ICT Beveiligingsbeleid

STICHTING PENSIOENFONDS THALES NEDERLAND
(SPTN)

1. Inhoudsopgave

2. Introductie

2.1. Dit Informatiebeveiligingsbeleid is gebaseerd op Verordening (EU) 2022/2554 inzake betreffende digitale operationele weerbaarheid voor de financiële sector (DORA) inclusief de gedelegeerde technische reguleringsnormen. DORA is van toepassing op SPTN met ingang van 17 januari 2025.

2.2. Dit beleid heeft de doelstelling om een alomvattend kader vast te stellen voor het beheer en de beveiliging van de ICT-activa van SPTN. Het heeft tot doel de vertrouwelijkheid, integriteit, beschikbaarheid en veerkracht van de informatiesystemen en gegevens van SPTN te waarborgen.

2.3. Dit beleid is gericht op het inrichten van een veilige en veerkrachtige ICT-infrastructuur die aansluit bij de strategie van SPTN voor digitale operationele weerbaarheid. De belangrijkste aandachtsgebieden zijn:

- Netwerkbeveiliging; en
- Behoud van de beschikbaarheid, authenticiteit, integriteit en vertrouwelijkheid van gegevens.

2.4. De structuur van dit beleid is gebaseerd op vereisten die DORA stelt aan het ICT-risicobeheerkader van SPTN. De onderstaande secties adresseren een specifiek onderwerp waaraan DORA inhoudelijke eisen stelt ten aanzien ICT-risicoraamwerk.

2.5. Het ICT-risicobeheerkader wordt ten minste jaarlijks geëvalueerd om ervoor te zorgen dat het effectief, relevant en consistent blijft met de informatiebeveiligingsdoelstellingen en het dreigingslandschap van SPTN, zoals uiteengezet in de verschillende beleidsstukken voor digitale operationele weerbaarheid, waaronder het ICT-bedrijfscontinuïteitsbeleid, de Beleidsnotitie IRM en de Beleidsnotitie ICT. Dit beleid wordt indien nodig bijgewerkt om wijzigingen in regelgeving, technologische vooruitgang of de veranderende behoeften van de organisatie weer te geven.

3. Reikwijdte en governance

3.1. Dit beleid is van toepassing op alle verbonden personen van SPTN en alle ICT-dienstverleners van het fonds die toegang hebben tot de informatiesystemen, ICT-activa en gegevens waarvan SPTN gebruik maakt, of die betrokken zijn bij het beheer of het gebruik van deze bronnen.

3.2. Het beleid heeft betrekking op alle ICT-operaties, incl. het beheer, het onderhoud en de monitoring van systemen, netwerken, applicaties en gegevens. Het omvat zowel interne operaties als operaties die worden geleverd door externe (ICT-)dienstverleners en leveranciers.

3.3. Het beleid omvat alle soorten gegevens, inclusief persoonsgegevens, financiële en operationele informatie, in alle ICT-systemen – zowel on-premise als in de cloud – die eigendom zijn van, beheerd of verwerkt worden door of namens SPTN.

3.4. Daarnaast is het beleid van toepassing op alle netwerkapparaten, zoals routers, switches, firewalls en draadloze toegangspunten, alsook alle apparatuur of systemen die betrokken zijn bij netwerkcommunicatie en gegevensoverdracht. Dit omvat zowel interne netwerken als externe verbindingen die worden beheerd door SPTN of de kritieke uitbestedingspartners en ICT-dienstverleners van het fonds.

3.5. De governance in het kader van dit beleid is in de tabel hieronder weergegeven.

Gremium	Verantwoordelijkheden
Algemeen bestuur	• Toezicht op de implementatie en effectiviteit van het risicobeheerkader voor ICT-risicobeheer en informatiebeveiliging.
Dagelijks bestuur, met ondersteuning van Bureau Pensioenzaken	• Monitoren van de ICT-beveiligingspraktijken van SPTN om ervoor te zorgen dat deze voldoen aan DORA en overige relevante regelgeving. • Borgen dat de organisatie voldoet aan haar rapportageverplichtingen onder DORA, inclusief het indienen van de vereiste rapporten bij de relevante autoriteiten.
[Externe] auditor	• Periodieke (interne) audits hebben ten doel de effectiviteit van het informatiebeveiligingsbeleid en de uitvoering van controles te beoordelen.

4. ICT-risicobeheer

4.1. Deze sectie beschrijft het kader en de procedures voor de identificatie, classificatie, beheersing en monitoren van ICT-gerelateerde risico's. Dit is essentieel voor het waarborgen van de vertrouwelijkheid, integriteit en beschikbaarheid van de ICT-systemen, gegevens en -diensten, in overeenstemming met DORA.

4.2. De onderstaande maatregelen heeft SPTN vastgelegd en geïmplementeerd in de ICT-risicoanalyse om alle door ICT ondersteunde bedrijfsfuncties, taken en verantwoordelijkheden, en de informatie- en ICT-activa die deze functies ondersteunen te identificeren, classificeren en documenteren.

Onderwerp	Uitwerking
Risicotolerantie en risicosoorten	• **Risicotolerantie-niveaus:** SPTN definieert en keurt specifieke risicotolerantieniveaus goed voor elk geïdentificeerd type ICT-risico. Deze niveaus zijn vastgesteld om ICT-risico's proactief te beheren en te beperken en tegelijkertijd de beveiliging van kritieke gegevens en systemen te waarborgen. • **Risicosoorten:** Geïdentificeerde risicosoorten omvatten, onder meer, cyberdreigingen, datalekken, systeemstoringen en kwetsbaarheden bij externe (ICT-)dienstverleners.
Risico identificatie en beheersingsmaatregelen	SPTN heeft de volgende maatregelen vastgelegd en geïmplementeerd ten einde de relevante risico's te identificeren en passende maatregelen te implementeren. • **Identificatieproces:** Het systematisch proces om potentiële ICT-

Onderwerp	Uitwerking
	risico's te identificeren, waaronder kwetsbaarheden en bedreigingen die van invloed kunnen zijn op bedrijfsfuncties, ICT-systemen en ondersteunende activa. • **Risicobeheersingsmaatregelen:** Wanneer risico's zijn geïdentificeerd, worden passende beheersingsmaatregelen geïmplementeerd en gedocumenteerd. Deze maatregelen worden periodiek beoordeeld op doeltreffendheid en indien nodig worden corrigerende en mitigerende maatregelen genomen om eventuele kwetsbaarheden aan te pakken. • **Documentatie:** Alle geïdentificeerde risico's en de bijbehorende beheersingsmaatregelen worden gedocumenteerd in een risicoregister, dat wordt bijgehouden en regelmatig wordt bijgewerkt door de ICT-risicobeheerrol.
Risk Assessment methodologie	• SPTN heeft in de Beleidsnotitie ICT een formeel proces en methodologie vastgesteld voor het uitvoeren van regelmatige risicobeoordelingen waaronder ICT-risicobeoordelingen. Dit omvat het evalueren van de waarschijnlijkheid en impact van geïdentificeerde risico's op de bedrijfsvoering en ICT-activa. • Alle risicobeoordelingen worden formeel gedocumenteerd, met een duidelijke identificatie van kwetsbaarheden, bedreigingen en de bijbehorende mitigatiestrategie.
Risicomonitoring	• SPTN heeft doorlopende monitoringprocessen opgezet om ervoor te zorgen dat de geïdentificeerde ICT-risico's binnen de gedefinieerde risicotolerantieniveaus blijven. Op verzoek levert Thales Nederland rapportages aan ten behoeve van de monitoring. Monitoring omvat een voortdurende beoordeling van de effectiviteit van risicobehandelingsmaatregelen. • De Sleutelfunctiehouder Risicobeheer is belast met het aanpassen van het risicobeheerproces als respons op nieuwe bedreigingen en veranderingen in de ICT-omgeving, en zorgt ervoor dat risico's tijdig worden geïdentificeerd en beperkt. De risicobeheersing door Thales Nederland en andere kritieke ICT-dienstverleners wordt gecoördineerd en beoordeeld door het Dagelijks Bestuur, met ondersteuning van het Bureau Pensioenzaken.
Risicomonitoring Restrisico's	• Na de implementatie van risicobehandelingsmaatregelen door SPTN worden eventuele resterende of resterende ICT-risico's in kaart gebracht door het Dagelijks Bestuur, met ondersteuning van het Bureau Pensioenzaken. • Acceptatie van restrisico's die de gedefinieerde tolerantieniveaus overschrijden, moet formeel worden goedgekeurd door het bestuur. • Er wordt een uitgebreide inventarisatie bijgehouden van geaccepteerde ICT-restrisico's, inclusief een gedetailleerde toelichting op de redenen voor de acceptatie ervan.
Integratie met bedrijfsstrategie	• **Consistentie met strategische wijzigingen:** Het ICT-risicobeheerproces sluit nauw aan bij veranderingen in de bedrijfsstrategie van SPTN en de strategie rondom digitale operationele weerbaarheid. Materiële wijzigingen worden

Onderwerp	Uitwerking
	beoordeeld op de mogelijke impact hiervan op het ICT-risicoprofiel van SPTN.
Doorlopende monitoring en aanpassingen	• **Omgevingsmonitoring:** SPTN monitort doorlopend ontwikkelingen en veranderingen in de ICT-omgeving, inclusief interne en externe dreigingen en kwetsbaarheden. Actieve monitoring zorgt voor tijdige signalering van veranderingen die van invloed kunnen zijn op het ICT-risicoprofiel. SPTN wordt via de Pensioenfederatie en via Thales Nederland periodiek geïnformeerd over wijzigingen in het ICT-dreigingslandschap. • **Aanpassing en respons:** De Sleutelfunctiehouder Risicobeheer is verantwoordelijk voor het aanpassen van het risicobeheerproces als respons op nieuwe bedreigingen en veranderingen in het ICT-landschap, en zorgt er in samenwerking met Thales Nederland voor dat risico's tijdig worden geïdentificeerd en beperkt.

5. ICT-activabeheer

5.1. Dit onderdeel heeft betrekking op de ICT-activa. De tabel hieronder beschrijft het effectief beheer van alle ICT-activa om de integriteit, vertrouwelijkheid en beschikbaarheid van informatie en systemen te waarborgen gedurende hun levenscyclus. Dit omvat de identificatie, registratie, het beheer en de bescherming van ICT-activa om de bedrijfsvoering te ondersteunen en te voldoen aan wettelijke vereisten. Thales Nederland voert het beheer van de ICT-activa uit ten behoeve van het fonds. Dit betreft alle software- of hardware in de netwerk- en informatiesystemen die door SPTN worden gebruikt, inclusief netwerken, gegevens en andere technologieën die door SPTN worden gebruikt om bedrijfsprocessen aan te wenden en clouddiensten en andere externe technologieën die daartoe worden aangeschaft (door aankoop of huur).

Onderwerp	Uitwerking
Aanhouden activa register	SPTN heeft alle ICT-activa geregistreerd in een uitgebreide inventarisatie van activa (CMDB). De inventaris moet details vastleggen incl.: • de unieke identificatiecode; • het type activa; • de locatie (fysiek of logisch); • de eigenaar; • vereisten inzake ICT-bedrijfscontinuïteit, met inbegrip van de hersteltijddoelstellingen (RTO's) en de herstelpuntdoelstellingen (RPO's); • of de ICT-asset kan zijn blootgesteld dan wel blootgesteld is aan externe netwerken; en • de configuratie en de levenscyclusstatus de einddata van de gewone, verlengde en op maat gemaakte ondersteuningsdiensten door de derde aanbieder van ICT-diensten. Het Dagelijks Bestuur, met ondersteuning van het Bureau Pensioenzaken, draagt zorg voor de actualisatie van het register en de inventaris wordt regelmatig beoordeeld en bijgewerkt om wijzigingen op te nemen, zoals

Onderwerp	Uitwerking
	nieuwe aanwinsten, buiten gebruik gestelde activa en statuswijzigingen. Het Dagelijks Bestuur, met ondersteuning van het Bureau Pensioenzaken, rapporteert periodiek aan het bestuur over de status van het register.
Activa classificatie en risk assessment	• **Classificatie:** SPTN classificeert ICT-activa op basis van de gevoeligheid en het kritieke karakter. Classificatiecategorieën kunnen omvatten, maar zijn niet beperkt tot, vertrouwelijk, intern gebruik en openbaar. • **Risk assessment:** Het Dagelijks Bestuur, met ondersteuning van het Bureau Pensioenzaken, evalueert de potentiële impact van bedreigingen en kwetsbaarheden op elk bedrijfsmiddel en proces tijdens de jaarlijkse risicobeoordeling. Gebruik de bevindingen om beveiligingsmaatregelen te prioriteren en de bijbehorende risico's te beheren.
Activa beheer verantwoordelijkheden	• **Eigenaarschap:** Het eigendom en de verantwoordelijkheden van ICT-activa wordt toegewezen aan specifieke personen, functies of teams. Eigenaren zijn verantwoordelijk voor het onderhoud, de beveiliging en het juiste gebruik van de aan hun toegewezen ICT-activa. • **Eindverantwoordelijkheid:** Eigenaren van de ICT-activa zijn verantwoordelijk voor de naleving van dit Informatiebeveiligingsbeleid en de procedures van hun activa.
Activa bescherming	• **Beveiligingsmaatregelen:** Thales Nederland implementeert passende beveiligingscontroles om activa te beschermen tegen ongeoorloofde toegang, schade of verlies. Dit kan zowel door fysieke beveiligingsmaatregelen voor hardware als logische beveiligingsmaatregelen voor software en data. • **Toegangscontroles:** Toegang tot ICT-middelen wordt beperkt op basis van rollen en verantwoordelijkheden. Uitsluitend geautoriseerd personeel toegang heeft tot kritieke bedrijfsmiddelen.
Beheer van levenscyclus ICT-activa	• **Acquisitie[1]:** Thales Nederland zorgt ervoor dat bij de aanschaf van nieuwe ICT-activa rekening wordt gehouden met de beveiligingsvereisten. SPTN heeft hiertoe een acquisitie en due diligence proces opgesteld. Dit proces dient ter evaluatie van leveranciers en producten op basis van hun beveiligingsfuncties en naleving van passende industriestandaarden. In het acquisitieproces worden technische (ICT-)specificaties geïdentificeerd waaronder kwaliteitsniveaus, prestatie, interoperabiliteit, milieubescherming, gezondheid, veiligheid of afmetingen, en met inbegrip van de eisen ten aanzien van het product met betrekking tot de naam waaronder het product wordt verkocht, terminologie, symbolen, tests en testmethoden, verpakking, markering of etikettering en conformiteitsbeoordelingsprocedures.

[1] Dit kan worden uitgewerkt in het procurement proces.

Onderwerp	Uitwerking
	• **Onderhoud:** SPTN heeft Thales Nederland ingeschakeld om ICT-activa onderhouden en bij te werken om ervoor te zorgen dat ze veilig en effectief werken, inclusief het toepassen van de nodige patches, updates en upgrades. • **Afwikkeling:** SPTN volgt de procedure van Thales Nederland voor het buiten gebruik stellen en afwikkelen van ICT-activa. De procedure vereist dat gegevens veilig worden gewist en dat hardware, indien nodig, fysiek wordt vernietigd.

6. Encryptie

6.1. Dit onderdeel beschrijft het beleid van SPTN om de vertrouwelijkheid, integriteit en beschikbaarheid van gevoelige gegevens te waarborgen door sterke versleutelingsmechanismen te implementeren voor gegevens in rust en in transit om informatie te beschermen tegen ongeoorloofde toegang en inbreuken.

6.2. SPTN verwacht dat haar ICT-dienstverleners die kritieke of belangrijke functies ondersteunen binnen dit beleid opereert. Ten aanzien van de eigen organisatie maakt SPTN gebruik van Thales Nederland om te voldoen aan deze beleidslijnen.

6.3. Uitbestedingspartijen hanteren regels voor het beheer van cryptografische sleutels tijdens hun gehele levenscyclus, incl. het genereren, vernieuwen, opslaan, back-uppen, archiveren, ophalen, overdragen, intrekken, herroepen en vernietigen van die cryptografische sleutels. Hieronder is het beleid van SPTN ten aanzien van de verschillende onderwerpen beschreven.

Onderwerp	Uitwerking
Encryptie standaarden	• **Industriestandaard algoritmen:** Alle versleuteling moet gebruikmaken van industriestandaard algoritmen zoals AES (Advanced Encryption Standard) met een minimale sleutellengte van 256 bits, of RSA met een minimale sleutellengte van 2048 bits. • **Sleutelbeheer:** Cryptografische sleutels moeten veilig worden gegenereerd, gedistribueerd, opgeslagen en buiten gebruik worden gesteld met behulp van best practices uit de branche.
Data in rust encryptie	• Alle gevoelige gegevens die zijn opgeslagen op media, waaronder databases, bestandssystemen en back-ups, moeten worden versleuteld met behulp van goedgekeurde versleutelingsstandaarden. • Versleuteling wordt geïmplementeerd voor databases, bestandssystemen en opslagapparaten die gevoelige of kritieke informatie bevatten. • Volledige schijfversleuteling (Full Disk Encryption) wordt gebruikt voor apparaten zoals laptops, mobiele apparaten en verwijderbare opslag die waarschijnlijk worden vervoerd of blootgesteld aan fysieke risico's. • Back-upmedia worden versleuteld voordat ze opgeslagen of naar een andere locatie worden verzonden.

Onderwerp	Uitwerking
Data in transit encryptie	• Alle gevoelige gegevens die via netwerken worden verzonden, zowel intern als extern, moeten worden versleuteld om ongeoorloofde toegang of onderschepping te voorkomen. Afhankelijk van de toepassing kan encryptie op één of meer van de volgende niveaus plaatsvinden: - Voorafgaand aan verzenden, op bestandsniveau versleutelen van gevoelige gegevens. - End-to-end encryptie (E2EE) toepassen voor communicatiekanalen zoals e-mail, berichten en services voor het delen van bestanden - API's en webservices dienen gebruik te maken van veilige protocollen, zoals HTTPS. Gebruik maken van TLS (Transport Layer Security) met een minimale versie van 1.3 voor het beveiligen van gegevens die via internet en binnen interne netwerken worden verzonden.
Encryptie sleutelbeheer	• Encryptiesleutels dienen gedurende de gehele levenscyclus beveiligd en beheerd te worden om ongeoorloofde toegang tot versleutelde gegevens te voorkomen. Daarbij worden de volgende uitgangspunten gehanteerd: - Cryptografische sleutels worden gescheiden van de versleutelde gegevens die ze beschermen. - Coderingssleutels worden regelmatig gedraaid en wanneer er een vermoeden van compromittering bestaat. - Een register wordt bijgehouden van alle certificaten en apparaten voor het opslaan van certificaten voor kritieke of belangrijke ICT-activa, en houd dit up-to-date. - Certificaten worden vernieuwd voordat ze zijn verlopen.
	-
Cryptografische controles en updates	• SPTN werkt regelmatig de cryptografische technologie bij of wijzigt deze op basis van de vooruitgang in de cryptoanalyse om weerbaarheid tegen cyberdreigingen te garanderen. • SPTN legt de goedkeuring van mitigerende maatregelen vast en geeft uitleg waar toonaangevende praktijken of normen niet kunnen worden nageleefd.

7. ICT Operaties

7.1. Dit onderdeel beschrijft het beleid om de veilige en veerkrachtige werking van alle ICT-systemen en -diensten binnen SPTN te waarborgen. Hierin worden de noodzakelijke controles en procedures geschetst om de ICT-infrastructuur van SPTN te beschermen en de operationele continuïteit te behouden.

7.2. SPTN vereist dat ICT-dienstverleners die een kritieke of belangrijke functie ondersteunen binnen de kaders van dit beleid opereren. In de tabel hieronder zijn staan de belangrijkste aspecten van ICT-operaties uiteengezet, inclusief de eisen die SPTN daaraan stelt.

Onderwerp	Uitwerking
Capaciteits- en performance-management	• **Capaciteitsplanning:** Beoordeel en plan regelmatig de transactionele capaciteitsbehoeften van ICT-systemen om ervoor te zorgen dat ze de huidige en toekomstige workloads aankunnen zonder de prestaties of beveiliging in gevaar te brengen. Denk aan lange of complexe inkoopprocessen en systemen intensief middelen gebruiken. • **Performance monitoring:** De prestaties van ICT-systemen worden continu bewaakt om eventuele problemen op te sporen en aan te pakken die van invloed kunnen zijn op de operationele efficiëntie of beveiliging. Kwantitatieve en kwalitatieve prestatiestatistieken worden gebruikt om knelpunten of beperkingen van middelen te identificeren en aan te pakken. • **Schaalbaarheid:** ICT-systemen dienen te zijn ontworpen en geconfigureerd om naar behoefte te schalen om aan de toenemende vraag te voldoen, inclusief zowel verticale als horizontale schaalopties. • **Optimalisatie van middelen:** Procedures worden opgesteld en toegepast om het gebruik van middelen te optimaliseren en capaciteitstekorten te voorkomen.
Logging	• Het gebruik van ICT-activa van SPTN en systeemhulpmiddelen wordt gelogd. Een log beschrijft wat er gebeurt binnen systemen. Logging kan informatie genereren als resultaat van onvoorziene omstandigheden of fouten en misbruik. • **Gebeurtenis identificatie:** Elke (kritieke) ICT-dienstverlener heeft duidelijk de gebeurtenissen geïdentificeerd die moeten worden geregistreerd. • **Review:** Elke (kritieke) ICT-dienstverlener voert regelmatig logboekcontroles uit om tekenen van verdachte activiteiten, inbreuken op de beveiliging of operationele problemen te identificeren met betrekking tot de ICT-activa. • **Frequentie:** De frequentie van de logboekbeoordelingen is gebaseerd op risicobeoordelingen en het belang van de gelogde gebeurtenissen. • **Log retentie en beveiliging:** Elke (kritieke) ICT-dienstverlener hanteert bewaarperioden voor logboeken en handhaaft deze en zorgt ervoor dat ze veilig worden opgeslagen en beschermd tegen manipulatie, verwijdering en ongeoorloofde toegang, zowel in rust als tijdens het transport. • **Tools:** Elke (kritieke) ICT-dienstverlener gebruikt, waar mogelijk, hulpprogramma's voor logboekanalyse om het logboekbeoordelingsproces te automatiseren.
Alerts:	• **Configuratie:** Elke (kritieke) ICT-dienstverlener configureert waarschuwingsmechanismen om relevant personeel op de hoogte te stellen van kritieke of ernstige gebeurtenissen die in logboeken zijn gedetecteerd. • **Respons:** SPTN heeft een incidentenregeling en SLA opgesteld waaruit blijkt voor elke (kritieke) ICT-dienstverlener wat het proces is voor een reactie op waarschuwingen, incl. het onderzoeken van mogelijke beveiligingsincidenten, het beoordelen van de impact

	ervan en het nemen van corrigerende maatregelen, indien nodig.
Foutafhandeling	• **Procedures en protocollen:** SPTN heeft, via Thales Nederland, procedures en protocollen opgesteld voor het afhandelen fouten, inclusief het identificeren, rapporteren en oplossen van problemen met ICT-systemen. De gedetailleerde beschrijving is verder uitgewerkt in de Incidentenregeling en het ICT-bedrijfscontinuïteitsbeleid. • **Onderhoudscontracten:** SPTN heeft uitsluitend ICT-activa die 'in-service' is waarbij actuele ondersteunings- en escalatiecontracten van toepassing zijn. Daarnaast bestaan er externe ondersteuningscontacten, in geval van onverwachte operationele of technische problemen. Thales Nederland coördineert en onderhoudt het dagelijks contact met de ICT-dienstverleners. De ondersteunings- en escalatiecontracten worden afgesloten conform de vereisten die worden gesteld aan contracten met ICT-dienstverleners, dan wel opgenomen in de SLA met ICT-dienstverleners. • **Systeemherstel:** Thales Nederland heeft, namens SPTN, procedures geïmplementeerd en gedocumenteerd voor het opnieuw opstarten, terugdraaien en herstellen van ICT-systemen die kunnen worden gebruikt in geval van verstoring van het ICT-systeem.
Ontwikkeling en testen	SPTN ontwikkelt geen ICT-activa, het maakt uitsluitend gebruik van ICT-activa die reeds ontwikkeld, getest en in productie zijn. Er wordt ook geen gebruikgemaakt van bètaversies van programmatuur. SPTN stelt de volgende voorwaarden aan ICT-Dienstverleners met betrekking tot ontwikkeling en het testen van zijn ICT-activa die betrekking hebben op (kritieke of belangrijke) uitbestede functies. • **Scheiding omgeving:** ontwikkelings-, test- en andere omgevingen dienen te worden gescheiden van ICT-productieomgevingen. Ontwikkeling en tests worden daarnaast uitgevoerd in afzonderlijke omgevingen zodat wordt voorkomen dat de productieactiviteiten worden verstoord. • **Tests in productie:** Alle gevallen waarin tests worden uitgevoerd in de productieomgeving, geïdentificeerd, beargumenteerd en uitdrukkelijk goedgekeurd. Het testen blijft beperkt tot specifieke, goedgekeurde gevallen.

8. Netwerkbeveiliging

8.1. Dit onderdeel beschrijft de netwerkbeveiligingsmaatregelen die getroffen worden om de ICT-infrastructuur van SPTN te beschermen tegen ongeoorloofde toegang, cyberdreigingen en operationele verstoringen. Dit beleid beschrijft de noodzakelijke controles en praktijken om de beveiliging, integriteit en beschikbaarheid van netwerkbronnen te waarborgen. Thales Nederland voert de maatregelen omtrent het netwerkbeveiligingsbeleid uit en adviseert in de keuzes. Elke ICT-dienstverlener opereert binnen het netwerkbeveiligingsbeleid van SPTN. De belangrijkste aspecten rond netwerkbeveiliging staan in de tabel hieronder.

Onderwerp	Uitwerking

Netwerksegregatie en segmentatie	Groepen van informatiediensten, gebruikers en -systemen worden in verschillende netwerken gescheiden. Bij de netwerksegregatie en segmentatie worden de volgende uitgangspunten gehanteerd.
	
	• **Segregatie en segmentatie:** Netwerksegregatie en segmentatie wordt uitgevoerd op basis van de volgende parameters:
	  - Het kritieke of belangrijke karakter van de functies die door ICT-systemen worden ondersteund.
	  - De vastgestelde risicoclassificatie van het ICT-actief.
	  - Het algemene risicoprofiel van ICT-activa die gebruikmaken van die ICT-systemen en netwerken.
	  - Onderhouden van uitgebreide documentatie van alle netwerkverbindingen en gegevensstromen om de structuur en interacties binnen het netwerk te begrijpen.
	• **Toegewijd beheernetwerk:** Elke (kritieke) ICT-dienstverlener gebruikt een apart en speciaal netwerk voor het beheer van ICT-activa om ongeoorloofde toegang te voorkomen en een veilig beheer van netwerkapparaten te garanderen.

Netwerk Toegangscontroles	• **Implementatie van toegangscontrole:**
	  - Netwerktoegangscontroles zijn geïmplementeerd om te voorkomen dat ongeautoriseerde apparaten of systemen verbinding maken met het netwerk van SPTN.
	  - Endpoints dienen te voldoen aan de beveiligingsvereisten van de organisatie voordat netwerktoegang wordt verleend.
	• **Versleuteling van netwerkverbindingen:**
	  - Conform het encryptiebeleid wordt versleuteling voor netwerkverbindingen via zakelijke, openbare, huishoudelijke, externe en draadloze netwerken geboden.

Netwerkdesign en beveiliging	• **Beveiligingseisen:** Netwerken worden ontworpen in overeenstemming met de ICT-beveiligingsvereisten, met inbegrip van toonaangevende praktijken om de vertrouwelijkheid, integriteit en beschikbaarheid van de netwerkinfrastructuur te waarborgen. • **Beveiliging dataverkeer:** Netwerkverkeer tussen interne netwerken en externe verbindingen wordt beveiligd, waaronder internet, om datalekken en ongeoorloofde toegang te voorkomen.
Firewall and Filtering Rules	Het verkeer tussen deze netwerksegmenten kan gecontroleerd en/of geblokkeerd worden door beveiligde koppelvlakken en firewalls in te stellen en dit te controleren. • **Firewall-beheer:** Thales Nederland identificeert en specificeert rollen en verantwoordelijkheden voor firewallregels en verbindingsfilters, inclusief het maken, goedkeuren en beoordelen ervan. • De kritieke ICT-dienstverleners controleren en updaten firewallregels regelmatig om opkomende bedreigingen aan te pakken. • Elke zes maanden wordt nagaan of de regels voor systemen die kritieke functies ondersteunen, adequaat zijn.
Isolatie en configuratiebeheer	SPTN hanteert de volgende uitgangspunten voor de isolatie- en configuratiebaseline.

	• **Tijdelijke isolatie:** Er worden maatregelen geïmplementeerd om subnetwerken of netwerkcomponenten tijdelijk te isoleren wanneer dat nodig is om beveiligingsincidenten in te dammen en te beperken. • **Veilige configuratiebaseline:** (Kritieke) ICT-dienstverleners tellen een veilige configuratiebaseline op voor alle netwerkcomponenten. Daarbij dienen de instructies van de ICT-dienstverleners en de toepasselijke normen voor het beveiligen van netwerkapparaten in acht te worden genomen.
Sessiebeheer	• **Time-outs** Er worden procedures of protocollen toegepast om systeem- en externe sessies te beperken, te vergrendelen of te beëindigen na een bepaalde periode van inactiviteit om het risico op ongeoorloofde toegang te verminderen. Deze sessies kunnen worden ingesteld per ICT-actief of netwerk, voor zover passend.
Overeenkomsten voor netwerkdiensten	• **Dienstenspecificaties:** in de dienstverleningsovereenkomst met netwerkbeheerders worden ICT- en informatiebeveiligingsmaatregelen, serviceniveaus en beheersvereisten voor alle netwerkdiensten, ongeacht of deze worden geleverd door interne of externe serviceproviders. • **Nadere contractuele eisen:** de contractuele vereisten zijn verder uitgewerkt in het Uitbestedingsbeleid.
Beveiliging van data in transit	Op basis van de uitkomsten van de goedgekeurde dataclassificatie en van de ICT- risicobeoordeling worden de volgende maatregelen genomen ten aanzien van data in transit van SPTN. Thales Nederland geeft uitvoering aan de implementatie van procedures. • **Waarborgen:** Er worden procedures geïmplementeerd om tijdens de overdracht van gegevens zorg te dragen voor de beschikbaarheid, authenticiteit, integriteit en vertrouwelijkheid. • **Preventie van datalekken: E**r zijn maatregelen geïmplementeerd om gegevenslekken te voorkomen en op te sporen en te zorgen voor een veilige overdracht van informatie tussen SPTN en externe partijen.
Vertrouwelijkheid en geheimhouding	**Geheimhoudingsverplichtingen:** SPTN implementeert, documenteert en evalueert regelmatig vertrouwelijkheids- en geheimhoudingsregelingen om informatie te beschermen. Deze regelingen worden vastgelegd in Gedragscode. Deze geheimhoudingsverplichtingen gelden zowel voor medewerkers van SPTN als voor derden die betrokken zijn bij de gegevensverwerking.

9. ICT project- en verandermanagement

9.1. SPTN waarborgt effectief beheer van ICT-projecten met behoud van de beschikbaarheid, authenticiteit, integriteit en vertrouwelijkheid van gegevens bij de aanschaf, het onderhoud en de ontwikkeling van ICT-activa en -systemen. Zodoende worden wijzigingen op de ICT-infrastructuur (ICT-activa en -diensten) efficiënt en effectief worden doorgevoerd met zo min mogelijk verstoring van de kwaliteit.

9.2. Dit onderdeel adresseert de governance en procesvereisten waaraan ICT-projectmanagement en wijzigingsbeheer dient te voldoen ten aanzien van ICT-activa van SPTN. (Kritieke) ICT-dienstverleners dienen hun project- en wijzigingsmanagement binnen de kaders van dit beleid

uit te voeren.

9.3. SPTN implementeert algemene procedures voor project- en wijzigingsmanagement in samenwerking met zijn (kritieke) ICT-dienstverleners. Deze staan uitgewerkt in de tabel hieronder.

Onderwerp	Uitwerking
Algemene vereisten ICT-projectmanagement en wijzigingsbeheer	• **Managementrapportage:** Het Dagelijks Bestuur wordt geïnformeerd over ICT-projecten die een impact hebben op kritieke of belangrijke functies. Dit gebeurt door middel van individuele verslagen of in geaggregeerde vorm die zowel bij de aanvang als gedurende het betreffende project aan het bestuur worden verstrekt. De rapportage kan periodiek of event-driven plaatsvinden. • **Testen van wijzigingen:** Alle projectvereisten, incl. beveiligingsvereisten, worden of zijn grondig getest voordat ze worden geïmplementeerd. Er is een uitgebreid testplan met functionele, beveiligings- en prestatieaspecten. De volgende punten zijn onderdeel van het testplan. - **Procedures**: De uitvoering van broncodebeoordelingen en het testen van softwarepakketten tijdens de integratie om de beveiliging en functionaliteit te verifiëren. Daarbij worden geanonimiseerde of gepseudonimiseerde gegevens gebruikt en wordt niet gewerkt in productieomgevingen om de integriteit en vertrouwelijkheid van gegevens te beschermen. • **Evaluatie:** Na materiële wijzigingen worden substantiële tests uitgevoerd onder belaste omstandigheden om de veerkracht van het systeem te garanderen.
Inhoudelijke eisen ICT-projectmanagement	SPTN vereist dat ICT-projectmanagement aan de volgende inhoudelijke en kwalitatieve eisen voldoet. Hierin nemen kritieke ICT-dienstverleners van SPTN tevens een plaats in. • **Definiëring projectdoelstelling:** Ieder ICT-project dient duidelijk geformuleerde doelstellingen te hebben om ervoor te zorgen dat ze in overeenstemming zijn met de strategische doelen en wettelijke vereisten van SPTN. Doelstellingen moeten specifiek, meetbaar, haalbaar, relevant en tijdgebonden (SMART) zijn. Ook wordt geformuleerd wat buiten de scope van de projectdoelstelling valt. • **Governancestructuur:** Er is een governancestructuur opgesteld die de rollen en verantwoordelijkheden van de belanghebbenden van het project schetst, waaronder projectsponsors, managers, teamleden en toezichthoudende instanties. Alternatieve governance in noodsituaties wordt hierin uitdrukkelijk meegenomen. • **Besluitvorming:** Beslissingsbevoegdheid en verantwoordingsplicht voor alle projectgerelateerde activiteiten, incl. goedkeuringsprocessen en escalatieprocedures, zijn gedefinieerd. Besluitvorming in noodsituaties wordt hierin uitdrukkelijk meegenomen. • **Projectplanning:** - **Tijdslijn en stappen**: Voor het relevante project wordt een gedetailleerd projectplan ontwikkeld met een tijdlijn, belangrijke mijlpalen en specifieke stappen die nodig zijn om de

	projectdoelstellingen te bereiken. Het plan bevat bepalingen voor regelmatige voortgangsbeoordelingen. - **Allocatie van middelen**: Er worden voldoende middelen toegewezen, waaronder personeel, budget en technologie, op basis van projectvereisten en tijdlijnen. • **Risicobeoordeling:** - **Assessment**: Voorafgaand aan een ICT-project wordt een grondige risicobeoordeling uitgevoerd om potentiële risico's te identificeren met betrekking tot de uitvoering, beveiliging, naleving en operationele impact van het project. Deze risicobeoordeling wordt vastgelegd en goedgekeurd. - **Mitigatie**: er worden risicomitigerende strategieën ontwikkeld en geïmplementeerd om geïdentificeerde risico's aan te pakken en hun impact op het slagen van het ICT-project te minimaliseren. • **Definiëring mijlpalen:** - **Identificatie**: Het projectplan definieert belangrijke mijlpalen die belangrijke voortgangspunten in de levenscyclus van het project markeren. Mijlpalen zijn afgestemd op projectdoelstellingen en kritieke succesfactoren. - **Evaluatie**: De voortgang worden regelmatig geëvalueerd en beoordeeld ten opzichte van mijlpalen om ervoor te zorgen dat het project op schema blijft en om eventuele afwijkingen aan te pakken.
Wijzigingsbeheer	SPTN stelt dat ICT-wijzigingsbeheer aan de volgende inhoudelijke en kwalitatieve uitgangspunten voldoet. • **Proces:** Er is een formeel wijzigingsbeheerproces vastgelegd om wijzigingen in de projectomvang, vereisten of technologie aan te kunnen. Wijzigingen worden geëvalueerd op hun impact op beveiliging, naleving en projectdoelstellingen. • **Documentatie:** Alle wijzigingen worden gedocumenteerd, incl. de grondgedachte, effectbeoordelingen en goedkeuringsgegevens. • **Verificatie:** Bij alle wijzigingen wordt aan de ICT-beveiligingseisen voldaan. Rollen en verantwoordelijkheden voor het specificeren, plannen, overstappen, testen en afronden van wijzigingen zijn gedefinieerd. • **Fallback-procedures:** Terugvalprocedure voor het afbreken of herstellen van mislukte wijzigingen worden geïdentificeerd. • **Noodwijzigingen:** Er is een proces voor het beheer van noodwijzigingen, met inbegrip van documentatie, beoordeling en beoordelingen na de implementatie van hun impact op bestaande ICT-beveiligingsmaatregelen. • **Evaluatie en testing:** Wijzigingen worden geëvalueerd met betrokkenheid van relevante belanghebbenden, zoals gebruikers en kritieke dienstverleners, bij het testproces. • **Databeveiliging in niet-productieomgeving:** In niet-productieomgevingen worden geanonimiseerde, gepseudonimiseerde of gerandomiseerde gegevens gebruikt.
Acquisitie, ontwikkeling en onderhoud –	SPTN zorgt ervoor dat bij de aanschaf van nieuwe ICT-activa rekening wordt gehouden met de beveiligingsvereisten.

algemeen	• Thales Nederland heeft hiertoe een acquisitie en due diligence proces opgesteld. Dit proces dient ter evaluatie van leveranciers en producten op basis van hun beveiligingsfuncties en naleving van passende industriestandaarden. • In het acquisitieproces worden technische specificaties geïdentificeerd waaronder kwaliteitsniveaus, prestatie, interoperabiliteit, milieubescherming, gezondheid, veiligheid of afmetingen, en met inbegrip van de eisen ten aanzien van het product met betrekking tot de naam waaronder het product wordt verkocht, terminologie, symbolen, tests en testmethoden, verpakking, markering of etikettering en conformiteitsbeoordelingsprocedures. • Daarbij wordt bijzondere aandacht voor ICT-beveiligingseisen en de goedkeuring daarvan door de betrokken bedrijfsfunctie en eigenaar van ICT-assets in overeenstemming met de interne governanceregelingen.
Acquisitie, ontwikkeling en onderhoud – beveiligingspraktijken en risicomitigatie	• **Identificatie:** Beveiligingspraktijken en methodologieën met betrekking tot de aanschaf, ontwikkeling en het onderhoud van ICT-systemen worden geïdentificeerd. • **Specificaties en goedkeuring:** SPTN, via haar ICT-dienstverleners, definieert technische specificaties en vereisten, met name gericht op ICT-beveiliging en verkrijgt de benodigde goedkeuringen daarvoor. • **Risicomitigatie:** Om het risico te mitigeren van onbedoelde wijziging of opzettelijke manipulatie van ICT-systemen tijdens ontwikkeling, onderhoud en implementatie te beperken worden maatregelen geïmplementeerd. ICT-activa dienen voor aanschaf te worden geautoriseerd met inachtneming van de risico's voor de ICT-diensten. Voor implementatie van applicaties en/of systeemsoftware wordt gecontroleerd of er een actuele back-up beschikbaar is ten behoeve van een black-out (terugvalscenario) procedure.

10. Fysieke en omgevingsbeveiliging

10.1. Dit onderdeel beschrijft het beleid van SPTN omtrent de fysieke en omgevingsmaatregelen om de beschikbaarheid, authenticiteit, integriteit en vertrouwelijkheid van ICT-activa en gegevens te bewaken. Dit adresseert het risico dat onbevoegden toegang krijgen tot ruimtes met informatie waar ze geen kennis van behoren te nemen dan wel dat informatie kan worden aangepast.

10.2. Het Dagelijks Bestuur, met ondersteuning van het Bureau Pensioenzaken, is verantwoordelijk voor de implementatie en monitoring van de fysieke en omgevingsmaatregelen van SPTN. De onderstaande maatregelen worden belegd bij de Thales Nederland. Kritieke ICT-dienstverleners worden geacht ICT-activa te bewaken binnen de kaders van dit fysieke en omgevingsbeveiligingsbeleid. In de tabel hieronder staan de aspecten van het beleid rond fysieke en omgevingsbeveiliging uiteengezet.

Onderwerp	Uitwerking
Beschermingsmaatregel en omgevingsterrein en	(Kritieke) ICT-dienstverleners hebben maatregelen geïmplementeerd om het kantoorgebouw, datacenters en kwetsbare omgevingsgebieden te

datacentra	beschermen tegen aanvallen, ongevallen en omgevingsdreigingen. Dit betreft in ieder geval onderstaande punten: • **Fysieke barrières:** Kantoorfaciliteiten worden door fysieke barrières beschermd. Hierbij kan gedacht worden aan hekken en poorten van het bedrijfsterrein en het kantoorpand. Daarnaast is het kantoor afgeschermd door beveiligde toegangspunten van om ongeoorloofde toegang te voorkomen. • **Bewaking:** Het kantoorpand beschikt over bewakingssystemen, incl. camera's en alarmsystemen, om de toegang tot het kantoor en overige kwetsbare gebieden te bewaken en vast te leggen. • **Toegangsbewaking:** De (kritieke) ICT-dienstverlener beschikt over (externe) werknemers als taak hebben de toegang tot kwetsbare gebieden te bewaken en te controleren. Hierbij kan gedacht worden aan medewerkers van de kantoorreceptie en beveiliging. Daarbij wordt gebruikgemaakt van de identificatie en logging van natuurlijke personen met geautoriseerde toegang tot bedrijfslocaties. Voor gasten wordt een bezoekerslog bijgehouden en identificatie vereist. • **Beheer van toegangsrechten:** De (kritieke) ICT-dienstverleners kennen enkel fysieke toegangsrechten toe aan geautoriseerde personen tot de bedrijfslocaties en ICT-assets. Deze toegangsrechten worden toegekend op een need-to-know- en least privilege-principes, en op ad-hoc basis. De toegangsrechten zijn gekoppeld aan de functieomschrijving van de desbetreffende (externe) werknemer. • **ICT-activa bescherming:** - **Op locatie:** ICT-activa op het bedrijfsterrein van (kritieke) ICT-dienstverleners wordt beveiligd met behulp van afsluitbare kasten, beveiligde ruimtes en gebieden met beperkte toegang. - **Off-premise:** Beveiligingsmaatregelen voor ICT-activa die buiten het bedrijfsterrein worden opgeslagen of gebruikt, met inbegrip van versleuteling en veilige transportmethoden**.**
Onderhoud en integriteit	• **Onderhoud ICT-activa:** ICT-activa en controleapparatuur, zoals fysieke toegangscontroleapparatuur en omgevingscontroles, worden regelmatig en adequaat onderhouden. De ICT-activa en controleapparatuur wordt onderhouden op basis van onderhoudscontracten en/of facilitaire diensten. • **Controle fysieke toegangssystemen:** fysieke toegangssystemen zoals kaartlezers, biometrische systemen en sloten worden onderhouden en periodiek getest.
Databescherming	• **Clear Desk beleid:** SPTN hanteert een duidelijk clear desk beleid voor alle verbonden personen om ervoor te zorgen dat gevoelige papieren en documenten niet onbeheerd worden achtergelaten in (open) ruimtes. • **Clear screen beleid:** SPTN hanteert een beleid voor clear screen toe om ongeoorloofde inzage van gevoelige informatie op (computer)beeldschermen in te voorkomen.
Rampen- en omgevingsdreiging	De (kritieke) ICT-dienstverleners beschermen ICT-activa tegen rampen- en omgevingsbedreigingen, zoals brand, waterschade en stroomuitval, waarbij rekening wordt gehouden met gevoelige gebieden en het kritieke

	karakter van de activiteiten of ICT-systemen en dat deze passend zijn gedefinieerd. • De beschermingsmaatregelen staan in verhouding tot het kritieke karakter van de ICT-activa die zich in gebouwen en de datacentrales bevinden.
Bescherming van onbeheerd ICT-activa	Onbeheerde ICT-activa wordt beveiligd door onder meer: • **Apparaatvergrendeling:** Gebruikers zijn verantwoordelijk voor het gebruik van vergrendelingsmechanismen van onbeheerde hardware en opslagruimtes. • **Toegangsbeveiliging:** De toegang tot gebieden waar onbeheerde ICT-activa worden opgeslagen of gebruikt dient altijd vergrendeld te worden.

11. ICT-beveiligingseisen rondom verbonden personen

11.1. Dit onderdeel legt de basis voor beveiligingseisen met betrekking tot ICT rondom de verbonden personen van SPTN.

11.2. Het doel is om te waarborgen dat alle bestuurders en overige verbonden personen hun verantwoordelijkheden ten aanzien van ICT-activa volledig begrijpen en in staat zijn om hun rol veilig en effectief te vervullen. Het beleid richt zich op het bevorderen van bewustzijn rondom informatiebeveiliging en de implementatie van strikte toegangsbeperkingen die zijn afgestemd op de functie en verantwoordelijkheden van de gebruiker.

11.3. Door middel van rolgebaseerde toegang wordt het gebruik van kritieke ICT-middelen beperkt tot bevoegde personen, waardoor risico's zoals ongeoorloofde toegang, diefstal, fraude en misbruik worden geminimaliseerd. Daarnaast draagt het beleid bij aan een cultuur van verantwoordelijkheid en integriteit binnen SPTN, waarbij alle gebruikers worden gestimuleerd om veilige werkmethoden te hanteren en potentiële veiligheidsrisico's tijdig te melden.

11.4. SPTN heeft de taak om beveiliging structureel onderdeel te maken van het arbeidsrechtelijke traject (functionering, beoordeling, eed/belofte, screening, disciplinaire maatregelen).

11.5. Het personeelsbeleid van de kritieke ICT-dienstverleners wordt uitgevoerd binnen de kaders van dit deze beleidsuiting van SPTN, om de informatiebeveiliging ten aanzien van ICT-activa te bewaken. De aspecten hiervan staan in de tabel hieronder.

Onderwerp	Uitwerking
Verantwoordelijkheden op het gebied van ICT-beveiliging	SPTN borgt in functiebeschrijvingen de gewenste kwaliteiten en de werkzaamheden met betrekking tot veiligheid op te nemen. • **Toewijzing van verantwoordelijkheden:** Voor alle functies wordt geïdentificeerd welke specifieke ICT-beveiligingsverantwoordelijkheden worden toegekend aan verbonden personen en ICT-dienstverleners met toegang tot ICT-activa. Deze verantwoordelijkheden worden vastgelegd in de functieomschrijving en vastgelegd in het personeelsbestand. De verantwoordelijkheden worden duidelijk gecommuniceerd naar de betreffende personen en ICT-dienstverleners.

	• **Roldefinitie:** De functieomschrijvingen definiëren de verantwoordelijkheden met betrekking tot ICT-beveiliging binnen de organisatie. Aan iedere rol/functie worden passende toegangsrechten en beveiligingsverantwoordelijkheden toegekend.
Vereisten voor personeel en externe (ICT-) dienstverleners	De verbonden personen zijn een cruciale factor voor het slagen van de informatiebeveiliging. De verbonden personen en ICT-dienstverleners dienen kennis te hebben van en te handelen naar de beveiligingsrichtlijnen en het informatiebeveiligingsbeleid. • **Naleving van het ICT-beveiligingsbeleid**: Alle verbonden personen en al het personeel van ICT-dienstverleners worden geïnformeerd over en dienen zich houden aan het ICT-beveiligingsbeleid, de procedures en protocollen. • **Bewustzijn van meldingskanalen**: Verbonden personen worden op de hoogte zijn van en gebruikmaken van gevestigde meldingskanalen voor het detecteren van afwijkend gedrag. Dit omvat meldingskanalen die voldoen aan de Wet bescherming klokkenluiders ingevolge Richtlijn (EU) 2019/1937. • **Teruggave van ICT-activa:** Bij beëindiging van het dienstverband zijn medewerkers verplicht om alle ICT-activa en materiële informatieactiva die tot de organisatie behoren, terug te geven.
Unieke identificatie en authenticatie	• **Unieke identiteitstoewijzing:** Een unieke identiteit en gebruikersaccount wordt toegewezen aan elke verbonden persoon of medewerker van een ICT-dienstverlener die toegang heeft tot de ICT- en informatiemiddelen met betrekking tot SPTN.
Levenscyclus beheer van identiteiten	• **Levenscyclusbeheer:** Er zijn processen voor het maken, wijzigen, beoordelen, tijdelijk deactiveren en beëindigen van gebruikersaccounts. Gegevens over identiteitstoewijzingen worden vastgelegd en bijgehouden. De gegevens worden bijgewerkt na een reorganisatie of beëindiging van contractuele relaties. • **Geautomatiseerde oplossingen:** Waar mogelijk worden geautomatiseerde oplossingen gebruikt voor de levenscyclus van identiteitsbeheer.
Toewijzing van toegangsrechten	• **Principes van toegang:** Toegang tot ICT-activa wordt op basis van de beginselen "need-to-know", "need-to-use" en "least privilege", onder meer voor toegang op afstand en in noodgevallen. • **Scheiding van taken:** Taken worden adequaat gescheiden om ongerechtvaardigde toegang tot kritieke gegevens te voorkomen en om combinaties van toegangsrechten te voorkomen die controles zouden kunnen omzeilen.
Gebruikers-verantwoordelijkheid	• **Minimalisering van generieke accounts:** Het gebruik van generieke en gedeelde accounts wordt beperkt om ervoor te zorgen dat gebruikers identificeerbaar zijn voor acties die binnen ICT-systemen worden uitgevoerd. • **Handhaving van de controle:** Controles om ongeoorloofde toegang tot ICT-activa te voorkomen, worden geïmplementeerd en gehandhaafd.
Procedures voor	• **Toegangsrechten toekennen en intrekken**: Rollen en

accountbeheer	verantwoordelijkheden worden toegekend voor het verlenen, beoordelen en intrekken van toegangsrechten. • **Geprivilegieerde toegang**: Waar nodig wordt geprivilegieerde, nood- en beheerderstoegang toegewezen op basis van need-to-use of ad-hoc vereisten. • **Beëindiging van de toegang**: Toegangsrechten worden onmiddellijk ingetrokken bij beëindiging van het dienstverband of wanneer toegang niet langer nodig is. Een functiewijziging wordt gezien als beëindiging van dienstverband. • **Herziening van toegangsrechten**: Toegangsrechten worden regelmatig bijgewerkt, ten minste jaarlijks voor niet-kritieke functies en iedere 6 maanden kritieke of belangrijke functies.
Verificatiemethoden	• **Vereisten voor authenticatie:** Er worden authenticatiemethoden gebruikt die in verhouding staan tot het risicoprofiel van ICT-activa en die aansluiten bij toonaangevende praktijken. Sterke authenticatiemethoden zijn vereist voor toegang op afstand, geprivilegieerde toegang en toegang tot kritieke of openbaar toegankelijke ICT-activa.
Fysieke toegangscontroles	• **Identificatie en registratie**: Personen die geautoriseerd zijn om toegang te krijgen tot gevoelige gebieden zoals datacenters worden geïdentificeerd en geregistreerd. • **Fysieke toegangsrechten toekennen**: De toegang tot kritieke ICT-activa wordt beperkt tot alleen geautoriseerde personen, op basis van de need-to-know- en least privilege-principes. • **Monitoring**: De fysieke toegang tot gevoelige gebieden wordt bewaakt en gecontroleerd.

Bijlage I – Versiebeheer

Versie	Wijzigingen Bijzonderheden	Auteur	Datum vaststellen
Versie 1 ICT-Beveiligingsbeleid	Initiële vastlegging ICT-Beveiligingsbeleid, in het licht van DORA	AF Advisors	Bestuur 6-12-2024