Art. 3. Principes van behoedzaam beheer

Om aan de principes van behoedzaam beheer te voldoen dient de exploitant, onderstaande beveiligingsmaatregelen toe te passen en deze te waarborgen in de nodige procedures:

1° De exploitant beheert de fysieke toegang tot zijn netwerk- en informatiesystemen;

2° De exploitant beveiligt zijn netwerk- en informatiesystemen die op afstand toegankelijk zijn, door middel van multifactorauthentificatie;

3° De exploitant installeert zo snel als mogelijk elke beveiligingsupdate van zijn software;

4° De exploitant beveiligt zijn netwerk – en informatiesystemen door firewalls;

5° De exploitant installeert een antivirus;

6° De exploitant beschermt de wifinetwerken door gebruik te maken van versleutelingsnormen;

7° De exploitant maakt back-ups van zijn informatie;

8° De exploitant beschermt de administratortoegang tot zijn netwerk;

9° De exploitant neemt maatregelen om diefstal van componenten van zijn netwerk- en informatiesystemen te voorkomen;

10° De exploitant meldt cyberincidenten aan het Agentschap en het CCB.

Art. 4. Referentiekader

De exploitant van de inrichting waarvan de netwerk- en informatiesystemen ingedeeld zijn in Cyber-5 kan zich baseren op het referentiekader van het niveau "small" gepubliceerd door het CCB, of op andere internationaal aanvaarde technische normen of aanbevelingen van het Internationaal Atoomenergie Agentschap om aan te tonen dat de nucleaire cyberbeveiligingsmaatregelen die hij genomen heeft inderdaad voldoen aan de nucleaire cyberbeveiligingsmaatregelen van behoedzaam beheer.

Art. 5. Dit reglement treedt in werking op 1 januari 2027.

Brussel, 10 september 2026.

Directeur-generaal,
P. ABSIL

Art. 3. Principes de gestion prudente

Pour satisfaire aux principes de gestion prudente, l'exploitant doit appliquer les mesures de sécurité suivantes, ainsi que les procédures garantissant l'application de ces mesures de sécurité :

1° L'exploitant gère les accès physiques à ses réseaux et systèmes d'information ;

2° L'exploitant sécurise ses réseaux et systèmes d'information accessibles à distance au moyen d'une authentification multifactorielle ;

3° L'exploitant installe toute mise à jour de sécurité de ses logiciels dans les meilleurs délais ;

4° L'exploitant sécurise son réseau et ses systèmes d'information par des pare-feux ;

5° L'exploitant installe un antivirus ;

6° L'exploitant protège ses réseaux Wifi en utilisant des normes de cryptage ;

7° L'exploitant fait des sauvegardes de ses informations ;

8° L'exploitant protège l'accès administrateur à son réseau ;

9° L'exploitant prend des mesures pour empêcher le vol de composants de ses réseaux et systèmes d'information ;

10° L'exploitant rapporte les incidents cyber à l'Agence et au CCB.

Art. 4. Cadre de référence

L'exploitant de l'établissement dont les réseaux et les systèmes d'information sont classés Cyber-5 peut s'appuyer sur le cadre de référence du niveau « small » publiés par le CCB ou sur d'autres normes techniques internationalement reconnues ou des recommandations de l'Agence internationale de l'Energie atomique pour démontrer que les mesures de cybersécurité nucléaire qu'il a mises en place constituent bien des mesures de cybersécurité nucléaire de gestion prudente.

Art. 5. Le présent règlement entre en vigueur le 1er janvier 2027.

Bruxelles, le 10 septembre 2026.

Le Directeur général,
P. ABSIL

FEDERAAL AGENTSCHAP VOOR NUCLEAIRE CONTROLE

[C − 2026/006874]

Technisch reglement betreffende de aanstelling van de afgevaardigde van de nucleaire cyberbeveiliging, het nucleaire cyberbeveiligingsdossier, het jaarverslag, de technische voorschriften en het verslag van de testen van de nucleaire cyberbeveiliging van inrichtingen bedoeld in het koninklijk besluit van 9 juli 2026 betreffende de nucleaire cyberbeveiliging

Gelet op de wet van 15 april 1994 betreffende de bescherming van de bevolking en van het leefmilieu tegen de uit ioniserende stralingen voortspruitende gevaren en betreffende het Federaal Agentschap voor Nucleaire Controle, artikel 24*bis* ingevoegd bij wet van 7 mei 2017;

Gelet op het koninklijk besluit van 9 juli 2026 tot uitvoering van artikel 17*sexies* van de wet van 15 april 1994 betreffende de bescherming van de bevolking en van het leefmilieu tegen de uit ioniserende stralingen voortspruitende gevaren en betreffende het Federaal Agentschap voor Nucleaire Controle, de artikelen 8,§ 5, 9,§ 12, 12,§ 2, 13,§ 2, 14,§ 2, 15,§ 5, 18,§ 4, 24 ;

Overwegende het referentiekader bevattende de praktische modaliteiten voor de beoordeling van minimale maatregelen voor het beheer van cyberbeveiligingsrisico's zoals voorzien in artikel 30, § 3 van de NIS2 wet, dat door de nationale cyberbeveiligingsautoriteit , met name via haar website, ter beschikking wordt gesteld van het publiek in toepassing van artikel 4 van het KB van 9 juni 2024 tot uitvoering van de NIS2-wet; momenteel het CyberFundamentals framework.

Besluit:

HOOFDSTUK 1. — *Definities en toepassingsgebied*

Artikel 1. Voor de toepassing van dit reglement wordt verstaan onder:

1° KB betreffende de nucleaire cyberbeveiliging: het koninklijk besluit van 9 juli 2026 tot uitvoering van artikel 17*sexies* van de wet van 15 april 1994 betreffende de bescherming van de bevolking en van het leefmilieu tegen de uit ioniserende stralingen voortspruitende gevaren en betreffende het Federaal Agentschap voor Nucleaire Controle;

AGENCE FEDERALE DE CONTROLE NUCLEAIRE

[C − 2026/006874]

Règlement technique relatif à la désignation du délégué à la cybersécurité nucléaire, au dossier de cybersécurité nucléaire, au rapport annuel, aux prescriptions techniques et au rapport de test de la cybersécurité nucléaire des établissements relevant de l'arrêté royal du 9 juillet 2026 relatif à la cybersécurité nucléaire

Vu la loi du 15 avril 1994 relative à la protection de la population et de l'environnement contre les dangers résultant des rayonnements ionisants et relative à l'Agence fédérale de Contrôle nucléaire, l'article 24*bis*, inséré par la loi du 7 mai 2017 ;

Vu l'arrêté royal du 9 juillet 2026 portant exécution de l'article 17*sexies* de la loi du 15 avril 1994 relative à la protection de la population et de l'environnement contre les dangers résultant des rayonnements ionisants et relative à l'Agence fédérale de Contrôle nucléaire, les articles 8,§ 5, 9,§ 12, 12,§ 2, 13,§ 2, 14,§ 2, 15,§ 5, 18,§ 4, 24 ;

Considérant le cadre de référence reprenant les modalités pratiques d'évaluation des mesures minimales de gestion des risques en matière de cybersécurité visées à l'article 30, § 3, de la loi NIS2 que l'autorité nationale de cybersécurité a mis à disposition du public, notamment sur son site internet, en application de l'article 4 de l'AR du 9 juin 2024 exécutant la loi NIS2, actuellement le CyberFundamentals framework.

Arrête :

CHAPITRE 1er. — *Définitions et champ d'application*

Article 1er. Pour l'application du présent règlement, on entend par :

1° AR relatif à la cybersécurité nucléaire : l'arrêté royal du 9 juillet 2026 portant exécution de l'article 17*sexies* de la loi du 15 avril 1994 relative à la protection de la population et de l'environnement contre les dangers résultant des rayonnements ionisants et relative à l'Agence fédérale de Contrôle nucléaire ;

2° Afgevaardigde voor NCB: de Afgevaardigde voor de Nucleaire cyberbeveiliging die de exploitant moet aanstellen in toepassing van artikel 8 van KB betreffende de nucleaire cyberbeveiliging;

3° Referentiekader: het referentiekader bedoeld in artikel 24 van het KB betreffende de nucleaire cyberbeveiliging.

HOOFDSTUK 2. — *Aanstelling van de Afgevaardigde voor NCB*

Art. 2. § 1. Om een aanvraag tot goedkeuring van de aanstelling van de Afgevaardigde voor NCB bij het Federaal Agentschap voor Nucleaire Controle (hierna het Agentschap) in te dienen, gebruikt de exploitant het formulier dat door het Agentschap op haar website ter beschikking wordt gesteld.

§ 2. Het Agentschap gaat na of de aanvraag tot goedkeuring van de aanstelling van de Afgevaardigde voor NCB volledig is alvorens over te gaan tot een onderzoek ten gronde.

§ 3. Het Agentschap keurt de aanstelling goed of verwerpt deze ten laatste 1 maand na de vaststelling van de volledigheid van de aanvraag. Deze periode kan langer duren indien deze gemotiveerd is

Art. 3. § 1. Indien de Afgevaardigde voor NCB de inrichting verlaat, of voor lange tijd afwezig is, brengt de exploitant het Agentschap hiervan onmiddellijk op de hoogte. De exploitant stelt binnen een termijn van één maand volgend op de kennisgeving aan het Agentschap een nieuwe Afgevaardigde voor NCB aan.

Deze termijn wordt verlengd tot drie maanden indien de afwezigheid van de Afgevaardigde voor NCB te wijten is aan de onmiddellijke beëindiging van de arbeidsovereenkomst of -relatie, of aan het overlijden van de Afgevaardigde voor NCB.

Het Agentschap keurt de aanstelling goed of verwerpt deze in overeenstemming met artikel 2, tenzij het reeds de aanduiding van de plaatsvervangende Afgevaardigde voor NCB heeft goedgekeurd en de exploitant deze plaatsvervanger als nieuwe Afgevaardigde voor NCB aanduidt.

HOOFDSTUK 3. — *Nucleaire cyberbeveiligingsdossier*

Art. 4. § 1. Het nucleair cyberbeveiligingsdossier wordt ingediend aan de hand van het formulier dat door het Agentschap ter beschikking wordt gesteld.

§ 2. Het nucleair cyberbeveiligingsdossier wordt aan het Agentschap overgemaakt conform de van toepassing zijnde regelgeving met betrekking tot het categoriseren van nucleaire of radiologische beveiligingsdocumenten. Voor het elektronisch overmaken wordt het volgend adres gebruikt: cyber@fanc.fgov.be.

Art. 5. Het nucleair cyberbeveiligingsdossier wordt ondertekend door de exploitant en de Afgevaardigde voor NCB.

HOOFDSTUK 4. — *Jaarverslag*

Art. 6. Het jaarverslag dat de Afgevaardigde voor NCB moet opstellen in toepassing van het artikel 9, § 11, van het KB betreffende de nucleaire cyberbeveiliging, dient ten minste de informatie te bevatten die opgenomen is in het formulier dat door het Agentschap ter beschikking wordt gesteld .

Dit verslag moet beveiligd worden rekening houdend met de van toepassing zijnde regelgevingen voor de categorisering van nucleaire of radiologische beveiligingsdocumenten.

HOOFDSTUK 5. — *Technische voorschriften*

Art. 7. De exploitant van de inrichting waarvan de netwerk- en informatiesystemen ingedeeld zijn in Cyber-1 kan zich baseren op het referentiekader van het niveau "essentieel", gepubliceerd door het CCB, of op andere internationaal aanvaarde technische normen of op de aanbevelingen van het Internationaal Atoomenergie Agentschap om aan te tonen dat de nucleaire cyberbeveiligingsmaatregelen die hij genomen heeft inderdaad voldoen aan de nucleaire essentiële cyberbeveiligingsmaatregelen.

Art. 8. De exploitant van de inrichting waarvan de netwerk- en informatiesystemen ingedeeld zijn in Cyber-2 of Cyber-3 kan zich baseren op het referentiekader van het niveau "belangrijk" gepubliceerd door het CCB, of op andere internationaal aanvaarde technische normen of op de aanbevelingen van het Internationaal Atoomenergie Agentschap om aan te tonen dat de nucleaire cyberbeveiligingsmaatregelen die hij genomen heeft inderdaad voldoen aan de nucleaire belangrijke cyberbeveiligingsmaatregelen.

Art. 9. De exploitant van de inrichting waarvan de netwerk- en informatiesystemen ingedeeld zijn in Cyber-4 kan zich baseren op het referentiekader van het niveau "basis", gepubliceerd door het CCB, of op andere internationaal aanvaarde technische normen of op de aanbevelingen van het Internationaal Atoomenergie Agentschap om

2° Délégué à la CSN : le délégué à la cybersécurité nucléaire, que l'exploitant doit désigner en application de l'article 8 de l'AR relatif à la cybersécurité nucléaire ;

3° Cadre de référence : le cadre de référence visé à l'article 24 de l'AR relatif à la cybersécurité nucléaire.

CHAPITRE 2. — *Désignation du Délégué à la CSN*

Art. 2. § 1er. Pour soumettre à l'Agence fédérale de contrôle nucléaire (ci-après l'Agence) la demande d'approbation de sa désignation du Délégué à la CSN, l'exploitant utilise le formulaire que l'Agence met à disposition sur son site web.

§ 2. L'Agence vérifie que la demande d'approbation de la désignation du Délégué à la CSN est complète avant d'en examiner le fond.

§ 3. L'Agence approuve ou rejette la désignation au plus tard un mois après la constatation de la complétude de la demande. Cette période peut être prolongée si cela est justifié.

Art. 3. § 1. Si le Délégué à la CSN quitte l'établissement ou s'en absente pour une longue période, l'exploitant en informe immédiatement l'Agence. L'exploitant désigne un nouveau Délégué à la CSN dans un délai d'un mois à compter de la notification à l'Agence.

Ce délai est porté à trois mois si l'absence du Délégué à la CSN est due à la résiliation immédiate de son contrat ou de sa relation de travail, ou à son décès.

L'Agence approuve ou rejette la désignation selon les modalités prévues à l'article 2, sauf si elle avait déjà approuvé la désignation d'un Délégué à la CSN suppléant et que l'exploitant désigne ce suppléant comme Délégué à la CSN remplaçant.

CHAPITRE 3. — *Le dossier de cybersécurité nucléaire*

Art. 4. § 1er. Le dossier de cybersécurité nucléaire est introduit en utilisant le formulaire que l'Agence met à disposition.

§ 2. Le dossier de cybersécurité nucléaire est transmis à l'Agence conformément à la réglementation en vigueur concernant la catégorisation des documents nucléaires et des documents de sécurité radiologique. Pour la transmission par voie électronique, l'adresse suivante doit être utilisée : cyber@fanc.fgov.be.

Art. 5. Le dossier de cybersécurité nucléaire est signé par l'exploitant et le Délégué à la CSN.

CHAPITRE 4. — *Rapport annuel*

Art. 6. Le rapport annuel établi par le Délégué à la CSN en application de l'article 9, § 11, de l'AR relatif à la cybersécurité nucléaire doit comprendre au moins les informations reprises dans le formulaire que l'Agence met à disposition.

Ce rapport annuel doit être sécurisé conformément à la réglementation en vigueur relative à la classification des documents nucléaires et des documents de sécurité radiologique.

CHAPITRE 5. — *Prescriptions techniques*

Art. 7. L'exploitant de l'établissement dont les réseaux et les systèmes d'information sont classés Cyber-1 peut s'appuyer sur le cadre de référence du niveau « essentiel » publiés par le CCB ou sur d'autres normes techniques internationalement reconnues ou des recommandations de l'Agence internationale de l'Energie atomique pour démontrer que les mesures de cybersécurité nucléaire qu'il a mises en place constituent bien des mesures de cybersécurité nucléaire essentielles.

Art. 8. L'exploitant de l'établissement dont les réseaux et les systèmes d'information sont classés Cyber-2 ou Cyber-3 peut s'appuyer sur le cadre de référence du niveau « important » publiés par le CCB ou sur d'autres techniques internationalement reconnues ou des recommandations de l'Agence internationale de l'Energie atomique pour démontrer que les mesures de cybersécurité nucléaire qu'il a mises en place constituent bien des mesures de cybersécurité nucléaire importantes.

Art. 9. L'exploitant de l'établissement dont les réseaux et les systèmes d'information sont classés Cyber-4 peut s'appuyer sur le cadre de référence du niveau « basique » publiés par le CCB ou sur d'autres techniques internationalement reconnues ou des recommandations de l'Agence internationale de l'Energie atomique pour démontrer que les

aan te tonen dat de nucleaire cyberbeveiligingsmaatregelen die hij genomen heeft inderdaad voldoen aan de nucleaire basis cyberbeveiligingsmaatregelen.

HOOFDSTUK 6. — *Verslag van het testen van de nucleaire cyberbeveiliging*

Art. 10. § 1. Het verslag van de testen zoals voorzien in artikel 15 van het KB betreffende de nucleaire cyberbeveiliging dient ten minste de volgende informatie te bevatten:

1° De specifieke uitgevoerde testen vermelden en aanduiden wat het doel was van elke test;

2° De geteste systemen, netwerken, applicaties of componenten beschrijven;

3° De duurtijd van de testen vermelden;

4° De functies en rollen die betrokken waren in het testproces aangeven;

5° De resultaten van de testen weergeven;

6° Een overzicht geven van de lessen die getrokken werden en de maatregelen die naar aanleiding van deze testen zullen genomen worden.

§ 2. Dit verslag moet beveiligd worden conform de van toepassing zijnde regelgeving met betrekking tot het categoriseren van nucleaire of radiologische beveiligingsdocumenten.

Art. 11. Dit reglement treedt in werking op 1 januari 2027.

Brussel, 10 september 2026.

De Directeur-generaal,
P. ABSIL

mesures de cybersécurité nucléaire qu'il a mises en place constituent bien des mesures de cybersécurité nucléaire de base.

CHAPITRE 6. — *Rapport des tests de la cybersécurité nucléaire*

Art. 10. § 1. Le rapport des tests, comme prévu à l'article 15 de l'AR relatif à la cybersécurité nucléaire doit comprendre au moins les informations suivantes :

1° Mentionner les tests spécifiques qui ont été effectués et indiquer l'objectif de chaque test ;

2° Décrire les systèmes, réseaux, applications ou composants testés ;

3° Mentionner la durée des essais ;

4° Indiquer les fonctions et rôles concernés dans le processus de test ;

5° Donner les résultats de ces tests ;

6° Donner un aperçu des enseignements tirés de ces tests et des mesures qui seront prises à la suite de ces tests.

§ 2. Ce rapport doit être protégé conformément à la réglementation en vigueur relative à la catégorisation des documents nucléaires et des documents de sécurité radiologique.

Art. 11. Le présent règlement entre en vigueur le 1er janvier 2027.

Bruxelles, le 10 septembre 2026.

Le Directeur général,
P. ABSIL

FEDERALE OVERHEIDSDIENST JUSTITIE

[C − 2026/006985]

Rechterlijke Orde

Bij koninklijke besluiten van 10 september 2026,

is mevr. Vancrayebeck N., rechter in de rechtbank van eerste aanleg Luik, aangewezen in de functie van rechter in de familie-en jeugdrechtbank bij deze rechtbank voor een termijn van één jaar, met ingang van 1 oktober 2026.

is mevr. de Wasseige F .,rechter in de rechtbank van eerste aanleg Namen, aangewezen in de functie van rechter in de familie- en jeugdrechtbank van deze rechtbank voor een termijn van één jaar, met ingang van 1 oktober 2026.

Het beroep tot nietigverklaring van de voormelde akten met individuele strekking kan voor de afdeling bestuursrechtspraak van de Raad van State worden gebracht binnen zestig dagen na deze bekendmaking. Het verzoekschrift tot nietigverklaring wordt ofwel per post aangetekend verzonden naar de griffie van de Raad van State, Wetenschapsstraat 33 te 1040 Brussel, ofwel wordt het ingediend volgens de elektronische procedure (zie daarvoor de rubriek "e-procedure" op de website van de Raad van State - http://www.raadvst-consetat.be/).

SERVICE PUBLIC FEDERAL JUSTICE

[C − 2026/006985]

Ordre judiciaire

Par arrêtés royaux du 10 septembre 2026,

Mme Vancrayebeck N., juge au tribunal de première instance de Liège, est désignée aux fonctions de juge au tribunal de la famille et de la jeunesse à ce tribunal, pour un terme d'un an prenant cours le 1er octobre 2026.

Mme de Wasseige F ., juge au tribunal de première instance de Namur, est désignée aux fonctions de juge au tribunal de la famille et de la jeunesse à ce tribunal, pour un terme d'un an prenant cours le 1er octobre 2026.

Le recours en annulation des actes précités à portée individuelle peut être soumis à la section du contentieux administratif du Conseil d'Etat endéans les soixante jours après cette publication. La requête en annulation est adressée au greffe du Conseil d'Etat, rue de la Science 33 à 1040 Bruxelles, soit sous pli recommandé à la poste, soit suivant la procédure électronique (voir à cet effet la rubrique "e-Procédure" sur le site Internet du Conseil d'Etat - http://www.raadvst-consetat.be/).

FEDERALE OVERHEIDSDIENST JUSTITIE

[C − 2026/007060]

Rechterlijke Orde. — Tweede oproep tot kandidaten voor een mandaat van lid van het wetenschappelijk comité van het Instituut voor gerechtelijke opleiding

1. Context

Het wetenschappelijk comité is een orgaan van het Instituut voor gerechtelijke opleiding opgericht door de wet van 31 januari 2007 inzake de gerechtelijke opleiding en kennisbeheer en tot oprichting van het Instituut voor gerechtelijke opleiding.

De opdracht van het wetenschappelijk comité bestaat erin om, op verzoek van de directie en de raad van bestuur of op eigen initiatief, onder meer adviezen te verstrekken of aanbevelingen te doen inzake:

1° het opleidingsbeleid van de magistraten, de gerechtelijke stagiairs en de personen bedoeld in artikel 2,4° tot 10° van voornoemde wet van 31 januari 2007;

2° de opleidingsprogramma's;

3° de organisatie van de opleiding;

4° de pedagogische methodes

5° het kennisbeheer ;

SERVICE PUBLIC FEDERAL JUSTICE

[C − 2026/007060]

Ordre judiciaire. — Deuxième appel aux candidats pour un mandat de membre du comité scientifique de l'Institut de formation judiciaire

1. Contexte

Le comité scientifique est un organe de l'institut de formation judiciaire instauré par la loi du 31 janvier 2007 sur la formation judiciaire et la gestion des connaissances et portant création de l'institut de formation judiciaire.

Le comité scientifique a pour mission de rendre des avis ou de recommander des actions, sur demande de la direction et du conseil d'administration ou d'initiative, notamment en matière de :

1° politique de formation des magistrats, des stagiaires judiciaires et des personnes visées à l'article 2, 4° à 10°, de la loi du 31 janvier 2007 précitée ;

2° programmes de formation ;

3° organisation de la formation ;

4° méthodes pédagogiques ;

5° la gestion des connaissances ;