					Ange namnet på den registrerade juridiska personen här							
Dokumentnummer: P07S					Dokumenttitel: **Policy för introduktion och avslut**							
Version: 1.0		Ikraftträdandedatum: 01.01.2025			Dokumentägare:							
X	Policy		Standard		Rutin		Formulär		Register		Övrigt	

Revisionshistorik				
Revisionsnummer	**Revisionsdatum**	**Ändringar**	**Granskad av**	**Processägare**

Godkännanden			
Namn	**Titel**	**Datum**	**Underskrift**

Anpassad till standarder och regelverk

Standard/regelverk	Klausul/artikel	Kommentar
ISO/IEC 27001:2022	Klausuler 6.2, 7	Krav avseende personalsäkerhet och medvetenhet
ISO/IEC 27002:2022	Kontroller 6.2, 6.5	Säkerhetspraxis för introduktion och avslut
NIST SP 800-53 Rev. 5	PS-4, AC-2, PL-4	Avslut av anställning, behörigheters livscykelhantering, planering
EU:s NIS2-direktiv	Artikel 21(2)(h)	Personalsäkerhet och livscykelhantering av behörigheter
EU:s DORA-förordning	Artikel 12	Åtkomstkontroller och behörighetsindragning för IKT-system
COBIT 2019	APO07, DSS01	Personalsäkerhet, logiska och fysiska åtkomstkontroller
EU:s GDPR	Artikel 32	Säkerhet för personuppgifter under anställning

1. Syfte

1.1 Denna policy fastställer processen för introduktion av nya anställda, entreprenörer och tredjepartsleverantörer samt för säker borttagning av åtkomst när personer lämnar organisationen eller byter roll.

1.2 Den säkerställer att behörighetstilldelning sker enligt principen om minsta privilegium, att samtliga tillgångar är registrerade och att kritiska åtgärder såsom systemavaktivering och återlämning av tillgångar genomförs utan dröjsmål.

1.3 Denna policy stödjer efterlevnad, korrekt verksamhetsutövning och dataskydd genom strukturerade och verifierbara aktiviteter för introduktion och avslut.

2. Omfattning

2.1 Denna policy gäller för:

2.1.1 Alla tillsvidareanställda och visstidsanställda

2.1.2 Entreprenörer, konsulter och praktikanter

2.1.3 Externa tjänsteleverantörer med systemåtkomst eller fysiskt tillträde

2.2 Den omfattar:

2.2.1 Introduktion: skapande av användarkonton, behörighetstilldelning och utlämning av utrustning

2.2.2 Avslut: borttagning av åtkomst, återtagande av organisationens tillgångar och säker avveckling av digitala identiteter

2.2.3 Interna rolländringar som kräver omkonfigurering av behörigheter eller omfördelning av tillgångar

2.3 Gäller för alla enheter, plattformar och platser som används för organisationens verksamhet.

3. Mål

3.1 Säkerställa att ny personal får åtkomst och resurser utifrån verifierade roller och ansvarsområden.

3.2 Säkerställa att användare som lämnar organisationen är fullständigt borttagna från system och lokaler senast vid arbetsdagens slut på sin sista arbetsdag.

3.3 Förhindra herrelösa konton och ej återlämnade tillgångar, vilka utgör en säkerhetsrisk.

3.4 Upprätthålla dokumenterade uppgifter om introduktion, interna förflyttningar och avslutsåtgärder.

3.5 Främja ansvarstagande genom checklistor och tvärfunktionell samordning mellan roller.

4. Roller och ansvar

4.1 Verkställande direktör

4.1.1 Godkänner åtkomst för privilegierade användare och utövar tillsyn över processen för introduktion och avslut.

4.1.2 Säkerställer att undantag är motiverade och att korrigerande åtgärder vidtas när processer inte följs.

4.2 Kontorsansvarig / HR

4.2.1 Initierar introduktion för nyanställda och informerar IT om avgångar.

4.2.2 Säkerställer att rättsliga dokument, till exempel sekretessavtal (NDA), samt policybekräftelser är färdigställda.

4.2.3 Upprätthåller checklistor för introduktion och avslut samt följer upp efterlevnaden av policyn.

[... Avsnitt 4.3–8 ingår inte i denna förhandsvisning. Köp det fullständiga dokumentet för att få tillgång till hela innehållet. ...]

9. Krav för granskning och uppdatering

9.1 Årlig granskning

9.1.1 Denna policy ska granskas minst en gång per år av verkställande direktör samt ansvariga för HR och IT.

9.2 Utlösande faktorer för tidigare granskning

9.2.1 Uppdateringar ska ske om:

9.2.1.1 Nya HR- eller IT-system införs

9.2.1.2 Byte av extern IT-tjänsteleverantör eller hanterad HR-tjänst sker

9.2.1.3 Säkerhetsrevisioner visar på processbrister

9.2.1.4 Regulatoriska skyldigheter förändras, till exempel vid uppdateringar av GDPR

9.2.1.5 Ett kritiskt fel i avslutsprocessen eller en överträdelse inträffar

9.3 Versionshantering och godkännande

9.3.1 Varje version av denna policy ska innehålla:

9.3.1.1 Versionsnummer och datum

9.3.1.2 Sammanfattning av ändringar

9.3.1.3 Godkännande av verkställande direktör

9.3.1.4 Arkiverade tidigare versioner som bevaras i minst tre år

9.4 Kommunikation och bekräftelse

9.4.1 All personal med ansvar för introduktion eller avslut ska informeras om uppdateringar av policyn. Årliga genomgångar i säkerhetsmedvetenhet eller återkommande repetitionsutbildning är obligatoriska.

10. Relaterade policyer och kopplingar

10.1 Denna policy stödjer och stöds av följande:

10.1.1 P2S – Policy för styrningsroller och ansvar: Säkerställer ansvarstagande i processer för åtkomst och introduktion

10.1.2 P4S – Åtkomstkontrollpolicy: Fastställer teknisk tillämpning av rollbaserad behörighetstilldelning och avaktivering

10.1.3 P6S – Riskhanteringspolicy: Bedömer risker som uppstår vid kontrollbrister i introduktions- och avslutsprocesser

10.1.4 P8S – Policy för informationssäkerhetsmedvetenhet och utbildning: Säkerställer krav på personalintroduktion vid introduktion

10.1.5 P30S – Policy för incidenthantering: Hanterar underlåtenhet att genomföra avveckling av åtkomst eller stöld av tillgångar som säkerhetsincidenter

11. Referensstandarder och ramverk

11.1 ISO/IEC 27001

11.1.1 Klausul 6.2 – Fastställer krav på personalsäkerhet

11.1.2 Klausul 7.2 – Föreskriver utbildning i säkerhetsmedvetenhet för ny personal

11.2 ISO/IEC 27002

11.2.1 Kontroller 6.2 och 6.5 – Beskriver säkerhetspraxis för introduktion och avslut av anställning

11.3 NIST SP 800-53 Rev. 5

11.3.1 PS-4 – Rutiner för avslut av anställning inklusive avaktivering av åtkomst

11.3.2 AC-2 – Säkerställer livscykelhantering av behörigheter för användaråtkomst

11.3.3 PL-4 – Kräver planering för personalförändringar

11.4 EU:s GDPR

11.4.1 Artikel 32 – Säkerställer lämplig säkerhet under och efter anställning, särskilt för åtkomst till personuppgifter

11.5 EU:s NIS2-direktiv

11.5.1 Artikel 21(2)(h) – Kräver personalsäkerhet och kontroller för livscykelhantering av behörigheter

11.6 EU:s DORA-förordning

11.6.1 Artikel 12 – Kräver att reglerade finansiella entiteter styr personalens åtkomst till IKT-system, inklusive rutiner för behörighetsindragning

11.7 COBIT 2019

11.7.1 APO07 – Manage Human Resources: Fastställer säkerhetskrav för personalens livscykel

11.7.2 DSS01 – Manage Operations: Omfattar styrning av logisk och fysisk åtkomst vid förändringar i anställning