					Voer hier de naam van de geregistreerde rechtspersoon in							
Documentnummer: P07					Documenttitel: **Onboarding- en offboardingbeleid**							
Versie: 1.0		Ingangsdatum: 01.01.2025			Documenteigenaar:							
X	Beleid		Standaard		Procedure		Formulier		Register		Overig	

Revisiegeschiedenis				
Revisienummer	**Revisiedatum**	**Wijzigingen**	**Beoordeeld door**	**Proceseigenaar**

Goedkeuringen			
Naam	**Functie**	**Datum**	**Handtekening**

Afgestemd op normen en regelgeving

Norm/regelgeving	Clausule/artikel	Opmerking
ISO/IEC 27001:2022	Clausule 7.2, Clausule 6	Competentie van personeel, veilige integratie en handhaving van verantwoordelijkheden bij uitdiensttreding of functiewijziging.
ISO/IEC 27002:2022	Beheersmaatregelen 6.2, 6.5, 5	Beheersmaatregelen voor onboarding, toegangsbeheer en de personeelslevenscyclus.
NIST SP 800-53 Rev.5	PS-4, PS-5, AC-2, AC-6, IA-4, IA-5, CM-5, AU-2, AU-6	Overplaatsing en uitdiensttreding van personeel, least privilege, auditlogging en toegangsbeheer tijdens en na personeelswijzigingen.
EU GDPR	Artikelen 5(1)(f), 25, 32; Overweging 39	Beperking van toegang, vertrouwelijkheid, bescherming en passende beheersmaatregelen voor personeelsgegevens.
EU NIS2	Artikel 21(2)(b, c, d)	Personele en operationele beveiligingsmaatregelen; mitigatie van insider threats; levenscyclusprocessen.
EU DORA	Artikelen 5, 8, 9	Governance, interne ICT-beheersing, ICT-risicobeheer en incidentbeheer tijdens personele overgangen.
COBIT 2019	APO07, BAI08, DSS05, MEA03	Human resources, kennisbeheer, beveiliging en naleving bij onboarding en offboarding.

1. Doel

1.1 Dit beleid stelt gestandaardiseerde procedures vast voor het beheren van onboarding, interne overplaatsingen en uitdiensttreding voor alle typen gebruikers.

1.2 Het waarborgt tijdige en veilige verlening en intrekking van toegangsrechten voor fysieke en logische toegang, met handhaving van vertrouwelijkheid, accountability en teruggave van bedrijfsmiddelen.

1.3 Dit beleid beperkt risico's die samenhangen met ongeautoriseerde toegang, datalekken en niet-geretourneerde bedrijfsmiddelen door onboarding- en offboardingbeheersmaatregelen te verankeren in HR-, IT- en beveiligingsprocessen.

1.4 Dit beleid ondersteunt ISO/IEC 27001:2022 Bijlage A beheersmaatregel 6.5 door te waarborgen dat personele beveiligingsverplichtingen tijdens en na het dienstverband of de opdrachtrelatie worden gehandhaafd.

2. Reikwijdte

2.1 Dit beleid is van toepassing op alle werknemers, contractanten, consultants, leveranciers en andere derden aan wie toegang wordt verleend tot de systemen, netwerken, faciliteiten of gegevens van de organisatie.

2.2 Het beleid regelt de volledige levenscyclus van:

2.2.1 onboarding (indiensttreding, contractering of tijdelijke inzet)

2.2.2 interne overplaatsingen of functiewijzigingen

2.2.3 offboarding (ontslagname, pensionering, beëindiging, afloop van contract)

2.3 Het beleid omvat:

2.3.1 logische toegang (systemen, applicaties, cloud, VPN)

2.3.2 fysieke toegang (toegangsbadges, sleutels, systemen voor gebouventoegang)

2.3.3 toegewezen bedrijfsmiddelen (laptops, telefoons, toegangstokens, inloggegevens)

2.3.4 beleidskennisname en vertrouwelijkheidsverplichtingen

2.4 Alle afdelingen (HR, IT, Facilitair, assetmanagement, Beveiliging en management) zijn verantwoordelijk voor de uitvoering van hun rol in onboarding- en offboardingworkflows.

3. Doelstellingen

3.1 Waarborgen dat aan alle medewerkers pas toegang wordt verleend nadat aan beveiligings-, opleidings- en contractuele randvoorwaarden is voldaan.

3.2 Toegangsrechten intrekken en bedrijfsmiddelen onmiddellijk terugvorderen bij functiewijziging of uitdiensttreding.

3.3 De vertrouwelijkheid, integriteit en beschikbaarheid (CIA) van de informatiesystemen en overige bedrijfsmiddelen van de organisatie tijdens personele overgangen waarborgen.

3.4 Auditeerbaarheid en juridische verdedigbaarheid ondersteunen door volledige registraties van onboarding- en uitdiensttredingsgebeurtenissen te bewaren.

3.5 De blootstelling aan insider threats verminderen door alle toegangsgebeurtenissen met betrekking tot personeel te valideren en te documenteren.

3.6 De personeelslevenscyclus van de organisatie afstemmen op risicogebaseerde beveiligingspraktijken en wettelijke verplichtingen.

4. Rollen en verantwoordelijkheden

4.1 Directie

4.1.1 keurt dit beleid goed en wijst bevoegdheden en middelen toe voor onboarding-, offboarding- en toegangsbeheerprocessen.

4.1.2 waarborgt dat personele overgangen de organisatie niet blootstellen aan onaanvaardbare beveiligings- of juridische risico's.

4.2 Human Resources (HR)

4.2.1 initieert onboarding- en offboardingworkflows voor werknemers en stelt relevante afdelingen in kennis van wijzigingen.

4.2.2 waarborgt dat antecedentenonderzoeken, contracten, geheimhoudingsverklaringen en beleidskennisname zijn afgerond voordat toegang wordt verleend.

4.2.3 informeert IT en Facilitair/assetmanagement over uitdiensttreding van medewerkers overeenkomstig de meldings-SLA.

4.2.4 stemt af met Juridische Zaken en Compliance om verplichtingen na uitdiensttreding af te dwingen, zoals geheimhoudingsclausules.

[... Secties 4.3–8 zijn niet opgenomen in dit voorbeeld. Koop het volledige document voor toegang tot de volledige inhoud. ...]

9. Eisen voor herziening en actualisering

9.1 Frequentie van beleidsbeoordeling

9.1.1 Dit beleid moet worden beoordeeld:

9.1.1.1 jaarlijks, of

9.1.1.2 na elk materieel incident waarbij misbruik van toegang, verlies van bedrijfsmiddelen of een procedureel falen betrokken is

9.1.1.3 bij implementatie van ingrijpende wijzigingen in HR- of IAM-platforms

9.1.1.4 bij regelgevende of juridische actualisaties die gevolgen hebben voor personeelsgegevens of verplichtingen

9.2 Beoordelingsproces en eigenaarschap

9.2.1 De ISMS-manager en de HR-directeur coördineren de beoordeling, met input van IT-beveiliging, Juridische Zaken en Compliance.

9.2.2 Alle wijzigingen moeten worden goedgekeurd door de directie en de ISMS-stuurgroep.

9.2.3 Herziene versies moeten opnieuw worden verspreid onder betrokken afdelingen en medewerkers voor hernieuwde kennisname.

9.3 Documentbeheersing en bewaring

9.3.1 Dit beleid moet het volgende omvatten:

9.3.2 versiebeheer, wijzigingshistorie en ingangsdatum

9.3.3 verantwoordelijke eigenaar en beoordelaar(s)

9.3.4 beleidsclassificatie en goedkeuringsregistratie

9.3.5 Vervallen versies moeten gedurende minimaal 3 jaar worden gearchiveerd overeenkomstig het beleid voor documentbeheer.

10. Gerelateerd beleid en samenhang

10.1.1 Dit beleid hangt rechtstreeks samen met:

10.1.2 P1 – Informatiebeveiligingsbeleid: stelt de beveiligingsdoelstellingen van de organisatie vast, waaronder governance van personele toegang.

10.1.3 P4 – Toegangsbeheerbeleid: bevat operationele vereisten voor het toekennen en intrekken van systeemtoegang en fysieke toegang op basis van onboarding- en offboardingtriggers.

10.1.4 P3 – Beleid inzake aanvaardbaar gebruik: vereist kennisname tijdens onboarding en ondersteunt handhaving na uitdiensttreding.

10.1.5 P6 – Risicobeheerbeleid: waarborgt dat risico's met betrekking tot gebruikerstoegang en personele overgangen worden beoordeeld en gemitigeerd in lijn met de principes van het ISMS.

10.1.6 P11 – Beleid voor beheer van gebruikersaccounts en autorisaties: regelt de technische beheersmaatregelen voor toegangsverlening en intrekking van toegangsrechten ter ondersteuning van dit beleid.

10.2 Deze beleidslijnen vormen een geïntegreerd stelsel van beheersmaatregelen voor het veilig en controleerbaar beheren van gebeurtenissen in de personeelslevenscyclus.

11. Referentienormen en -raamwerken

11.1 Dit beleid is afgestemd op internationaal erkende raamwerken voor beveiliging, privacy en IT-governance om te waarborgen dat onboarding- en offboardingprocessen veilig, traceerbaar en in overeenstemming met juridische en organisatorische vereisten zijn.

11.2 ISO/IEC 27001:

11.2.1 Clausule 7.2 – Competentie en Clausule 6.2 – Doelstellingen voor informatiebeveiliging: dit beleid ondersteunt de ontwikkeling van personele competentie en de veilige integratie van personen in rollen die invloed hebben op ISMS-doelstellingen.

11.2.2 Bijlage A beheersmaatregel 6.5 – Verantwoordelijkheden na uitdiensttreding of wijziging van dienstverband: dit beleid implementeert beheersmaatregelen voor resterende toegangsrechten, gegevensbeheer en contractuele verplichtingen bij vertrek.

11.2.3 Bijlage A beheersmaatregel 5.9 – Screening en 6.2 – Arbeidsvoorwaarden: onboardingprocedures omvatten antecedentenonderzoek en mechanismen voor beleidskennisname die in lijn zijn met deze clausules.

11.3 NIST SP 800-53 Rev.5:

11.3.1 PS-4 (uitdiensttreding van personeel) en PS-5 (overplaatsing van personeel): dit beleid handhaaft de gestructureerde verwijdering of wijziging van toegangsrechten, toegangspassen en bedrijfsmiddelen.

11.3.2 AC-2 (accountbeheer) en AC-6 (least privilege): bepalingen waarborgen dat toegang op de functie is afgestemd en tijdig wordt ingetrokken wanneer deze niet langer noodzakelijk is.

11.3.3 IA-4 (beheer van identificatoren) en IA-5 (beheer van authenticatiemiddelen): ondersteunt veilig beheer van authenticatiemiddelen tijdens en na personeelswijzigingen.

11.3.4 CM-5 (toegangsbeperkingen voor wijzigingen): voorkomt ongeautoriseerde wijzigingen na uitdiensttreding door verhoogde toegangsrechten in te trekken.

11.3.5 AU-2 en AU-6: logging en traceerbaarheid van toegangsgebeurtenissen worden versterkt door integratie van IAM en documentatie en audittrail.

11.4 EU GDPR (2016/679):

11.4.1 Artikel 5(1)(f): beschermt persoonsgegevens tegen ongeautoriseerde toegang, in dit beleid afgedwongen door gebruikerstoegang tijdens offboarding in te trekken.

11.4.2 Artikel 32: schrijft passende technische en organisatorische beheersmaatregelen voor ter beveiliging van persoonsgegevens gedurende de arbeidslevenscyclus.

11.4.3 Artikel 25 – Gegevensbescherming door ontwerp: waarborgt dat onboarding en offboarding gegevensminimalisatie, bewaring en rechtmatige toegangsbeheersmaatregelen integreren.

11.4.4 Overweging 39: benadrukt beperking van toegang en vertrouwelijkheid, ondersteund door de opzet van dit beleid.

11.5 EU NIS2-richtlijn (2022/2555):

11.5.1 Artikel 21(2)(b, c, d): vereist personele en operationele beveiligingsmaatregelen om toegangsbeheer, mitigatie van insider threats en levenscyclusprocessen te adresseren; al deze elementen zijn in dit beleid verwerkt.

11.6 EU DORA (2022/2554):

11.6.1 Artikel 5 – Governance en interne beheersing: dit beleid ondersteunt interne ICT-governance met betrekking tot mensgerelateerd risico en toegangsbeheer.

11.6.2 Artikel 8 – ICT-risicobeheer: past beheersmaatregelen toe op personele overgangen die kritieke bedrijfsmiddelen of gereguleerde omgevingen kunnen blootstellen.

11.6.3 Artikel 9 – Classificatie en beheer van incidenten: waarborgt dat incidenten gerelateerd aan uitdiensttreding meldbaar zijn en worden beperkt door juiste deprovisioning en afhandeling van bedrijfsmiddelen.

11.7 COBIT 2019:

11.7.1 APO07 – Managed Human Resources: definieert rollen, verantwoordelijkheden en levenscyclusacties voor onboarding en uitdiensttreding in lijn met governancedoelstellingen.

11.7.2 BAI08 – Knowledge Management: versterkt de documentatie van procedures, kennisborging en overdracht van beheersing aan het einde van het dienstverband.

11.7.3 DSS05 – Managed Security Services: handhaaft deactivering van gebruikers, beheer van bedrijfsmiddelen en accountability tijdens rolwisselingen.

11.7.4 MEA03 – Monitoren, evalueren en beoordelen van naleving: waarborgt dat onboarding- en offboardingbeheersmaatregelen worden beoordeeld tijdens interne en externe audits.