					Voer hier de naam van de geregistreerde rechtspersoon in							
Documentnummer: P07S					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	Clausules 6.2, 7	Vereisten inzake personeelsbeveiliging en bewustwording
ISO/IEC 27002:2022	Beheersmaatregelen 6.2, 6.5	Beveiligingspraktijken voor onboarding en uitdiensttreding
NIST SP 800-53 Rev.5	PS-4, AC-2, PL-4	Uitdiensttreding van personeel; levenscyclusbeheer van accounts; planning
EU NIS2	Artikel 21(2)(h)	Personeelsbeveiliging en beheer van de levenscyclus van toegangsrechten
EU DORA	Artikel 12	Toegangscontrole en intrekking van toegangsrechten voor ICT-systemen
COBIT 2019	APO07, DSS01	Beveiliging van personeel, logische en fysieke toegangscontroles
EU AVG	Artikel 32	Beveiliging van persoonsgegevens tijdens het dienstverband

1. Doel

1.1 Dit beleid definieert het proces voor de onboarding van nieuwe medewerkers of contractanten en voor de veilige intrekking van toegang wanneer personen uit dienst treden of van functie veranderen.

1.2 Het waarborgt dat toegang wordt verleend volgens het least-privilege-principe, dat alle bedrijfsmiddelen worden geregistreerd en dat kritieke acties, zoals systeemdeactivering en gegevensherstel, tijdig worden uitgevoerd.

1.3 Dit beleid ondersteunt naleving, operationele integriteit en gegevensbescherming door middel van gestructureerde en auditeerbare onboarding- en offboardingactiviteiten.

2. Reikwijdte

2.1 Dit beleid is van toepassing op:

2.1.1 alle vaste en tijdelijke medewerkers

2.1.2 contractanten, consultants en stagiairs

2.1.3 externe dienstverleners met systeemtoegang of fysieke toegang

2.2 Dit beleid omvat:

2.2.1 onboarding: het aanmaken van gebruikersaccounts, het verlenen van toegang en de uitgifte van apparatuur

2.2.2 offboarding: het verwijderen van toegang, het innemen van bedrijfsactiva en het veilig afsluiten van digitale identiteiten

2.2.3 interne functiewijzigingen die herconfiguratie van toegang of herverdeling van bedrijfsmiddelen vereisen

2.3 Dit beleid is van toepassing op alle apparaten, platforms en locaties die worden gebruikt voor officiële bedrijfsactiviteiten.

3. Doelstellingen

3.1 Waarborgen dat nieuwe medewerkers toegang en middelen ontvangen op basis van geverifieerde functies en verantwoordelijkheden.

3.2 Bevestigen dat vertrekkende gebruikers uiterlijk aan het einde van hun laatste werkdag volledig uit systemen en faciliteiten zijn verwijderd.

3.3 Voorkomen van verweesde accounts en niet-ingeleverde bedrijfsmiddelen, aangezien deze een beveiligingsrisico vormen.

3.4 Gedocumenteerde registraties bijhouden van onboarding-, functiewijzigings- en offboardingacties.

3.5 Verantwoordingsplicht bevorderen door middel van checklists en afstemming tussen betrokken functies.

4. Rollen en verantwoordelijkheden

4.1 Algemeen directeur (GM)

4.1.1 Keurt toegang met verhoogde bevoegdheden goed en houdt toezicht op het onboarding- en offboardingprogramma.

4.1.2 Zorgt ervoor dat uitzonderingen worden onderbouwd en dat corrigerende maatregelen worden genomen wanneer processen niet worden gevolgd.

4.2 Office Manager / HR

4.2.1 Start de onboarding van nieuwe medewerkers en stelt IT op de hoogte van uitdiensttredingen.

4.2.2 Zorgt voor de afronding van juridische documenten, zoals een geheimhoudingsovereenkomst, en voor kennisneming van het informatiebeveiligingsbeleid.

4.2.3 Beheert onboarding- en offboardingchecklists en bewaakt de naleving van het beleid.

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

9. Vereisten voor herziening en actualisatie

9.1 Jaarlijkse herziening

9.1.1 Dit beleid moet ten minste eenmaal per jaar worden beoordeeld door de Algemeen directeur (GM) en de verantwoordelijken voor HR en IT.

9.2 Triggers voor eerdere herziening

9.2.1 Actualisatie moet plaatsvinden indien:

9.2.1.1 nieuwe HR- of IT-systemen worden ingevoerd

9.2.1.2 een wijziging plaatsvindt van externe IT-dienstverlener of beheerde HR-dienst

9.2.1.3 beveiligingsaudits proceshiaten aan het licht brengen

9.2.1.4 regelgevende verplichtingen wijzigen, zoals wijzigingen in de AVG

9.2.1.5 een kritieke fout in offboarding of een inbreuk plaatsvindt

9.3 Versiebeheer en goedkeuring

9.3.1 Elke versie van dit beleid moet het volgende bevatten:

9.3.1.1 versienummer en datum

9.3.1.2 samenvatting van wijzigingen

9.3.1.3 goedkeuring door de Algemeen directeur (GM)

9.3.1.4 gearchiveerde eerdere versies die ten minste drie jaar worden bewaard

9.4 Communicatie en kennisneming

9.4.1 Alle medewerkers die verantwoordelijk zijn voor onboarding of uitdiensttreding moeten op de hoogte worden gebracht van beleidsupdates. Jaarlijkse bewustwordingssessies of opfrisbriefings zijn verplicht.

10. Gerelateerde beleidsdocumenten en samenhang

10.1 Dit beleid ondersteunt en wordt ondersteund door het volgende:

10.1.1 P2S – Beleid inzake governancerollen en -verantwoordelijkheden: waarborgt verantwoordingsplicht in toegangs- en onboardingprocessen

10.1.2 P4S – Toegangscontrolebeleid: stelt technische handhaving vast voor rolgebaseerde toegangsverlening en deactivering

10.1.3 P6S – Risicobeheerbeleid: beoordeelt risico's die voortvloeien uit het falen van onboarding- en offboardingmaatregelen

10.1.4 P8S – Beleid voor bewustwording en opleiding op het gebied van informatiebeveiliging: stelt vereisten vast voor introductie van personeel tijdens onboarding

10.1.5 P30S – Incidentresponsbeleid (P30): behandelt het niet intrekken van toegangsrechten of diefstal van bedrijfsmiddelen als beveiligingsincidenten

11. Referentienormen en -kaders

11.1 ISO/IEC 27001

11.1.1 Clausule 6.2 – Stelt vereisten vast voor personeelsbeveiliging

11.1.2 Clausule 7.2 – Verplicht bewustwordingstraining voor nieuwe medewerkers

11.2 ISO/IEC 27002

11.2.1 Beheersmaatregelen 6.2 en 6.5 – Beschrijven beveiligingspraktijken voor onboarding en uitdiensttreding

11.3 NIST SP 800-53 Rev. 5

11.3.1 PS-4 – Procedures voor uitdiensttreding van personeel, inclusief deactivering van toegang

11.3.2 AC-2 – Waarborgt beheer van de levenscyclus van gebruikerstoegang

11.3.3 PL-4 – Vereist planning voor personeelsovergangen

11.4 EU AVG

11.4.1 Artikel 32 – Waarborgt passende beveiliging tijdens en na het dienstverband, met name voor toegang tot persoonsgegevens

11.5 EU NIS2-richtlijn

11.5.1 Artikel 21(2)(h) – Vereist personeelsbeveiliging en beheersmaatregelen voor de levenscyclus van toegangsrechten

11.6 EU DORA

11.6.1 Artikel 12 – Vereist dat gereguleerde financiële entiteiten de toegang van personeel tot ICT-systemen beheersen, inclusief procedures voor intrekking van toegangsrechten

11.7 COBIT 2019

11.7.1 APO07 – Manage Human Resources: stelt vereisten vast voor beveiliging binnen de personeelslevenscyclus

11.7.2 DSS01 – Manage Operations: omvat beheersing van logische en fysieke toegang tijdens overgangen in het dienstverband