					Indsæt navnet på den registrerede juridiske enhed her							
Dokumentnummer: P07					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 regler

Standard/regulering	Klausul/artikel	Kommentar
ISO/IEC 27001:2022	Klausul 7.2, klausul 6	Personalekompetence, sikker integration og håndhævelse af ansvar ved fratrædelse og ændringer.
ISO/IEC 27002:2022	Kontroller 6.2, 6.5, 5	Onboarding, adgang og kontroller for personalets livscyklus.
NIST SP 800-53 Rev.5	PS-4, PS-5, AC-2, AC-6, IA-4, IA-5, CM-5, AU-2, AU-6	Personaleovergange og fratrædelser, princippet om mindst privilegium, revisionslogning og adgangsstyring under og efter personaleændringer.
EU GDPR	Artikel 5(1)(f), 25, 32; betragtning 39	Begrænsning af adgang, fortrolighed, beskyttelse og passende kontroller for personoplysninger.
EU NIS2	Artikel 21(2)(b, c, d)	Personale- og driftsmæssige sikkerhedsforanstaltninger, håndtering af insidertrusler og livscyklusprocesser.
EU DORA	Artikel 5, 8, 9	Styring, intern IKT-kontrol, IKT-risiko og hændelseshåndtering under personaleovergange.
COBIT 2019	APO07, BAI08, DSS05, MEA03	Human resources, vidensstyring, sikkerhed og efterlevelse ved onboarding og fratrædelse.

1. Formål

1.1 Denne politik fastsætter standardiserede procedurer for håndtering af onboarding, interne omplaceringer og fratrædelser på tværs af alle brugertyper.

1.2 Den sikrer rettidig og sikker provisionering og afprovisionering af brugeradgang til fysisk og logisk adgang, samtidig med at fortrolighed, ansvarlighed og tilbagelevering af aktiver håndhæves.

1.3 Denne politik reducerer risici forbundet med uautoriseret adgang, datalækage og ikke-returnerede aktiver ved at indarbejde kontroller for onboarding og fratrædelse i HR-processer, IT-processer og sikkerhedsprocesser.

1.4 Den understøtter ISO/IEC 27001:2022 Annex A-kontrol 6.5 ved at sikre, at personalesikkerhedsforpligtelser håndhæves under og efter ansættelse eller engagement.

2. Omfang

2.1 Denne politik gælder for alle medarbejdere, kontraktansatte, konsulenter, leverandører og andre tredjeparter, der gives adgang til organisationens systemer, netværk, faciliteter eller data.

2.2 Den regulerer den fulde livscyklus for:

2.2.1 onboarding (ansættelse, kontraktindgåelse eller midlertidigt engagement)

2.2.2 interne omplaceringer eller rolleændringer

2.2.3 fratrædelse (opsigelse, pensionering, afskedigelse, kontraktudløb)

2.3 Politikken omfatter:

2.3.1 logisk adgang (systemer, applikationer, cloud, VPN)

2.3.2 fysisk adgang (adgangskort, nøgler, bygningsadgangssystemer)

2.3.3 tildelte aktiver (bærbare computere, telefoner, tokens, legitimationsoplysninger)

2.3.4 bekræftelse af politikker og fortrolighedsforpligtelser

2.4 Alle afdelinger (HR, IT, Facilities, Security og ledelsen) er ansvarlige for at udføre deres rolle i arbejdsgange for onboarding og offboarding.

3. Mål

3.1 At sikre, at alt personale kun tildeles adgang efter opfyldelse af sikkerhedsmæssige, uddannelsesmæssige og kontraktlige forudsætninger.

3.2 At tilbagekalde adgangsrettigheder og tilbagelevere organisationens aktiver straks ved rolleændring eller fratrædelse.

3.3 At opretholde fortrolighed, integritet og tilgængelighed (CIA) for organisationens aktiver under personaleovergange.

3.4 At understøtte revisionsspor og juridisk robusthed gennem fuldstændige optegnelser over onboarding- og fratrædelseshændelser.

3.5 At reducere eksponering for insidertrusler ved at validere og dokumentere alle adgangshændelser relateret til personale.

3.6 At tilpasse organisationens personalelivscyklus til risikobaserede sikkerhedspraksisser og regulatoriske krav.

4. Roller og ansvar

4.1 Direktionen

4.1.1 Godkender denne politik og allokerer beføjelser og ressourcer til processer for onboarding, fratrædelse og adgangsstyring.

4.1.2 Sikrer, at personaleovergange ikke udsætter organisationen for unødig sikkerheds- eller juridisk risiko.

4.2 Human Resources (HR)

4.2.1 Iværksætter arbejdsgange for onboarding og fratrædelse for medarbejdere og underretter relevante afdelinger om ændringer.

4.2.2 Sikrer, at baggrundstjek, kontrakter, fortrolighedsaftaler og bekræftelse af politik er gennemført, før adgang tildeles.

4.2.3 Informerer IT og Facilities om medarbejderes fratrædelser i overensstemmelse med den fastsatte SLA for underretning.

4.2.4 Koordinerer med Juridisk og Compliance for at håndhæve forpligtelser efter ansættelsesophør (f.eks. fortrolighedsklausuler).

[... 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 Frekvens for gennemgang af politikken

9.1.1 Denne politik skal gennemgås:

9.1.1.1 årligt, eller

9.1.1.2 efter enhver væsentlig hændelse, der involverer misbrug af adgang, tab af aktiver eller procedurefejl

9.1.1.3 ved implementering af større ændringer i HR- eller IAM-platforme

9.1.1.4 ved regulatoriske eller juridiske opdateringer, der påvirker personoplysninger eller forpligtelser

9.2 Proces og ejerskab for gennemgang

9.2.1 ISMS Manager og HR-direktøren skal koordinere gennemgangen med input fra IT-sikkerhed, Juridisk og Compliance.

9.2.2 Alle ændringer skal godkendes af Direktionen og Informationssikkerhedsstyregruppen (ISSC).

9.2.3 Reviderede versioner skal redistribueres til berørte afdelinger og medarbejdere med henblik på fornyet bekræftelse.

9.3 Dokumentstyring og opbevaring

9.3.1 Denne politik skal omfatte:

9.3.2 versionsstyring, ændringshistorik og ikrafttrædelsesdato

9.3.3 ansvarlig ejer og reviewer(e)

9.3.4 politikklassifikation og godkendelsesregistrering

9.3.5 Forældede versioner skal arkiveres i mindst 3 år i overensstemmelse med politikken for dokumentstyring.

10. Relaterede politikker og sammenhænge

10.1.1 Denne politik er direkte integreret med:

10.1.2 P1 – Politik for informationssikkerhed: Fastlægger organisationens sikkerhedsmål, herunder styring af personaleadgang.

10.1.3 P4 – Politik for adgangskontrol: Angiver operationelle krav til tildeling og tilbagekaldelse af systemadgang og fysisk adgang baseret på udløsere fra onboarding og fratrædelse.

10.1.4 P3 – Politik for acceptabel brug: Kræver bekræftelse ved onboarding og understøtter håndhævelse efter fratrædelse.

10.1.5 P6 – Politik for risikostyring: Sikrer, at risici ved brugeradgang og overgange evalueres og afbødes i overensstemmelse med ISMS-principper.

10.1.6 P11 – Politik for håndtering af brugerkonti og privilegier: Regulerer de tekniske kontroller for provisionering og afprovisionering af brugeradgang til understøttelse af denne politik.

10.2 Disse politikker udgør et integreret kontrolsystem til sikker og ansvarlig håndtering af hændelser i personalets livscyklus.

11. Referencestandarder og rammeværk

11.1 Denne politik er tilpasset internationalt anerkendte rammeværk for sikkerhed, databeskyttelse og IT-styring for at sikre, at processer for onboarding og fratrædelse er sikre, sporbare og i overensstemmelse med juridiske og organisatoriske krav.

11.2 ISO/IEC 27001:

11.2.1 Klausul 7.2 – Kompetence og klausul 6.2 – Mål for informationssikkerhed: Denne politik understøtter etablering af personalekompetence og sikker integration af personer i roller, hvor de påvirker ISMS-mål.

11.2.2 Annex A-kontrol 6.5 – Ansvar efter fratrædelse eller ændring af ansættelse: Denne politik håndhæver fuldt ud kontroller vedrørende resterende adgangsrettigheder, dataforvaltning og kontraktlige forpligtelser ved fratrædelse.

11.2.3 Annex A-kontrol 5.9 – Screening og 6.2 – Ansættelsesvilkår: Onboarding-procedurer omfatter baggrundsverifikation og mekanismer til bekræftelse af politik i overensstemmelse med disse klausuler.

11.3 NIST SP 800-53 Rev.5:

11.3.1 PS-4 (Personnel Termination) og PS-5 (Personnel Transfer): Denne politik håndhæver struktureret fjernelse eller ændring af adgangsrettigheder, fysiske adgangskort og aktiver.

11.3.2 AC-2 (Account Management) og AC-6 (Least Privilege): Bestemmelserne sikrer, at adgang er tilpasset rollen og straks tilbagekaldes, når den ikke længere er nødvendig.

11.3.3 IA-4 (Identifier Management) og IA-5 (Authenticator Management): Understøtter sikker håndtering af legitimationsoplysninger under og efter personaleændringer.

11.3.4 CM-5 (Access Restrictions for Change): Forhindrer uautoriserede ændringer efter fratrædelse ved at tilbagekalde forhøjede adgangsrettigheder.

11.3.5 AU-2 og AU-6: Logning og sporbarhed af adgangshændelser styrkes gennem integration med IAM og revisionsspor.

11.4 EU GDPR (2016/679):

11.4.1 Artikel 5(1)(f): Beskytter personoplysninger mod uautoriseret adgang, hvilket her håndhæves ved at tilbagekalde brugeradgang under offboarding.

11.4.2 Artikel 32: Kræver passende tekniske og organisatoriske kontroller for at sikre personoplysninger gennem hele ansættelseslivscyklussen.

11.4.3 Artikel 25 – Databeskyttelse gennem design: Sikrer, at onboarding og fratrædelse integrerer dataminimering, opbevaring og lovlige kontroller for adgang.

11.4.4 Betragtning 39: Fremhæver adgangsbegrænsning og fortrolighed, som understøttes af denne politiks struktur.

11.5 EU NIS2-direktivet (2022/2555):

11.5.1 Artikel 21(2)(b, c, d): Kræver personale- og driftsmæssige sikkerhedsforanstaltninger til håndtering af adgangsstyring, håndtering af insidertrusler og livscyklusprocesser, som alle afspejles i denne politik.

11.6 EU DORA (2022/2554):

11.6.1 Artikel 5 – Styring og intern kontrol: Denne politik understøtter intern IKT-styring relateret til menneskelige risici og adgangsstyring.

11.6.2 Artikel 8 – Styring af IKT-risiko: Anvender kontroller på personaleovergange, der kan udsætte kritiske aktiver eller regulerede miljøer for risiko.

11.6.3 Artikel 9 – Klassifikation og styring af hændelser: Sikrer, at brud relateret til fratrædelse er indberetningspligtige og afbødes gennem korrekt afprovisionering af adgang og håndtering af aktiver.

11.7 COBIT 2019:

11.7.1 APO07 – Managed Human Resources: Definerer roller, ansvar og livscyklusaktiviteter for onboarding og fratrædelse i overensstemmelse med styringsmål.

11.7.2 BAI08 – Knowledge Management: Understøtter dokumentation af procedurer, fastholdelse af viden og overdragelse af kontroller ved ansættelsens ophør.

11.7.3 DSS05 – Managed Security Services: Håndhæver deaktivering af brugere, aktivkontrol og ansvarlighed under rolleovergange.

11.7.4 MEA03 – Monitor, Evaluate, and Assess Compliance: Sikrer, at kontroller for onboarding og offboarding vurderes under interne og eksterne revisioner.