					Indsæt navnet på den registrerede juridiske enhed her							
Dokumentnummer: P07S					Dokumenttitel: **Politik for onboarding og fratrædelse**							
Version: 1.0		Ikrafttrædelsesdato: 01.01.2025			Dokumentejer:							
X	Politik		Standard		Procedure		Formular		Register		Andet	

Revisionshistorik				
Revisionsnummer	**Revisionsdato**	**Ændringer**	**Gennemgået af**	**Procesejer**

Godkendelser			
Navn	**Stilling**	**Dato**	**Underskrift**

Tilpasset relevante standarder og reguleringer

Standard/regulering	Klausul/artikel	Kommentar
ISO/IEC 27001:2022	Klausul 6.2, 7	Krav til personalesikkerhed og bevidstgørelse
ISO/IEC 27002:2022	Kontroller 6.2, 6.5	Sikkerhedspraksis for onboarding og fratrædelse
NIST SP 800-53 Rev.5	PS-4, AC-2, PL-4	Fratrædelse af personale, kontolivscyklus og planlægning
EU NIS2	Artikel 21(2)(h)	Personalesikkerhed og livscyklusstyring af adgange
EU DORA	Artikel 12	Adgangsstyring og tilbagekaldelse for IKT-systemer
COBIT 2019	APO07, DSS01	Personalesikkerhed samt logisk og fysisk adgangsstyring
EU GDPR	Artikel 32	Sikkerhed for personoplysninger under ansættelsesforhold

1. Formål

1.1 Denne politik fastlægger processen for onboarding af nye medarbejdere og kontrahenter samt sikker fjernelse af adgang, når personer fratræder eller skifter rolle.

1.2 Den sikrer, at adgang tildeles efter princippet om mindst privilegium, at alle aktiver registreres, og at kritiske handlinger såsom deaktivering af systemadgang og tilbagelevering af aktiver gennemføres rettidigt.

1.3 Denne politik understøtter compliance, driftsintegritet og databeskyttelse gennem strukturerede og revisionssporbare onboarding- og fratrædelsesaktiviteter.

2. Omfang

2.1 Denne politik gælder for:

2.1.1 Alle fastansatte og midlertidigt ansatte medarbejdere

2.1.2 Kontrahenter, konsulenter og praktikanter

2.1.3 Eksterne tjenesteudbydere med systemadgang eller fysisk adgang

2.2 Den omfatter:

2.2.1 Onboarding: Oprettelse af brugerkonti, tildeling af adgang og udlevering af udstyr

2.2.2 Fratrædelsesproces: Fjernelse af adgang, tilbagelevering af virksomhedens aktiver og sikker lukning af digitale identiteter

2.2.3 Interne rolleændringer, der kræver ændring af adgang eller omfordeling af aktiver

2.3 Politikken gælder for alle enheder, platforme og lokationer, der anvendes til officielle forretningsformål.

3. Målsætninger

3.1 Sikre, at nye medarbejdere får adgang og ressourcer på baggrund af verificerede roller og ansvarsområder.

3.2 Bekræfte, at fratrædende brugere er fuldstændigt fjernet fra systemer og faciliteter senest ved udgangen af deres sidste arbejdsdag.

3.3 Forebygge forældreløse konti og aktiver, der ikke er tilbageleveret, da disse udgør en sikkerhedsrisiko.

3.4 Opretholde dokumenterede registreringer af onboarding-, rolleændrings- og fratrædelsesaktiviteter.

3.5 Fremme ansvarlighed gennem tjeklister og tværgående koordinering på tværs af roller.

4. Roller og ansvar

4.1 Direktør

4.1.1 Godkender adgang for højt privilegerede brugere og fører tilsyn med onboarding- og fratrædelsesprogrammet.

4.1.2 Sikrer, at undtagelser er begrundede, og at korrigerende handlinger iværksættes, når processer ikke følges.

4.2 Office Manager / HR

4.2.1 Iværksætter onboarding for nyansatte og underretter IT om fratrædelser.

4.2.2 Sikrer færdiggørelse af juridiske dokumenter, herunder fortrolighedserklæringer (NDA), samt bekræftelse af sikkerhedspolitikker.

4.2.3 Vedligeholder onboarding- og offboardingtjeklister og overvåger efterlevelse af politikken.

[... Afsnit 4.3–8 er ikke inkluderet i denne forhåndsvisning. Køb det fulde dokument for at få adgang til det komplette indhold. ...]

9. Krav til gennemgang og opdatering

9.1 Årlig gennemgang

9.1.1 Denne politik skal gennemgås mindst én gang årligt af direktøren og de HR- og IT-ansvarlige.

9.2 Udløsere for tidligere gennemgang

9.2.1 Opdateringer skal foretages, hvis:

9.2.1.1 Nye HR- eller IT-systemer indføres

9.2.1.2 Der sker ændring af ekstern IT-leverandør eller administreret HR-tjeneste

9.2.1.3 Sikkerhedsaudits afdækker procesmangler

9.2.1.4 Regulatoriske forpligtelser ændres, f.eks. ved opdateringer til GDPR

9.2.1.5 Der opstår et kritisk svigt i fratrædelsesprocessen eller en sikkerhedshændelse

9.3 Versionsstyring og godkendelse

9.3.1 Hver version af denne politik skal indeholde:

9.3.1.1 Versionsnummer og dato

9.3.1.2 Resumé af ændringer

9.3.1.3 Godkendelse fra direktøren

9.3.1.4 Arkiverede tidligere versioner, som opbevares i mindst tre år

9.4 Kommunikation og bekræftelse

9.4.1 Alle medarbejdere med ansvar for onboarding eller fratrædelse skal underrettes om opdateringer af politikken. Årlig bevidstgørelse eller genopfriskningstræning er obligatorisk.

10. Relaterede politikker og sammenhænge

10.1 Denne politik understøtter og understøttes af følgende:

10.1.1 P2S – Politik for styringsroller og ansvarsområder: Sikrer ansvarlighed i adgangs- og onboardingprocesser

10.1.2 P4S – Politik for adgangskontrol: Etablerer teknisk håndhævelse af rollebaseret tildeling og deaktivering

10.1.3 P6S – Politik for risikostyring: Vurderer risici som følge af svigt i onboarding- og fratrædelseskontroller

10.1.4 P8S – Politik for informationssikkerhedsbevidsthed og -uddannelse: Fastlægger krav til introduktion af medarbejdere ved onboarding

10.1.5 P30S – Politik for hændelseshåndtering: Behandler manglende afprovisionering af adgang eller tyveri af aktiver som sikkerhedshændelser

11. Referencestandarder og -rammeværker

11.1 ISO/IEC 27001

11.1.1 Klausul 6.2 – Fastsætter krav til personalesikkerhed

11.1.2 Klausul 7.2 – Fastsætter krav om bevidstgørelsestræning for nye medarbejdere

11.2 ISO/IEC 27002

11.2.1 Kontroller 6.2 og 6.5 – Beskriver sikkerhedspraksis for onboarding og fratrædelse af medarbejdere

11.3 NIST SP 800-53 Rev. 5

11.3.1 PS-4 – Procedurer for fratrædelse af personale, herunder deaktivering af adgang

11.3.2 AC-2 – Sikrer livscyklusstyring af brugeradgang

11.3.3 PL-4 – Kræver planlægning af personaleovergange

11.4 EU GDPR

11.4.1 Artikel 32 – Sikrer passende sikkerhed under og efter ansættelse, særligt for adgang til personoplysninger

11.5 EU NIS2-direktivet

11.5.1 Artikel 21(2)(h) – Kræver personalesikkerhed og kontroller for livscyklusstyring af adgang

11.6 EU DORA

11.6.1 Artikel 12 – Kræver, at regulerede finansielle enheder styrer medarbejderes adgang til IKT-systemer, herunder procedurer for tilbagekaldelse

11.7 COBIT 2019

11.7.1 APO07 – Manage Human Resources: Fastsætter sikkerhedskrav for medarbejderlivscyklussen

11.7.2 DSS01 – Manage Operations: Omfatter styring af logisk og fysisk adgang ved overgange i ansættelsesforhold