninghouders/aanvragers ook opgenomen in de 2025 versie van het VOBK (Handreiking voor een veilig ontwerp en het veilig bedrijven van kernreactoren). In sommige gevallen is het niet voor de hand liggend hoe deze aanbevelingen passen in de Nederlandse context, en hoe de IAEA en Nederlandse terminologie overeenkomen. Waar mogelijk geeft deze handreiking verdere toelichting op dit soort situaties.

De volgende tabel licht toe hoe bindend de verschillende types van documenten worden beschouwd:

| Soort Document | Verwachting |
|---|---|
| Documenten van toepassing verklaard in een goedkeuringsbesluit | Verplicht |
| IAEA Nuclear Security Series No. 13, 14 en 15 | Referentiedocument. Specifieke bepalingen vaak verplicht wegens opname in regelgeving. |
| Alle andere IAEA Nuclear Security Series publicaties | Referentiedocument |
| ISO, EN en NEN normen | Referentiedocument |

Referentiedocumenten worden door de ANVS gebruikt om te beoordelen of de wijze waarop aan de het toetsingskader wordt voldaan, overeenkomt met de stand-der-techniek.

Bij IAEA Nuclear Security Series staan doorgaans aanbevelingen voor de Staat, de toezichthouder en de vergunninghouder. Uiteraard is het enkel de verwachting dat de vergunninghouder de documenten als referentie gebruikt waar deze ook aan de vergunninghouder gericht zijn.

Uiteraard moet bij de referentiedocumenten de context overeenkomen met de na te leven vereisten. Voorbeeld: wanneer een certificering van een deur op basis van een norm een inbraakweerstand van 5 minuten aangeeft tegen een inbreker, dan gaat de ANVS dit niet ter discussie stellen. Maar dit betekent niet noodzakelijk dat genoemde deur ook een weerstand van 5 minuten heeft tegen de tegenstander beschreven in de DBT, die mogelijk gebruik maakt van zwaardere middelen. Daarvoor is bijkomende onderbouwing vereist.

Merk ook op dat het volgen van bovenstaande referenties nog geen garanties geeft voor een goedkeuring van de effectieve implementatie. Een beveiligingscamera kan aan een bepaalde norm voldoen, maar dat betekent niet dat deze op de juiste plek staat geïnstalleerd of de juiste functie vervult binnen het totale beveiligingssysteem.

# 5 Proces

Het proces voor vooroverleg en vergunningverlening staat in meer detail beschreven in de ANVS hand-reikingen vooroverleg en vergunningverlening.

Aandacht voor beveiliging is belangrijk in alle fasen van bedrijfsvoering voor een nucleaire inrichting. Al in de planningsfase is het nodig om rekening te houden met beveiliging, waaronder een gepaste locatie, voldoende informatiebeveiliging en bepalingen met betrekking tot het ontwerp.[1] In dit hoofdstuk wordt een overzicht gegeven van de verwachtingen aan een aanvrager of vergunninghouder betreffende de verschillende fasen.

1 Zie IAEA Nuclear Security Series No. 35-G: Security During the Lifetime of a Nuclear Facility en NSS No. 45-T: Regulatory Authorization and Related Inspections for Nuclear Security During the Lifetime of a Nuclear Facility

Een vergunninghouder kan kiezen om een beveiligingspakket tot één of meerdere fases (bijv. de ontwerpfase) te beperken. In dat geval moet het aangepaste beveiligingspakket voorafgaand aan de overgang naar een volgende fase (bijv. de bouwfase) ter goedkeuring aan de ANVS worden voorgelegd. Hierbij is het wenselijk om al vroegtijdig contact op te nemen met de ANVS om vertragingen bij faseovergangen te voorkomen. De verwachtingen per fase zijn hieronder samengevat.

## 5.1 Fasen 1 en 2: Voorbereiding en Locatiekeuze

Het is aan de aanvrager om vanaf het begin voldoende rekening te houden met de effecten en beperkingen van een gekozen locatie betreffende beveiliging.

Belangrijke factoren betreffende locatiekeuze die tijdens deze fasen aan de orde komen zijn onder andere (niet limitatief):

- Eventuele lokale of regionale dreigingen.
- Beveiligingsinterfaces en onderlinge afhankelijkheden met bestaande nabijgelegen nucleaire inrichtingen.
- Topografie met een mogelijke impact op de beveiliging van de locatie.
- Potentiële impact van een radiologische lozing op het milieu of de bevolking.
- De beschikbaarheid van externe respons om tijdig te kunnen reageren op een beveiligingsincident.
- Vrije ruimte voor (her)inrichting en uitbreiding, indien beveiligingsbehoeften zouden toenemen.

Voorafgaand aan het indienden van een vergunningaanvraag volgens artikel 15, onder b, Kernenergiewet (KEW) gaat een initiatiefnemer in overleg met de ANVS over de inhoud van de aanvraag (vooroverleg). Voor en tijdens dit vooroverleg is het aan de initiatiefnemer om voldoende aandacht te besteden aan in ieder geval informatiebeveiliging, security by design, vertrouwensfuncties en het beveiligingspakket. Verwachtingen betreffende deze onderwerpen zijn in meer detail beschreven in de ANVS handreiking vooroverleg.

## 5.2 Fase 3: Ontwerp

Tijdens het volledige ontwerpproces wordt verwacht dat de aanvrager voldoende aandacht heeft voor security by design. Hiervoor is in ieder geval toegang tot de staatsgeheime referentiedreiging vereist.

De verwachting is dat een aanvrager in deze fase:

- Een initiële versie voorbereidt van het **beveiligingspakket voor de bouwfase**, hierover overlegt met de ANVS en voorbereidingen treft om deze maatregelen uit te voeren. Belangrijke beveiligingsrisico's in deze fase betreffen bijvoorbeeld informatiebeveiliging, beïnvloeding van het ontwerpproces, invloeden op nabijgelegen nucleaire inrichtingen, en supply chain risico's.
- Vroegtijdig voorbereidingen treft voor de beveiliging tijdens de **inbedrijfstelling en bedrijfsfase** en hiermee rekening houdt in het ontwerp. De basis hiervoor zijn gedetailleerde analyses van relevante diefstal- en sabotagescenario's, afgeleid van de referentiedreiging. Belangrijke beveiligingsmaatregelen met een potentieel grote invloed op het (concept- of basis-)ontwerp zijn bijvoorbeeld bouwtechnische maatregelen (dikte van muren, ...), elektronische maatregelen (keuzes voor de inzet van digitale meet- en regelapparatuur voor bepaalde veiligheidsfuncties), digitale maatregelen (zoals afspraken over informatiebeveiliging, het borgen van de echtheid en integriteit van componenten, monitoring en logging van netwerken) en de toepassing van *security by design*.

## 5.3 Fase 4: Bouwfase

Voorafgaand aan het begin van de bouw van een nucleaire inrichting moet een aanvrager over een oprichtingsvergunning beschikken. Vanaf dit moment moet een vergunninghouder ook beschikken over een goedgekeurd beveiligingspakket voor in ieder geval de bouwfase, ook al zijn nog geen nucleair materiaal of radiologische stoffen aanwezig.

Zo nodig wordt een beveiligingspakket door de vergunninghouder tijdens de bouwfase meerdere keren herzien.

De verwachting is dat een vergunninghouder, op basis van een goedgekeurd beveiligingspakket:

- Alle structuren, systemen en componenten (SSCs) die een veiligheidsfunctie of beveiligingsfunctie (gaan) vervullen heeft geïdentificeerd, hiervoor een beveiligingsstrategie heeft ontwikkeld en beschreven, en de nodige beveiligingsmaatregelen neemt om het risico van ongewenste beïnvloeding van deze systemen aantoonbaar te beheersen;
- Voldoende maatregelen neemt om ongewenste beïnvloeding of diefstal van gevoelige informatie te voorkomen;
- Voldoende maatregelen neemt om ongewenste beïnvloeding van medewerkers en/of leveranciers te voorkomen;

- De ANVS actief informeert, en waar nodig betrekt, bij het ontwikkelen van een beveiligingspakket voor de commissioning- en bedrijfsfase;
- De nodige verificaties, tests, certificeringen en accreditaties uitvoert en documenteert om de effectiviteit van het beveiligingssysteem als deel van de aanvraag tot goedkeuring van het beveiligingspakket voor de commissioning- en bedrijfsfase aan te tonen;
- De ANVS in staat stelt om aanwezig te zijn bij verificaties, tests, certificeringen en accreditaties;
- Handelt in overeenstemming met het goedgekeurde beveiligingspakket en medewerking verleent aan het toezicht op het goedgekeurde beveiligingspakket.

Tijdens de constructie houdt de ANVS toezicht op basis van het goedgekeurde beveiligingspakket voor de bouwfase.

## 5.4 Fasen 5 en 6: Inbedrijfstelling en bedrijfsfase

Tijdens de inbedrijfstelling en bedrijfsfase moet de vergunninghouder handelen volgens het goedgekeurde beveiligingspakket voor deze fase. Voor wijzigingen tijdens deze fasen zie hoofdstuk 5.9.

## 5.5 Fasen 7 en 8: Uit bedrijf stellen en ontmanteling

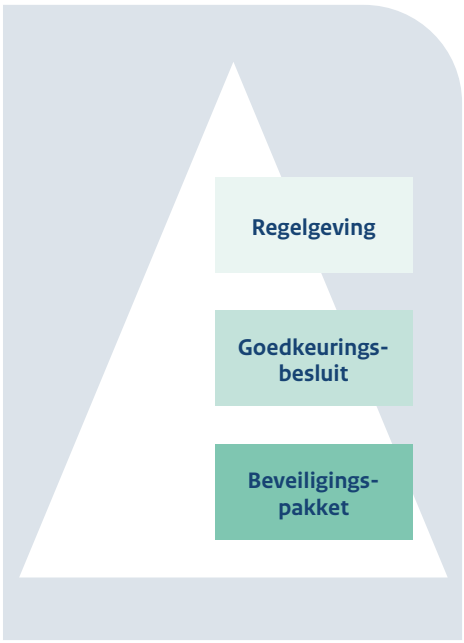
Voor het uit bedrijf stellen en de ontmanteling van een inrichting moet een vergunninghouder beschikken over een goedgekeurd beveiligingspakket voor deze fase. In principe blijven de eisen uit de bedrijfsfase van toepassing, maar dan met een graduele aanpak op basis van de resterende risico's.

## 5.6 Vergunning, goedkeuringsbesluit, beveiligingspakket

**Kernenergiewetvergunning**: een nucleaire inrichting als bedoeld in artikel 15, onder b, KEW moet over een kernenergiewetvergunning beschikken.[2] Deze vergunning stelt geen specifieke eisen aan nucleaire beveiliging.

**Goedkeuringsbesluit beveiligingspakket**: een beveiligingspakket behoeft goedkeuring van de Autoriteit.[3] Deze goedkeuring wordt vastgelegd in een goedkeuringsbesluit. De Autoriteit kan aan de goedkeuring van een beveiligingspakket voorschriften verbinden.[4]

**Beveiligingspakket**: een vergunninghouder als bedoeld in artikel 15, onder b, KEW moet beschikken over een beveiligingspakket met een beschrijving van de wijze waarop de inrichting of het categorie I-, II-, en III-materiaal wordt beveiligd.[5] De vergunninghouder moet het goedgekeurde beveiligingspakket in acht nemen en eenmaal goedgekeurd is de inhoud van dit beveiligingspakket bindend.[6] De IAEA noemt dit een security plan.[7]




2 Kew, art. 15, onder b.

3 Bkse, artikel 22b.

4 Bkse, artikel 22b.

5 Bkse artikel 22a, 1e lid

6 Bkse artikel 22, 3e lid, a.

7 IAEA Nuclear Security Series No. 13: Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities (INFCIRC/225/Revision 5), onder 3.27.

## 5.7 Vergunningsaanvraag en goedkeuringsaanvraag

Bij de aanvraag voor een vergunning artikel 15, onder b, Kernenergiewet (KEW) moet de aanvrager aantoonbaar maken dat voldoende rekening werd gehouden met security by design.

Een vergunninghouder moet beschikken over een goedgekeurd beveiligingspakket. Het is daarom nodig om voorafgaand aan het verkrijgen van een vergunning een aanvraag tot goedkeuring voor een beveiligingspakket in te dienen. Het heeft de voorkeur van de ANVS dat dit gebeurt samen met de vergunningsaanvraag. Hiervoor is voorafgaande afstemming met de ANVS nodig. De uitgangspunten hiervoor zijn in deze handreiking beschreven.

## 5.8 Goedkeuringsbesluit en Toezicht

De ANVS kan aan de goedkeuring van een beveiligingspakket voorschriften verbinden. Deze voorschriften kunnen bijvoorbeeld betrekking hebben op het gebruik van specifieke normen, meldplichten of toegangsbeperkingen.

Naast de wet- en regelgeving vormen het goedkeuringsbesluit en het goedgekeurde beveiligingspakket de basis voor het toezicht op nucleaire beveiliging door de ANVS.

## 5.9 Wijziging van een goedgekeurd beveiligingspakket

Wijzigingen van het beveiligingspakket die een negatief effect hebben of kunnen hebben vereisen goedkeuring door de ANVS. Bij deze wijzigingen is het aan te raden om de ANVS voegtijdig te informeren. Conform internationale standaarden zoals genoemd in het VOBK verwacht de ANVS dat een vergunninghouder beschikt over een actuele procedure voor wijzigingsbeheer.

# 6 Toelichting bij de DBT

Merk op: De DBT of referentiedreiging valt onder het Geheimhoudingsbesluit Kernenergiewet en is een gerubriceerd document. In de DBT staat een korte toelichting over het gebruik. Omdat deze toelichting niet gerubriceerd is, wordt deze hieronder herhaald in 6.1 – 6.3, en nog aangevuld met bijkomende uitleg onder 6.4.

## 6.1 Doel van de DBT

Het doel van de DBT is het vaststellen van een referentiedreiging die een nucleaire vergunninghouder moet kunnen weerstaan. Om te kunnen weerstaan, moet het doel van de tegenstander vermeden kunnen worden. Deze doelen zijn als volgt bepaald:

1. Diefstal van kernmateriaal
2. Sabotage met radiologische consequenties
3. Aantonen van kritische kwetsbaarheden in het beveiligingssysteem

## 6.2 Bepaling van de basisprofielen voor de inrichting

Een inrichting moet rekening houden met **profiel A** wanneer er Categorie I kernmateriaal aanwezig is op de site, of wanneer sabotage zou kunnen leiden tot hoge radiologische consequenties (HRC). Op het moment van vaststelling van deze DBT is HRC bepaald als een dosis van 100 mSv over 7 dagen aan de rand van de site.

Een inrichting moet rekening houden met **profiel B** wanneer er geen Categorie I kernmateriaal aanwezig is op de site, maar wel categorie II of III kernmateriaal. Ook mag sabotage niet kunnen leiden tot HRC.

Een inrichting moet rekening houden met **profiel C** wanneer er geen Categorie I, II of III kernmateriaal aanwezig is op de site, maar sabotage wel zou kunnen leiden tot onaanvaardbare radiologische consequenties (URC). Op het moment van vaststelling van deze DBT is URC bepaald als het overschrijden van waarden uit Bijlage 2 van het Bkse.

Is er helemaal geen kernmateriaal on-site, én kan sabotage niet leiden tot URC, dan zijn geen van de drie voorgenoemde profielen van toepassing.

Naast de selectie van profiel A, B of C, slaat **profiel D** op demonstranten en activisten. Dit profiel is deze van toepassing op alle inrichtingen. Bij voorbeeld: Een inrichting met categorie I kernmateriaal, moet dus rekening houden met zowel profiel A als profiel D.

Doorgaans geldt dus dat twee profielen van toepassing zijn: (A, B of C) + D.

## 6.3 Elementen van de profielen

In de kolommen die bij elk profiel horen, staan de eigenschappen zoals middelen, wapens en kennis waar de tegenstander in kwestie gebruik van kan maken. Merk daarbij het volgende op:

- Alle elementen uit een kolom kunnen gecombineerd worden. Dat betekent niet dat alle elementen uit een kolom ook combineerbaar zijn in éénzelfde scenario.
- De termen en cijfers in de verschillende vakken oordelen niet over waarschijnlijkheid. Als in een vak bijvoorbeeld “5 personen” staat, betekent dit niet dat vijf het maximaal mogelijke, of meest waarschijnlijke aantal personen is. Wat het wel betekent is dat de vergunninghouder in de uitwerking van scenario’s rekening moet houden met vijf personen.
- Alle elementen in de vakken kunnen ingezet worden tijdens een kwaadwillige actie. Het doel van de vergunninghouder is niet om het element in kwestie tegen te houden, maar het einddoel van de aanval. Bijvoorbeeld: Als er sprake is van een drone of een computervirus, moet de vergunninghouder niet kunnen aantonen dat deze drone of dat virus volledig geweerd kunnen worden. Wel moet de vergunninghouder met die drone of dat virus rekening houden in de scenario’s, en bijvoorbeeld kunnen aantonen dat aan het eind van het scenario, geen kernmateriaal gestolen wordt, en geen radiologische consequenties optreden.

Voor **gereedschap** wordt verwezen naar de Loss Prevention Standard (LPS) 1175. Op het moment van vaststelling wordt hiervoor versie 8.2 gebruikt. Mogelijke gereedschapscategorieën zijn A, B, C, D, E, F, G, H en worden beschreven in de standaard. Merk op dat voertuigen, vuurwapens en explosieven niet mee zijn opgenomen in deze gereedschapscategorieën. De verwijzing naar gereedschap via LPS categorieën houdt geen verplichting in om voor onderbouwing van bij voorbeeld vertragingstijden van barrières ook LPS certificering te gebruiken.

Voor de **cybercomponent** wordt verwezen naar zogenaamde “Threat Actor Sophistication” uit de STIX Core Concepts. Op het moment van vaststelling wordt hiervoor versie 2.0 gebruikt. Mogelijke sophistication levels zijn: none, minimal, intermediate, advanced, expert, innovator, strategic. De ANVS kan verdere toelichting verschaffen over hoe deze levels zich verhouden tot bij voorbeeld technieken uit het Mitre Att&ck framework, terug te vinden via https://attack.mitre.org/

## 6.4 Afwijking van profielen binnen een inrichting

### Aanwezigheid van kernmateriaal

Voor diefstal-scenario’s moet profiel A toegepast worden op locaties waar categorie I kernmateriaal aanwezig is. Voor locaties met categorie II of III kernmateriaal wordt profiel B toegepast. Voor locaties zonder categorie I, II of III kernmateriaal, zijn aparte diefstalscenario’s niet nodig. Hierbij toont de vergunninghouder aan dat de hoeveelheid aan categorie II en III kernmateriaal niet accumuleert tot categorie I, of dat deze locaties voldoende en afzonderlijk beveiligd zijn.

### Radiologische consequenties van sabotage

Wanneer de radiologische consequenties van mogelijke sabotage berekend worden, hangt de keuze voor een profiel af van de vraag of HRC bereikt kunnen worden. Bij overschrijden van HRC is profiel A van toepassing. Blijven de mogelijke consequenties onder de HRC limiet, dan is profiel B van toepassing. Merk op dat deze berekeningen per gebouw of installatie kunnen worden uitgevoerd, zolang een brand of explosie in de ene locatie geen directe gevolgen kan hebben voor een andere locatie.

In andere woorden: Twee tegen elkaar staande of nabijgelegen gebouwen waarbij een brand of een explosie in het ene gebouw ook kan leiden tot radiologische consequenties in het andere gebouw, moeten collectief beschouwd worden in de berekeningen. Staan beide gebouwen ver genoeg van elkaar verwijderd zodat een brand of een explosie in het ene gebouw niet kan leiden tot radiologische consequenties in het andere gebouw, dan wordt voor beide gebouwen afzonderlijk bepaald of de HRC limiet bereikt kan worden, en welk DBT-profiel vervolgens gebruikt dient te worden voor scenario’s.

# 7 HRC en vitale zones

Voor de aanduiding van vitale zones en voor het bepalen van DBT-profielen, speelt de berekening van radiologische consequenties een belangrijke rol, en met name of deze al dan niet de HRC-limiet overstijgen. De bepaling van deze limiet is het onderwerp van de Handreiking Toepassing URC en HRC.

Hierbij maakt de ANVS de volgende aannames:

1. De gebruikte inventaris is gebaseerd op de hoeveelheid splijtstoffen en andere radioactieve stoffen beschreven in het beveiligingspakket. Het is hierbij mogelijk om af te wijken van de in de kernenergiewetvergunning vergunde hoeveelheid. Wanneer in het beveiligingspakket andere hoeveelheden kernmateriaal worden gehanteerd dan in de vergunning, moet de reden hiervoor wel worden toegelicht.
2. De analyse voor de keuze van een DBT-profiel houdt geen rekening met bestaande veiligheids- en beveiligingsmaatregelen. Voor de profielkeuze wordt dus uitgegaan van het "worst-case-scenario"[8]. Voor een reactor is dit bijvoorbeeld een ongefilterde, volledige lozing naar de lucht van een inventaris aan het einde van een bestralingscyclus. Wanneer na keuze van het DBT-profiel scenario's worden uitgewerkt, kan in de analyse van die scenario's in bepaalde gevallen wel rekening gehouden worden met de relevante maatregelen.
3. Als de volledige inventaris binnen een gebouw of zone bij een lozingspercentage van 100% bij normale weersomstandigheden niet kan leiden tot HRC, is het niet nodig verdere berekeningen uit te voeren of rekening te houden met HRC.
4. In alle andere gevallen is het aan de inrichting om door middel van analyses aantoonbaar te maken dat geen HRC limiet bereikt wordt.
5. Wanneer de vergunninghouder ervan uitgaat dat voor een gebouw of zone mogelijke radiologische consequenties de HRC limiet wel overschrijden, is het niet noodzakelijk dit aan te tonen door middel van analyses.

# 8 Uitwerken van scenario's

In de DBT staan verschillende profielen (Zie 6. Toelichting bij de DBT).

DBT profielen beschrijven alle mogelijke opties qua uitrusting, kennis en intenties van de tegenstander. Op basis hiervan beschrijft een scenario één specifieke combinatie van:

- tegenstander,
- middelen,
- kennis,
- intenties (bijv. het veroorzaken van HRC),
- duidelijk geïdentificeerd aanvalsdoel (sabotagegevoelige installatie, hoeveelheid splijtstoffen of gerubriceerde informatie),
- aanvalstactiek (bijv. het openlijk veroorzaken van een explosie).

Voor het van toepassing zijnde profiel moet de vergunninghouder aantonen dat de inrichting en het categorie I-, II-, of III-materiaal beveiligd zijn tegen de dreigingen zoals omschreven in de referentiedreiging. De effectiviteit kan worden gedemonstreerd door voor verschillende relevante scenario's aan te tonen dat bestaande beveiligingsmaatregelen voldoende zijn om het beveiligingsdoel te bereiken.

Voor de vertaling van DBT profielen naar scenario's let de ANVS op de volgende criteria:

1. Er wordt gevraagd om een gedetailleerde analyse uit te voeren van alle scenario's die mogelijk HRC kunnen veroorzaken. De regelgeving vereist een hoog betrouwbaarheidsniveau voor beveiliging tegen Hoge Radiologische Gevolgen (HRC). Het is daarom nodig om alle scenario's te identificeren die, onafhankelijk van bestaande beveiligings- of veiligheidsmaatregelen, tot HRC kunnen leiden.
2. Per gebouw/locatie wordt er gevraagd om ten minste één scenario voor diefstal van nucleair materiaal, informatie of sabotage te onderzoeken (voor zover van toepassing).
3. Per gebouw/locatie wordt er gevraagd om scenario's met ten minste de volgende elementen te onderzoeken (zo ver van toepassing): (a) maximale aantal tegenstanders met zware wapens, (b) maximale hoeveelheid explosieven, (c) insider, (d) hybride aanval, (e) stand-off, (f) vliegtuig. Deze elementen hoeven niet noodzakelijk in één scenario gecombineerd te worden.

8 Het gaat hier om een theoretische situatie, niet om scenario's zoals die later in detail moeten worden uitgewerkt.

# 9 Informatiebeveiliging

De ANVS evalueert de beveiliging van de volgende informatie:

- Alle informatie aangewezen onder het Geheimhoudingsbesluit Kernenergiewet
- Alle informatie waarvan de compromittering zou kunnen leiden tot een verhoging van het risico op diefstal van categorie I, II of III kernmateriaal, of tot sabotage met radiologische consequenties boven de URC-limiet.

Zie bijlage 1 voor een lijst met maatregelen voor de beveiliging van dergelijke informatie, die de ANVS als aanvaardbare nalevingswijze beschouwt.

# 10 Perspectief beoordeling digitale beveiliging

Voor beoordeling van digitale beveiliging bij nucleaire inrichtingen, evalueert de ANVS vanuit de volgende perspectieven.

## 10.1 DBT-scenario's

De vergunninghouder is in staat om via scenario's vanuit de toepasselijke DBT-profielen aan te tonen dat een fysieke, digitale of gecombineerde dreiging niet kan leiden tot diefstal van kernmateriaal, radiologische consequenties boven HRC, of compromittering van gerubriceerde of proliferatiegevoelige informatie.

## 10.2 NSS No. 17-T

De vergunninghouder kan aantonen te voldoen aan alle aanbevelingen – voor zover van toepassing op vergunninghouder – uit NSS No. 17-T, of heeft een goede verantwoording in gevallen waar ervoor gekozen is om op een andere manier een vergelijkbaar beveiligingsniveau te bereiken. (Zie toelichting bij 4. Referentiedocumenten)

Voor inspectie op digitale beveiliging wordt voornamelijk naar twaalf verschillende onderwerpen gekeken, die alle aan bod zullen komen tijdens thematische inspecties. Deze onderwerpen zijn:

1. Organisatorische en administratieve aspecten
2. Digitale assets en hun functie binnen de inrichting
3. Risico management
4. Beveiligingsmaatregelen – conceptuele aspecten
5. Beveiligingsmaatregelen – preventie
6. Beveiligingsmaatregelen – detectie
7. Beveiligingsmaatregelen – respons
8. Beveiliging van de toeleveringsketen
9. Change management
10. Evaluatie van de beveiligingsmaatregelen
11. Meldingen en geleerde lessen
12. Beveiligingscultuur

# 11 Vertrouwensfuncties

De nucleaire sector is in Artikel 3 van het besluit beveiliging netwerk- en informatiesystemen aangewezen als vitale aanbieder. Daarom zijn ook bij nucleaire inrichtingen vertrouwensfuncties aan te wijzen op basis van de Wet veiligheidsonderzoeken. De lijst van aangewezen vertrouwensfuncties maakt volgens artikel 22a, onder b, Bkse, integraal deel uit van het beveiligingspakket.

Conform de Wet veiligheidsonderzoeken wijst de Minister van Infrastructuur en Waterstaat vertrouwensfuncties aan en doet hierbij mededeling aan de desbetreffende nucleaire inrichting. De Minister krijgt bij deze aanwijzing ondersteuning van de sub Beveiligingsambtenaar (sub BVA). Vanuit deze rol draagt de sub BVA

binnen de ANVS zorg voor het (doen) opstellen van de lijsten vertrouwensfuncties. De sub BVA is gemachtigd om het (doen) opstellen van de lijsten vertrouwensfuncties te beleggen bij nucleaire inrichtingen. Bij het opstellen van de lijsten vertrouwensfuncties biedt deze handreiking verduidelijking.

Vertrouwensfuncties zijn functies die de mogelijkheid geven om de nationale veiligheid te schaden, bijvoorbeeld omdat een functie toegang geeft tot gerubriceerde informatie of tot mogelijke doelwitten of middelen voor een aanslag of spionage. Splijtstoffen van categorie I en installaties die in geval van sabotage direct of indirect tot hoge radiologische consequenties (HRC) kunnen leiden, worden door de ANVS in ieder geval beschouwd als dergelijke doelwitten of middelen voor een aanslag in de zin van door de AIVD opgestelde Leidraad aanwijzing vertrouwensfuncties.

In ieder geval zijn de volgende functies te beschouwen als functies die regelmatig toegang geven tot staatsgeheime informatie en/of mogelijke doelwitten of middelen voor een aanslag of spionage en die als vertrouwensfunctie aangewezen dienen te worden:
- De beveiligingsdeskundige en diens plaatsvervanger(s);
- Alle personen met rechtstreekse toegang tot gerubriceerde informatie;
- Alle personen waarvan verwacht wordt dat zij regelmatig met gerubriceerde informatie in aanraking komen;
- Alle personen die onbegeleid toegang hebben tot vitale zones van de inrichting.

Wanneer bij toegang tot vitale zones vertrouwensfuncties / VGB's voor alle betrokkenen niet haalbaar zijn, wordt de vergunninghouder verwacht te documenteren hoe zij een gelijkwaardig niveau van betrouwbaarheid kunnen waarborgen.

# 12 Inhoud beveiligingspakket

In Bijlage 2 – Template beveiligingspakket worden de elementen benoemd waarvan een beschrijving verwacht wordt in het beveiligingspakket van de inrichting. Hieronder volgt meer toelichting over hoe en met welke randvoorwaarden deze elementen beschreven dienen te worden.

## 12.1 Technische onderbouwing

De volgende informatie in de beveiligingspakketten behoeft in ieder geval onderbouwing als deze informatie gebruikt wordt om weerstand tegen de referentiedreiging aan te tonen:
- Vertraging (tijd);
- Detectiekans (waarschijnlijkheid);
- Responstijden (tijd);
- Radiologische gevolgen;
- Beschikbaarheid van mitigerende maatregelen.

Er zijn verschillende manieren om deze informatie te onderbouwen, onder andere:
- Testen, waaronder Factory Acceptance Tests (FATs) en Site Acceptance Tests (SATs);
- Certificering of accreditatie;
- Engineering Judgement;
- Oefeningen.

Alle onderbouwingen moeten gedocumenteerd zijn en samen met een beveiligingspakket aan de ANVS worden voorgelegd. Onderbouwende analyses maken bij voorkeur geen integraal deel uit van het beveiligingspakket, maar worden samen met een beveiligingspakket als onderbouwende informatie aangeleverd.

## 12.2 Doelgerichte aanpak

Nederlandse wet- en regelgeving rondom nucleaire beveiliging, waaronder het Bkse, is doelgericht en formuleert bijna geen specifieke beveiligingsmaatregelen. Prescriptieve details betreffende nucleaire beveiliging dienen opgenomen te worden in het beveiligingspakket of onderliggende documentatie.


| | |
|---|---|
| **Bkse, artikel 22, derde lid, a** | De houder van een vergunning voor een inrichting als bedoeld in artikel 15, onder b, van de wet treft de beveiligingsmaatregelen die redelijkerwijs nodig zijn om de inrichting of de in bijlage 1 genoemde splijtstoffen of ertsen, die krachtens het zevende of achtste lid zijn aangewezen als categorie I-, II- of III-materiaal, te beveiligen tegen de dreigingen zoals omschreven in de referentiedreiging. |
| **Goedkeuringsbesluit** | De vergunninghouder neemt alle nodige maatregelen om toegang van voertuigen boven 3.5 ton tot een gebeid van 20 meter rondom gebouw A te voorkomen. Uitzonderingen behoeven schriftelijke goedkeuring door de ANVS. |
| **Beveiligingspakket** | Gebouw A is voorzien van een hek op 25 meter afstand, voorzien van regelmatig geteste en onderhouden statische aanrijbeveiliging die voldoet aan norm ASTM F2656 M50:P1. |
| **Uitwerking beveiligingspakket in procedures, werkinstructies en daadwerkelijke maatregelen.** | Op een afstand van 25 meter rondom gebouw A zijn voor de hek barrières met ASTM F2656 M50 : P1 certificering geplaatst, met een maximale afstand van een meter tussen elke barrière. Barrières worden jaarlijks gecontroleerd en onderhouden volgens het beschreven onderhoudsprogramma. |

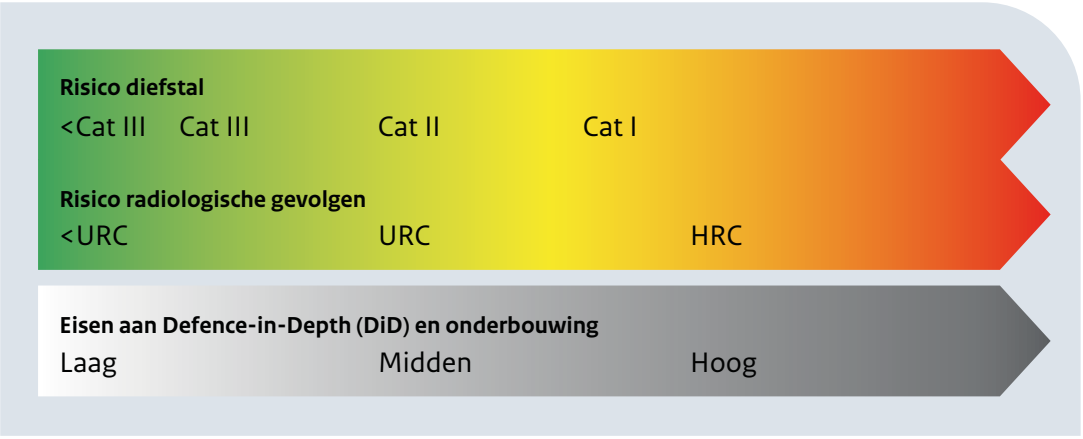
## 12.3 Defence in depth

Een enkelvoudig falen van een beveiligingsmaatregel mag niet direct leiden tot het falen van het gehele beveiligingssysteem, of tot succesvolle diefstal of sabotage. Onder andere door gebruik van meerdere beveiligingsschillen, diverse en redundante systemen en een goede beveiligingscultuur kan een beveiligingspakket aantonen dat een voldoende verdediging in de diepte bereikt wordt. Voor hogere beveiligingsrisico's is ook een hogere mate van verdediging in de diepte vereist.

## 12.4 Graduele Aanpak

Hogere risico's eisen een hoger niveau van beveiliging. Dit wordt ook graduele aanpak genoemd, en vereist dat het beveiligingssysteem een hoger niveau van beveiliging biedt voor:

- Nucleair materiaal met een hogere beveiligingscategorie;
- Hogere consequenties van sabotage;
- Hogere consequenties van diefstal;
- Hoger gerubriceerde informatie.




## 12.5 IBO-EBO aansluiting

De aansluiting tussen IBO en EBO staat vermeld in de ANVS-verordening artikel 3.3, 4e lid, en in het Bkse artikel 22a, 1e lid onder c. De ANVS ziet toe op deze aansluiting, en let daarbij op het volgende:

Uit de analyses van scenario's, gebaseerd op de toepasselijke DBT-profielen, moet blijken hoe lang de inrichting weerstand kan bieden tegen de tegenstander, en hoe lang het de uitvoering van bepaalde aanvalsdoelen (zoals diefstal of sabotage) kan vermijden. Met de meest conservatieve van deze tijden, moet afstemming gebeuren tussen de inrichting en de Externe Beveiligingsorganisatie. Hierbij moet ten minste het volgende gedocumenteerd worden:

- De kritieke scenariotijden
- Wie de rol van EBO invult
- Afspraken met de EBO
- Verklaring van de EBO over hun interventietijd, of over de mogelijkheid om al dan niet binnen de kritieke scenariotijden te kunnen ingrijpen

# 13 Evaluaties

Er worden met geregelde frequentie verschillende soorten evaluaties verwacht van het beveiligingssysteem.

Om te beginnen wordt in het Bkse, Artikel 22f, 2e lid, gevraagd om een jaarlijkse een evaluatieprogramma uit te voeren. De ANVS verzoekt om de resultaten van die evaluatie binnen de maand na uitvoering aan haar toe te zenden. De onderwerpen die de ANVS verwacht behandeld te zien, zijn terug te vinden in bijlage 3.

Verder moet er in navolging van Artikel 22c, 1e en 2e lid een gewijzigd beveiligingspakket opgesteld worden, nadat de referentiedreiging is gewijzigd. Dit gebeurt in de praktijk ongeveer elke drie jaar. Hierbij evalueert de vergunninghouder of het beveiligingssysteem nog voldoende weerstand biedt tegen de referentiedreiging.

Tenslotte wordt er ook in het kader van de tienjaarlijkse evaluatie (10EVA) gevraagd om naar beveiliging te kijken (zie handreiking tienjaarlijkse evaluatie nucleaire installaties). Specifiek wordt hier naar de stand der techniek gevraagd, en naar de relatie tot veiligheid. Wat de stand der techniek betreft, kan in 10EVA verwezen worden naar de laatste update van het beveiligingspakket. De enige bijkomstige analyse die dan nog dient te gebeuren, betreft de safety-security interface. De vergunninghouder geeft hierbij invulling aan Artikel 22, 5e lid van het Bkse waarin staat dat beveiligingsmaatregelen en veiligheidsmaatregelen elkaar moeten complementeren en niet belemmeren, en dat hij zodanige maatregelen moet treffen dat het ontstaan van mogelijk conflicten tussen deze, zoveel mogelijk wordt tegengegaan en zo spoedig mogelijk worden opgeheven.

| Soort evaluatie en frequentie | Focus |
|---|---|
| Jaarlijkse evaluatie + na beveiligingsinbreuk | Controleren, testen en oefenen.<br>Zie ook bijlage 3 |
| Bij nieuwe DBT (ca elke drie jaar) | Effectiviteit ten opzichte van de dreiging in de DBT |
| Tienjaarlijks (10EVA) | Safety-security interface |

# Bijlage 1: Overzicht met maatregelen voor informatiebeveiliging

**Gebruikte acroniemen:**

**ETS** Elektronisch Toegangssysteem.

**IDSS** Indringer Detectie en Signalering (Systeem).

**PSM** Plant Security Manager

**TBB** Te Beveiligen Belangen, waaronder (1) alle informatie aangewezen onder het Geheimhoudingsbesluit Kernenergiewet, en (2) alle informatie waarvan de compromittering zou kunnen leiden tot een verhoging van het risico op diefstal van categorie I, II of III kernmateriaal, of tot sabotage met radiologische consequenties boven de URC-limiet.

| Categorie | ID | Maatregel |
|---|---|---|
| 1. Bestuur en organisatie | 1.1 | Bij het samenstellen van alle maatregelen wordt het “Need-to-Know” principe toegepast. |
| | 1.2 | De organisatie garandeert dat TBB slechts op Nederlands grondgebied wordt gegenereerd, bewerkt en opgeslagen (fysiek of digitaal). Afwijkingen hiervan behoeven voorafgaande goedkeuring door de ANVS. |
| | 1.3 | De organisatie geeft voorlichting aan medewerkers die werken met TBB betreffende de procedures en de bijbehorende verantwoordelijkheden, bij aanstelling op een vertrouwensfunctie en vervolgens periodiek, doch tenminste eenmaal per jaar. |
| 2. Incidenten | 2.1 | Er is een procedure opgesteld voor het behandelen van informatiebeveiligings-incidenten. Deze is bekend bij allen die werken aan of toegang hebben tot een TBB. |
| | 2.2 | Gegevens t.a.v. toegang tot en inzicht in een TBB zijn vastgelegd en worden gedurende de aangegeven periode bewaard om achteraf onderzoek naar vermoede beveiligings-incidenten mogelijk te maken. |
| 3. Personeel | 3.1 | Een geldige VGB voor het vervullen van een vertrouwensfunctie is aanwezig voor alle betrokken medewerkers en deze is niet ouder dan 5 jaar. |
| | 3.2 | Toegang tot TBB is zonder geldige VGB niet toegestaan. |
| | 3.5 | Een overzicht van alle de VGB, de VOG en verklaringen van bekendheid met de geheimhoudingsplicht is aanwezig. |
| | 3.9 | Na het beëindigen van de arbeidsovereenkomst zijn alle (fysieke en digitale) TBB terug-gegeven aan de organisatie. In het Beveiligingsplan is het proces hiervoor beschreven. |
| 4. Fysiek | 4.1 | TBB moet worden beveiligd zodat enerzijds compromittering wordt voorkomen en anderzijds compromittering wordt gedetecteerd/gesignaleerd. |
| | 4.2 | Fysieke toegang tot het compartiment met een TBB is tot op individueel niveau controleerbaar. |
| | 4.3 | Toegang tot het TBB of compartiment is alleen door middel van Two-factor Authenticatie verleend. |
| | 4.4 | Alleen een geautoriseerd persoon kan zelfstandig toegang krijgen tot een TBB of tot een compartiment waarin zich een TBB bevindt. |
| | 4.5 | In alle compartimenten met een TBB wordt personeel zonder autorisatie (zoals bezoekers) begeleid door personeel met een autorisatie. Van personen zonder autorisatie is vooraf de identiteit vastgesteld en geregistreerd. De registratie hiervan wordt minimaal een jaar bewaard. |

| Categorie | ID | Maatregel |
|---|---|---|
| 4. Fysiek (vervolg) | 4.6 | De uitgifte van sleutels voor toegang tot compartimenten en opbergmiddelen met een TBB is geregistreerd. Bij de uitgifte van sleutels is gecontroleerd of men over een autorisatie beschikt. De registratie hiervan wordt minimaal een jaar bewaard. Sleutels zijn voor zo min mogelijk personen toegankelijk. |
| | 4.7 | Er zijn uitsluitend sleutels gebruikt. |
| | 4.8 | Cijfercombinaties en sleutels van opbergmiddelen en compartimenten dienen opgeborgen/beveiligd te worden overeenkomstig het beveiligingsniveau van het desbetreffende TBB. |
| | 4.9 | Cijfercombinaties van sloten worden, zonder dat een eerder gebruikte combinatie wordt gekozen, veranderd:<br>- indien een nieuw opbergmiddel of slot in gebruik wordt genomen;<br>- indien een medewerker die de combinatie kent, wordt overgeplaatst;<br>- indien wordt vermoed of vaststaat dat compromittering heeft plaatsgevonden;<br>- uiterlijk zes maanden na de laatste wijziging van de combinatie. |
| | 4.10 | Alvorens een TBB buiten het reguliere, in het beveiligingsplan beschreven, proces te plaatsen, is hier toestemming voor verkregen. De beveiliging van het TBB wordt hierbij op hetzelfde niveau gehouden. |
| | 4.11 | Het “Clear Desk principe” en “clear screen principe”is toegepast in alle compartimenten waar zich een TBB bevindt of kan bevinden. Een TBB wordt niet onbeveiligd achter gelaten. |
| | 4.12 | Beheer- en instandhoudingsmaatregelen zijn getroffen om beveiligingsmaatregelen blijvend te laten functioneren. |
| | 4.13 | Het verlies van een authenticatiemiddel voor TBB, zoals (elektronische) sleutel, dient behandeld te worden als een Beveiligingsincident. |
| | 4.14 | Compartimenten met een TBB zijn afsluitbaar. |
| | 4.15 | In het beveiligingsplan is een sluit- en sleutelplan opgenomen. Ramen, deuren en opbergmiddelen zijn afgesloten bij afwezigheid van geautoriseerd personeel. |
| | 4.16 | Een compartiment waarin een TBB is opgeborgen is afgesloten met een slot voorzien van een gecertificeerde cilinder en sleutels. Wanneer een slot met een cilinder niet kan worden toegepast, wordt een gelijkwaardig gecertificeerd of getest mechanisme gebruikt, waardoor onbevoegd betreden niet mogelijk is zonder sporen van braak. |
| | 4.17 | Toegangsdeuren met een elektronisch toegangssysteem (ETS) die toegang geven tot TBB zijn voorzien van een deurdranger en een (elektronisch en akoestisch) alarm tegen te lang openstaan. |
| | 4.18 | Nooddeuren in het compartiment zijn alleen naar buiten toe te openen. Bij openen klinkt een elektronisch of akoestisch signaal. |
| | 4.19 | Het compartiment met een TBB of een opbergmiddel met een TBB, zijn op alle vlakken (drie dimensionaal) van inbraakwerende maatregelen voorzien volgens geldende normen. |
| | 4.20 | Opbergmiddelen tot 1000 kilogram zijn verankerd. |
| | 4.21 | De ramen en glazen wanden in een compartiment met een TBB zijn voorzien van inkijk beperkende maatregelen. |
| | 4.22 | Er zijn voorzieningen getroffen om elektronische apparatuur die niet strikt noodzakelijk zijn voor het uitvoeren van werkzaamheden buiten de compartimenten te houden. |

| Categorie | ID | Maatregel |
|---|---|---|
| 5. Elektronisch | 5.1 | Het compartiment waarin een opbergmiddel met een TBB is geplaatst, is voorzien van een IDSS. |
| | 5.2 | In een ruimte met een TBB zijn geen camera's, smartdevices, microfoons of andere apparatuur met een opnamefunctionaliteit aanwezig. |
| | 5.3 | Er is een ETS voor gecontroleerde toegang tot het compartiment geïnstalleerd en in werking. |
| 6. Respons | 6.1 | Meldingen uit het IDSS en het ETS moeten leiden tot tijdige interventie. |
| | 6.2 | Na een alarm vindt controle van het compartiment met een TBB plaats door de organisatie. |
| | 6.3 | Personeel dat alarmverificatie uitvoert, heeft ten tijde van de alarmverificatie niet de beschikking over sleutels of codes die toegang geven tot het TBB. |
| 7. Transport en verzenden | 7.1 | Een TBB wordt uitsluitend buiten het compartiment gebracht als dit voor de voortgang van de werkzaamheden absoluut noodzakelijk is. |
| | 7.2 | De organisatie stelt voorschriften op voor het transporteren en verzenden van een TBB en houdt hier toezicht op. |
| | 7.3 | Een TBB mag nooit mee naar huis worden genomen. |
| | 7.4 | Elektronische verzending van TBB, ook versleuteld, is niet toegestaan. |
| 8. Verwerking en ontwikkeling | 8.1 | Geregistreerd is wie TBB onder zijn berusting heeft, werkzaamheden hiermee heeft uitgevoerd of heeft ingezien. |
| | 8.2 | De organisatie beschikt over een procedure ter markering van nieuw opgestelde informatie en houdt hier toezicht op. |
| | 8.3 | De organisatie beschikt over een procedure ter vernietiging van nieuw opgestelde informatie en houdt hier toezicht op. |
| 9. Digitaal gebruik | 9.1 | ICT-bedrijfsmiddelen die relevant zijn voor het verwerken of beveiligen van TBB worden niet gebruikt voor niet-TBB-gerelateerde activiteiten. |
| | 9.2 | Er is een actuele beschrijving van de ICT-infrastructuur beschikbaar die relevant zijn voor het verwerken of beveiligen van TBB. |
| | 9.3 | Een netwerk waarop TBB zijn opgeslagen, heeft geen verbinding met een ander netwerk. |
| | 9.4 | Beheer op afstand van apparatuur en systemen die relevant zijn voor het verwerken of beveiligen van TBB is niet toegestaan. |
| | 9.5 | Het gebruik van een public of private clouddienst (computing, opslag, transport) is niet toegestaan voor de verwerking en opslag van TBB. |
| | 9.6 | Er zijn procedures voor de behandeling van gegevensdragers die ingaan op ontvangst, opslag, rubricering, toegangsbeperkingen, verzending, hergebruik en vernietiging. |
| | 9.7 | Het gebruik van draadloze communicatie is niet toegestaan voor het werken met TBB. |
| | 9.8 | Telewerken met TBB is niet toegestaan. |

# Bijlage 2: Beveiligingspakket Nucleaire Inrichting

(Inrichting)

**Deze template is ongerubriceerd. Na invulling geldt het Geheimhoudingsbesluit Kernenergiewet en moet het rubriceringsniveau vermeld worden.**

# Inhoud

# Bijlage 2: Beveiligingspakket Nucleaire Inrichting

**(Inrichting)**

## Deel A.1: Gegevens Nucleaire Inrichting

Deel A bevat informatie over de vergunninghouder en installaties, die samen voldoende overzicht geeft over de meest relevante beveiligingsrisico's en de beheersing daarvan.

| Kolom A<br>Referentie | Kolom B<br>Basisinformatie | Kolom C<br>Antwoord |
|---|---|---|
| **1** | **Vergunninghouder / Installatie** | |
| 1.1 | Type inrichting | |
| 1.2 | Naam vergunninghouder volgens Kernenergiewetvergunning | |
| 1.3 | ANVS Kenmerk Kernenergiewetvergunning | |
| 1.4 | Datum afgifte vigerende Kernenergiewetvergunning | |
| 1.5 | Fysieke adres installatie | |
| 1.6 | Naam vertegenwoordiger vergunninghouder | |
| 1.7 | Andere vergunningen | |
| 1.8 | DBT-profielen van toepassing op de inrichting | |
| **2** | **Beveiligingsdeskundige** | |
| 2.1 | Naam aangewezen beveiligingsdeskundige | |
| 2.2 | Naam aangewezen plv. beveiligingsdeskundige | |
| **3** | **Contactgegevens** | |
| 3.1 | Algemeen nummer vergunninghouder | |
| 3.2 | Telefoonnummer te gebruiken bij beveiligingsincidenten (24/7) | |
| 3.3 | Andere noodnummers (met toelichting) | |
| 3.4 | Telefoonnummer aangewezen beveiligingsdeskundige | |
| 3.5 | E-mail adres aangewezen beveiligingsdeskundige | |
| 3.6 | Telefoonnummer aangewezen plv. beveiligingsdeskundige | |
| 3.7 | E-mail adres aangewezen plv. beveiligingsdeskundige | |
| **4** | **Gegevens andere radioactieve stoffen** | |
| 4.1 | Hoogste beveiligingscategorie radioactieve stoffen | |
| **5** | **Gegevens gerubriceerde informatie** | |
| 5.1 | Hoogst mogelijke rubricering aanwezige informatie | |
| 5.2 | Informatie aanwezig in fysieke vorm | |
| 5.3 | Informatie aanwezig in digitale vorm | |

| Kolom A<br>Referentie | Kolom B<br>Basisinformatie | Kolom C<br>Antwoord |
|---|---|---|
| **6** | **Gegevens beveiligingsgebieden** | |
| 6.1 | Aantal afzonderlijke observatiegebieden | |
| 6.2 | Aantal afzonderlijke beveiligde gebieden | |
| 6.3 | Aantal afzonderlijke vitale gebieden | |
| 6.4 | Aantal fysieke gebieden waarin gerubriceerde informatie opgeslagen en gebruikt wordt | |
| **7** | **Externe Beveiligingsorganisatie** | |
| 7.1 | Verantwoordelijke politieregio | |
| 7.2 | Contactpersoon bij politie | |
| 7.3 | Datum laatste herziening van de schriftelijke afspraken met de politie | |
| **8** | **Vertrouwensfuncties** | |
| 8.1 | Datum laatste herziening van de lijst vertrouwensfuncties | |
| 8.2 | Aantal personen geplaatst op vertrouwensfuncties | |

## Deel A.2: Gegevens nucleair materiaal en dosisverwachtingen

| Kolom A<br>Type zone | Kolom B<br>Beschrijving zone | Kolom C<br>Hoogst mogelijke beveiligings-categorie nucleair materiaal per zone | Kolom D<br>Typische samen-stelling, hoeveelheid en vorm nucleair materiaal per zone volgens vergunning | Kolom E<br>Hoogst mogelijke dosis bij incidenten / ongevallen |
|---|---|---|---|---|
| *Gebouw / beveiligd gebied / vitaal gebied* | *Benoem alle beveiligde gebieden en vitale gebieden* | *Cat. I / II / III* | *HEU / LEU / Pu / ...*<br>*Bestraald / niet bestraald*<br>*Verrijkingsgraad*<br>*Hoeveelheid in kilogram*<br>*Vorm van het materiaal* | *Dosis in mSv over 7 dagen, gemeten aan de inrichtingsgrens*<br>*Verwijzing naar analyse* |
| **Gebouw A** | | | | |
| | | | | |
| | | | | |
| **Gebouw B** | | | | |
| | | | | |
| | | | | |

## Deel B: Plattegrond en gebiedsaanwijzing

Deel B bevat plattegronden van de nucleaire inrichting, met ten minste:

1. Plattegrond met de volledige inrichting en de directe omgeving, inclusief aanduiding van alle gebouwen, toegangswegen, en wegen binnen de inrichting.
2. Plattegrond van de inrichting, met aanduiding van de zonering volgens Bkse (observatiegebied, beveiligd gebied, vitaal gebied) en van het Centrale Alarmstation.

## Deel C: Verwijzingstabel

Deel C bevat een overzicht van belangrijke wettelijke verplichtingen betreffende nucleaire beveiliging, en verwijzingen naar de delen van het beveiligingspakket waar aangetoond wordt op welke manier de vergunninghouder aan deze verplichtingen voldoet.

| Kolom A<br>Eisen Bkse (of anders aangegeven) | Kolom B<br>Toelichting | Kolom C<br>Verwijzingen (incl. pagina) |
|---|---|---|
| **Art. 22 (3)** | Analyse van de beveiligingsmaatregelen die redelijkerwijs nodig zijn om de inrichting onderscheidenlijk het categorie I-, II-, of III-materiaal te beveiligen tegen de dreigingen zoals omschreven in de referentiedreiging. | |
| **Art. 22 (3)** | Analyse van de beveiligingsmaatregelen die nodig zijn om te voorkomen dat de in de bijlage II genoemde maximale waarde voor de hoeveelheid radioactiviteit geëmitteerd naar de lucht, bepaald overeenkomstig de bijlage II, of de maximale waarden voor de effectieve dosis ontvangen door een lid van de bevolking of een werknemer als bedoeld in artikel 1.2 juncto bijlage 1 van het Besluit basisveiligheidsnormen stralingsbescherming, bepaald overeenkomstig de bijlage II, worden overschreden. | |
| **Art. 22 (4)** | Beschrijving van de aard van het materiaal en de inrichting, en de manier waarop de combinatie en het niveau van de beveiligingsmaatregelen hierop afgestemd is. | |
| **Art. 22 (4)** | Beschrijving van de omvang van de mogelijke gevolgen door blootstelling aan straling van mensen, dieren, planten en goederen in het geval van diefstal of sabotage van categorie I, II, of III-materiaal of van sabotage van inrichtingen, en de manier waarop de combinatie en het niveau van de beveiligingsmaatregelen hierop afgestemd is. | |
| **Art. 22 (5)** | Beschrijving van de manier waarop de vergunninghouder borgt dat beveiligingsmaatregelen en nucleaire veiligheidsmaatregelen zodanig zijn ontworpen en uitgevoerd dat deze elkaar complementeren en niet belemmeren | |
| **Art. 22 (5)** | Beschrijving van de maatregelen dat het ontstaan van mogelijke conflicten tussen de beveiligingsmaatregelen en nucleaire veiligheidsmaatregelen zoveel mogelijk wordt tegengegaan of, waar deze conflicten zich toch zouden voordoen, deze zo spoedig mogelijk worden opgeheven. | |
| **Art. 22a (1)** | Beschrijving van de wijze waarop de inrichting of het categorie I-, II-, en III-materiaal wordt beveiligd, met verwijzing naar de analyse uitgevoerd volgens artikel 3 (1) en (2). | |
| **Art. 22a (1)** | Aanwijzing van een beveiligingsdeskundige en diens plaatsvervanger, die belast zijn met de uitvoering en de naleving van de beveiligingsmaatregelen en die voldoen aan de opleidingseisen, genoemd in de bijlage III en een daarop betrekking hebbend opleidingsplan. | |
| **Art. 22a (1)** | Aanwijzingsbesluit vertrouwensfuncties als bedoeld in artikel 1 van de Wet veiligheidsonderzoeken. | |

| Kolom A<br>Eisen Bkse (of anders aangegeven) | Kolom B<br>Toelichting | Kolom C<br>Verwijzingen (incl. pagina) |
|---|---|---|
| **Art. 22a (1)** | Plan interne beveiligingsorganisatie met ten minste een omschrijving van de interne beveiligingsorganisatie en de daarmee verband houdende verantwoordelijkheden. | |
| **Art. 22a (1)** | Omschrijving van de getroffen en te treffen beveiligingsmaatregelen. | |
| **Art. 22a (1)** | Aanwijzing van een alarmcentrale. | |
| **Art. 22a (1)** | Aanwijzing van een bedrijfsbeveiligingsdienst. | |
| **Art. 22a (1)** | Evaluatieprogramma bestaande uit testen, controles, audits en oefeningen om de doeltreffendheid van de beveiligingsmaatregelen te kunnen beoordelen. | |
| **Art. 22a (1)** | Procedure voor de registratie van personen die toegang hebben of kunnen verlenen tot een vitaal gebied. | |
| **Art. 22a (2)** | Tijdstip waarop plannen en maatregelen zijn uitgevoerd, met een daarop gericht plan van aanpak. | |
| **Art. 22b (1)** | Beschrijving van de manier waarop wijzigingen, en de mogelijke effecten van wijzigingen op het niveau van de beveiliging, beheerd worden (bijvoorbeeld een procedure voor wijzigingsbeheer). | |
| | | |
| **ANVS-Verordening Art. 3.3 (1)** | Beschrijving van verantwoordelijkheden betreffende de fysieke -, informatie-, cyber- en andere beveiligingsaspecten. | |
| **ANVS-Verordening Art. 3.3 (1)** | Beschrijving van verantwoordelijkheden betreffende de uitvoering van taken en maatregelen om gesaboteerd of zoekgeraakt materiaal alsmede informatie tijdig te ontdekken. | |
| **ANVS-Verordening Art. 3.3 (1)** | Beschrijving van verantwoordelijkheden betreffende de mogelijke compenserende maatregelen betreffende het beveiligingspakket | |
| **ANVS-Verordening Art. 3.3 (1)** | Beschrijving van verantwoordelijkheden betreffende het onverwijld informeren van de Autoriteit over de in het derde lid bedoelde gebeurtenissen en situaties. | |
| **ANVS-Verordening Art. 3.3 (2)** | Beschrijving van de bevoegdheden en de instructies van de beveiligingsdeskundige en diens plaatsvervanger. | |
| **ANVS-Verordening Art. 3.3 (2)** | Beschrijving van de bevoegdheden en de instructies van de bedrijfsbeveiligingsdienst. | |
| **ANVS-Verordening Art. 3.3 (2)** | Beschrijving van de bevoegdheden en de instructies van de alarmcentrale. | |
| **ANVS-Verordening Art. 3.3 (3)** | Beschrijving van de maatregelen voor diefstal van categorie I-, II-, of III-materiaal. | |
| **ANVS-Verordening Art. 3.3 (3)** | Beschrijving van de maatregelen voor sabotage van categorie I-, II-, of III-materiaal, of van de inrichting. | |

| Kolom A<br>Eisen Bkse (of anders aangegeven) | Kolom B<br>Toelichting | Kolom C<br>Verwijzingen (incl. pagina) |
|---|---|---|
| **ANVS-Verordening Art. 3.3 (3)** | Beschrijving van de maatregelen voor diefstal of het in de openbaarheid komen van de referentiedreiging, van het beveiligingspakket, of van andere gevoelige informatie aangaande de beveiliging van de inrichting of van categorie I-, II-, of III-materiaal. | |
| **ANVS-Verordening Art. 3.3 (3)** | Beschrijving van de maatregelen voor diefstal of ongewenste wijziging van gerubriceerde informatie. | |
| **ANVS-Verordening Art. 3.3 (3)** | Maatregelen in geval van dreiging van, of een poging tot diefstal of sabotage. | |
| **ANVS-Verordening Art. 3.3 (4)** | Beschrijving van de manier waarop het plan interne beveiligingsorganisatie aansluit aan het plan externe beveiligingsorganisatie | |
| **ANVS-Verordening Art. 3.3 (4)** | Beschrijving van de wijze van optreden van de korps-chef, de burgemeester en de officier van justitie. | |
| **ANVS-Verordening Art. 3.3 (5)** | Een omschrijving van de manier waarop het management van een vergunninghouder voldoet op het punt van beveiliging aan de eisen, opgenomen in bijlage III van de ANVS-Verordening. | |
| **Art. 22 (6)** | Beschrijving van de manier waarop de organisatorische, bouwkundige, elektronische en informatie-beveiligingsmaatregelen ten minste weerstand bieden tegen de dreigingen uit de referentiedreiging en die zorgdragen voor een tijdige respons. | |
| **ANVS-Verordening Art. 3.4** | Beschrijving van de manier waarop beveiligingsmaatregelen zijn getroffen die redelijkerwijs nodig zijn om de alarmcentrale te beveiligen tegen de dreigingen zoals omschreven in de referentiedreiging. | |
| **ANVS-Verordening Art. 3.4** | Beschrijving van de beveiligingsmaatregelen met betrekking op de vakbekwaamheid en betrouwbaarheid van diegenen die de apparatuur in de alarmcentrale ontwerpen, installeren en onderhouden. | |
| **ANVS-Verordening Art. 3.4** | Beschrijving van de beveiligingsmaatregelen met betrekking op technische eisen aan de apparatuur in de alarmcentrale en voorzieningen voor de continuïteit van het functioneren ervan. | |
| **ANVS-Verordening Art. 3.4** | Beschrijving van de beveiligingsmaatregelen met betrekking op de vakbekwaamheid en betrouwbaarheid van diegenen die toegang hebben tot, of werkzaamheden verrichten in de alarmcentrale. | |
| **ANVS-Verordening Art. 3.5 (1)** | Beschrijving van de manier waarop het terrein waarop de inrichting en de daarbij behorende gebouwen zich bevinden is verdeeld in observatiegebied, beveiligd gebied, en vitaal gebied. | |
| **ANVS-Verordening Art. 3.5 (2)** | Beschrijving van de beveiligingsmaatregelen met betrekking op de afscherming en verlichting van observatiegebied, beveiligd gebied, en vitaal gebied, en de gebouwen in die gebieden. | |

| Kolom A<br>Eisen Bkse (of anders aangegeven) | Kolom B<br>Toelichting | Kolom C<br>Verwijzingen (incl. pagina) |
|---|---|---|
| **ANVS-Verordening Art. 3.5 (2)** | Beschrijving van de beveiligingsmaatregelen met betrekking op het toezicht op observatiegebied, beveiligd gebied, en vitaal gebied, en de gebouwen in die gebieden. | |
| **ANVS-Verordening Art. 3.5 (2)** | Beschrijving van de beveiligingsmaatregelen met betrekking op de beperking van toegang en eventuele begeleiding van personen en voertuigen in observatiegebied, beveiligd gebied, en vitaal gebied, en de gebouwen in die gebieden. | |
| **ANVS-Verordening Art. 3.5 (2)** | Beschrijving van de beveiligingsmaatregelen met betrekking op de controle op die toegang. | |
| **ANVS-Verordening Art. 3.5 (2)** | Beschrijving van de beveiligingsmaatregelen met betrekking op het tegengaan van ongewenste beïnvloeding van toegangscontrolesystemen. | |
| **ANVS-Verordening Art. 3.5 (2)** | Beschrijving van de beveiligingsmaatregelen met betrekking op het betreden of binnengaan van het terrein, een gebied of gebouw door voertuigen, personen of goederen. | |
| **Art. 22d** | Beschrijving van de manier waarop de vergunninghouder gebeurtenissen meldt die aan onverkorte toepassing van het beveiligingspakket in de weg staan. | |
| **Art. 22d** | Beschrijving van de manier waarop de vergunninghouder onmiddellijk compenserende maatregelen neemt en deze voorlegt aan de ANVS. | |
| **ANVS-Verordening Art. 3.6** | Beschrijving van de manier waarop de vergunninghouder het evaluatieprogramma uitvoert en het beveiligingspakket jaarlijks op doeltreffendheid beoordeelt. | |
| **Art. 22g** | Beschrijving van de manier waarop de vergunninghouder elke tien jaar beoordeelt of het beveiligingspakket voldoet aan de stand van de techniek. | |

# Bijlage 3: Aanpak Jaarlijkse Evaluatie

De vergunninghouder evalueert jaarlijks de effectiviteit van het nucleaire beveiligingssysteem.

Deze evaluatie houdt rekening met de volgende elementen voor de 12 maanden voorafgaand aan de evaluatie:

- Incidenten met betrekking tot nucleaire beveiliging.
- Technische gegevens over de werking van het beveiligingssysteem, o.a. storingen, foute alarmen, meldingen, doorgevoerde onderhoudswerkzaamheden, uitgevoerde testen, aanpassingen, vervangingen.
- Interne en externe meldingen relevant voor beveiliging, waaronder meldingen door werknemers, rappoorten over near-misses of incidenten.
- Dreigingsinformatie, inclusief onderzoek in open bronnen over nieuw of gewijzigde technische dreigingen, middelen en tactieken.
- Technische informatie over kwetsbaarheden, geschiktheid en effectiviteit van de toegepaste beveiligingsmaatregelen, inclusief Common Vulnerability Disclosure (CVE) informatie en informatie van leveranciers.

De evaluatie bevat de volgende informatie:

- Een overzicht van uitgevoerde beveiligingsoefeningen, met beschrijving van het geoefende scenario, betrokken partijen, oefendoelen, resultaten en (status van) genomen vervolgacties.
- Een overzicht van beveiligingsincidenten, met beschrijving van het incident, resultaten van verder onderzoek, en (status van) genomen vervolgacties. *Voorbeeld*: schending van het vier-ogen principe of toegang door niet-geautoriseerde personen.
- Een overzicht van uitgevoerde wijzigingen met betrekking op nucleaire beveiliging, met de wijzigingscategorie, hierover gemaakte meldingen of verzoeken aan de ANVS, en status van de wijzigingen.
- Een overzicht van aanwezige structuren en systemen met een significante beveiligingsfunctie met vermelding van de leverancier, type systeem, functie, hardware- en softwareversie.
  Voorbeeld: gebruikte technologie voor toegangspaslezers, leverancier, systeemversie.
- Een overzicht van aanwezige structuren, systemen en procedures met een significante beveiligingsfunctie met vermelding van de aantal uitgevoerde tests, meest recente test, en percentage van geslaagde tests.
  Voorbeelden: werking van detectiemiddelen, barrières, communicatiemiddelen, responstijden. Tevens een overzicht van de gemiddelde testfrequentie per systeem en totale percentage van structuren, systemen en procedures met een significante beveiligingsfunctie die in de vorige 12 maanden getest zijn.
- Een overzicht van de invulling van functies belangrijk voor nucleaire beveiliging.

De evaluatie trekt in ieder geval conclusies over de volgende onderwerpen, en onderbouwt deze conclusies met beschikbare gegevens:

- De effectiviteit van het beveiligingssysteem als geheel in relatie tot de referentiedreiging en de formeel vastgestelde en daadwerkelijk geoefende responstijden.
- De noodzaak voor wijzigingen van het beveiligingssysteem op basis van veroudering, testresultaten, effectiviteit of een gewijzigde dreiging.

**Dit document is een uitgave van:**

De Autoriteit Nucleaire Veiligheid
en Stralingsbescherming (ANVS)

Koningskade 4 | 2596 AA Den Haag
Postbus 16001 | 2500 BA Den Haag

www.anvs.nl

Juni 2026