

## **Bijlage - Vragen en uitleg bij de brief oproep tot vergroten weerbaarheid Min OCW (december 2025)**

### **Waarom krijgt mijn organisatie deze brief van de minister?**

- De minister heeft alle erfgoedinstellingen in Nederland deze oproep verstuurd, via de verschillende koepels.
- De minister vindt het belangrijk dat alle collectiebeherende erfgoedinstellingen in het licht van de actuele veiligheidssituatie aan de slag gaan met veiligheidszorg.
- Hij sluit met zijn oproep aan op de aanpak voor het vergroten van de maatschappelijke weerbaarheid door het kabinet.
- Het kabinet roept overheden, instellingen, bedrijven, groeperingen en burgers op gezamenlijk weerbaarheid op te bouwen tegen risico's en bedreigingen.
- Weerbaarheid is een taak van ons allemaal, dus ook van erfgoedinstellingen.
- De oproepbrief sluit aan op de verantwoordelijkheid die erfgoedbeheerders hebben.
- Als we ons erfgoed willen behouden voor toekomstige generaties, is hun inzet cruciaal.

### **Hoe kan ik bij mijn instelling beginnen met het verbeteren van mijn veiligheidszorg?**

- Het is belangrijk dat u niet wacht op een crisis of calamiteit.
- U kunt een start maken met inventariseren van de situatie van uw eigen instelling aan de hand van een aantal vragen, zoals bijvoorbeeld:
  - Welke risico's zijn voor óns relevant?
  - Wat hebben we al geregeld?
  - Wat is een logische volgende stap?
- Een goede eerste stap is de 5 stappen-aanpak 'crisisbewust in vijf stappen'. Deze aanpak ondersteunt erfgoedeigenaren en -beheerders. De publicatie is hier te vinden: <https://www.cultureelerfgoed.nl/documenten/2020/01/01/poster-crisisbewust-in-5-stappen>
- In de voorbereidende fase kunt u al veel doen: een calamiteitenplan opstellen, een crisis- en collectiehulpverleningsteam (CHV-team) samenstellen en oefenen.
- Ook kan duurzame samenwerking met bijvoorbeeld organisaties uit uw omgeving, collega-instellingen en hulpdiensten veel opleveren.

### **Mijn organisatie heeft al een collectiehulpverleningsplan (CHV-plan). Wat zijn goede tips voor vervolgstappen?**

- Omdat crises zich ook door de hele organisatie kunnen voltrekken, is het van belang dat u beziet hoe uw CHV-plan samenhangt met de rest van uw veiligheidsbeleid.
- Een crisis kan immers niet alleen de collectie, maar ook uw gebouw(en), ICT-systemen en werknemers raken.
- Het is belangrijk om scenario's te oefenen om te bezien waar u nog verbeteringen in uw veiligheidsbeleid kunt aanbrengen. <https://www.cultureelerfgoed.nl/onderwerpen/v/veilig-erfgoed/calamiteit-voor-tijdens-na/oefenen-en-opleiden>
- Besteed ook aandacht aan digitale veiligheid. Voor alle culturele en erfgoedinstellingen is het goed om zich bewust te zijn van het gevaar en gevolgen van cyberaanvallen. <https://www.den.nl/cyberveiligheid>
- Lees bijvoorbeeld de ervaringen van het Utrechts Archief dat slachtoffer was: [Culturele organisatie gehackt: Het Utrechts Archief deelt... | DEN](#)

### **Hoe moet ik een selectie- of prioriteitenlijst voor mijn collectie maken?**

- In geval van nood zullen er snel keuzes moeten worden gemaakt over wat u het eerst in veiligheid brengt. Het is verstandig om daar van tevoren over na te denken door het opstellen van een selectie- of prioriteitenlijst.
- Omdat prioriteiten kunnen veranderen door de tijd heen, is het aan te raden om een dergelijke selectie periodiek te herzien.

- Alleen al het gesprek hierover maakt dat er in uw organisatie bewust wordt nagedacht over te maken keuzes. Dit helpt u in een crisissituatie.
- Begin 2026 komt via de website van de Museumvereniging een handreiking beschikbaar om u indien nodig op weg te helpen.

### **Moet ik mijn selectie- of prioriteitenlijst inleveren bij het ministerie of de Rijksdienst voor het Cultureel Erfgoed (RCE)?**

- Nee, dat vragen wij niet van u.
- Het delen van een selectie- of prioriteitenlijst brengt altijd risico's met zich mee.
- Het is van belang dat u goede afspraken maakt over hoe, door wie en met wie uw selectie- of prioriteitenlijsten gedeeld worden.
- Indien u uw selectie- of prioriteitenlijst zou willen gaan delen met hulpdiensten zoals politie of brandweer, kunt u met hen het gesprek aangaan over hoe dit veilig kan. U kunt hierover ook uw [Veiligheidsregio](#) benaderen.

### **Waar vind ik informatie over het verbeteren van mijn veiligheidszorg?**

- Op verschillende websites kunt u informatie vinden:
  - o Rijksdienst voor het Cultureel Erfgoed: <https://www.cultureelerfgoed.nl/onderwerpen/v/veilig-erfgoed>
  - o De kennisbank van OPEN (overleg provinciale erfgoedinstellingen Nederland): <https://www.openerfgoed.nl/> en dan meer specifiek <https://www.openerfgoed.nl/kennisbank-thema/veiligheid-en-risicos/>
  - o De Museumvereniging: <https://museumvereniging.nl/kennisbank/weerbaar-erfgoed-wat-kun-je-zelf-doen/>
  - o Stappenplan cyberveiligheid van DEN: <https://www.den.nl/cyberveiligheid>
- We raden u daarnaast aan in gesprek te gaan met collega-erfgoedbeheerders om van elkaar te leren en samen op te trekken in deze belangrijke opgave.

### **Is er ook op een andere manier hulp en ondersteuning te krijgen?**

- U kunt ook contact opnemen met de organisaties voor erfgoedondersteuning in uw provincie. Voor Friesland zijn dat:
  - Stichting Erfgoed & Publiek: <https://erfgoedpubliek.nl/>
  - Museumfederatie Fryslân: <https://www.museumfederatiefryslan.nl/>
  - Contactpersoon is [Mirjam Pragt](#)
- U kunt voor meer specifieke informatie over uw erfgoeddomein ook terecht bij de verschillende koepels: de Museumvereniging, OPEN, Federatie grote monumentengemeenten, Federatie instandhouding monumenten, Koninklijke Bibliotheek, Nationaal Archief, Monumentenwacht, Stichting Academisch Erfgoed, Provinciaal vakberaad archeologie, Convent van Gemeentelijke Archeologen

### **Ik heb vooral vragen over het verbeteren van de cyberveiligheid van mijn organisatie.**

- Voor cyberveiligheid kunt u een veiligheidscheck die is ontwikkeld door DEN uitvoeren: <https://www.den.nl/kennis-en-inspiratie/cyberveilig-check>
- DEN ontwikkelde daarnaast een stappenplan cyberveiligheid: <https://www.den.nl/kennis-en-inspiratie/cyberveiligheid-in-culturele-organisaties>.

### **Wat doet de overheid voor mij zodat ik mijn veiligheidszorg kan verbeteren?**

- Veiligheidszorg is in de eerste plaats uw eigen verantwoordelijkheid. Om u daarin te ondersteunen, hebben de Rijksdienst voor het Cultureel Erfgoed, OPEN, Museumvereniging en DEN verschillende handreikingen en tools ontwikkeld. Zie hierboven onder: Waar vind ik informatie over het verbeteren van mijn veiligheidszorg?
- Het ministerie verkent daarnaast binnen de Taskforce Veilig Erfgoed in hoeverre de erfgoedsector verder ondersteund kan worden.

- Op de website van de RCE worden actualiteiten vanuit de Taskforce geplaatst bij het onderwerp veilig erfgoed. Zie ook de [terugkoppelingen](#) op de website van Landschap Erfgoed Utrecht.

### **Wat is de Taskforce Veilig Erfgoed en wat heb ik eraan?**

- De Taskforce is ingesteld door de minister van Onderwijs, Cultuur en Wetenschap.
- In de taskforce zijn alle deeldomeinen in de erfgoedsector (musea, monumenten, bibliotheken, archieven, Werelderfgoed), de Nederlandse Unesco Commissie, Blue Shield Nederland, gemeenten, provincies, het ministerie van Defensie en de veiligheidsregio's vertegenwoordigd.
- Het doel is de weerbaarheid van de erfgoedsector te vergroten door een gezamenlijke inspanning van overheden en de sector zelf.
- De Taskforce beoogt de bewustwording van risico's en dreigingen in het erfgoedveld te vergroten en de erfgoedsector op weg te helpen om het erfgoed dat zij beheren beter te beschermen.
- De Taskforce werkt aan concrete acties om de weerbaarheid van de erfgoedsector te verhogen. De Taskforce zet daarbij primair in op het faciliteren van zelfredzaamheid van erfgoedbeheerders en -eigenaren.
- Er is al veel informatie beschikbaar over de veiligheidszorg voor erfgoedinstellingen, maar in de loop van 2026 zal dit verder worden aangevuld, met name met informatie over regionale netwerken en de Veiligheidsregio en over praktische hulpmiddelen voor de erfgoedsector bij oefensituaties en acute nood.

### **Wat kunnen mijn organisatie en ik doen om ons voor te bereiden op hybride dreiging en/of een militaire conflict?**

- Op de website en kennisbank van de RCE is informatie beschikbaar die ondersteunen bij het opstellen van veiligheidsplannen voor de collectie en de organisatie.  
<https://www.cultureelerfgoed.nl/onderwerpen/veilig-erfgoed>
- Besteed ook aandacht aan de digitale kant van uw organisatie (collectiebeheersystemen, installaties, kaartsystemen, etc.).  
Het stappenplan cyberveiligheid van DEN ondersteunt instellingen zich beter voor te bereiden op digitale dreigingen voor de organisatie.  
<https://www.den.nl/kennis-en-inspiratie/cyberveilig-check>

### **Wat is hybride dreiging en wat betekent het voor mijn (erfgoed)instelling?**

- Bij hybride dreiging gaat het om cyberoperaties, spionage en sabotage.
- Zowel bij hybride dreiging als in militaire conflicten kan cultureel erfgoed worden getroffen. In conflicten kan cultureel erfgoed ingezet worden als strategie, variërend van desinformatie en propaganda tot doelbewuste vernietiging. Het is hierom van belang de weerbaarheid van de erfgoedsector te verhogen.

### **Hoe krijg ik meer informatie over wat de Taskforce Veilig Erfgoed gaat opleveren?**

- Op de website van de RCE worden actualiteiten vanuit de Taskforce geplaatst bij het onderwerp veilig erfgoed.
- U kunt voor meer specifieke informatie over uw erfgoeddomein ook terecht bij de verschillende koepels die in de Taskforce vertegenwoordigd zijn: de Museumvereniging, Federatie grote monumentengemeenten, Federatie instandhouding monumenten, Koninklijke Bibliotheek, Nationaal Archief, Monumentenwacht, Stichting Academisch Erfgoed, OPEN (Overleg Provinciale Erfgoedinstellingen Nederland), Provinciaal vakberaad archeologie, IPO, VNG en UNESCO.