					Ange namnet på den registrerade juridiska personen här							
Dokumentnummer: P07					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 där så är tillämpligt

Standard/regelverk	Klausul/artikel	Kommentar
ISO/IEC 27001:2022	Klausul 7.2, klausul 6	Personalkompetens, säker integrering samt genomförande av ansvar vid avslut eller förändring av anställning.
ISO/IEC 27002:2022	Kontroller 6.2, 6.5, 5	Introduktion, åtkomst och kontroller för personalens livscykel.
NIST SP 800-53 Rev.5	PS-4, PS-5, AC-2, AC-6, IA-4, IA-5, CM-5, AU-2, AU-6	Personalövergångar och avslut, principen om minsta privilegium, revisionsloggning samt åtkomsthantering vid och efter personalförändringar.
EU:s GDPR	Artiklarna 5(1)(f), 25, 32; skäl 39	Begränsning av åtkomst, konfidentialitet, skydd och lämpliga kontroller för personuppgifter.
EU:s NIS2-direktiv	Artikel 21(2)(b, c, d)	Personalrelaterade och operativa säkerhetsåtgärder, hantering av insiderhot samt livscykelprocesser.
DORA-förordningen	Artiklarna 5, 8, 9	Styrning, intern kontroll av IKT, IKT-risker och incidenthantering vid personalövergångar.
COBIT 2019	APO07, BAI08, DSS05, MEA03	Personalresurser, kunskapshantering, säkerhet och regelefterlevnad vid introduktion och avslut.

1. Syfte

1.1 Denna policy fastställer standardiserade rutiner för att hantera introduktion, interna förflyttningar och avslut för samtliga användartyper.

1.2 Den säkerställer snabb och säker tilldelning av åtkomst samt avveckling av behörigheter för fysiskt tillträde och logisk åtkomst, samtidigt som konfidentialitet, ansvarsskyldighet och återtagande av tillgångar upprätthålls.

1.3 Denna policy minskar risker kopplade till obehörig åtkomst, dataläckage och ej återlämnade tillgångar genom att integrera kontroller för introduktion och avslut i HR-processer, IT-processer och säkerhetsprocesser.

1.4 Den stöder ISO/IEC 27001:2022 bilaga A kontroll 6.5 genom att säkerställa att personalsäkerhetsrelaterade skyldigheter tillämpas under och efter anställning eller uppdrag.

2. Omfattning

2.1 Denna policy gäller för alla anställda, entreprenörer, konsulter, leverantörer, tredjepartstjänsteleverantörer och andra tredje parter som beviljas åtkomst till organisationens system, nätverk, lokaler eller data.

2.2 Policyn reglerar hela livscykeln för:

2.2.1 introduktion (anställning, kontraktering eller tillfälligt uppdrag)

2.2.2 interna förflyttningar eller rolländringar

2.2.3 avslut (uppsägning, pensionering, entledigande eller kontraktets utgång)

2.3 Policyn omfattar:

2.3.1 logisk åtkomst (system, applikationer, molntjänster, VPN)

2.3.2 fysiskt tillträde (passerkort, nycklar, system för inpassering i byggnader)

2.3.3 tilldelade tillgångar (bärbara datorer, telefoner, tokens, autentiseringsuppgifter)

2.3.4 bekräftelse av policyer och sekretessförpliktelser

2.4 Alla avdelningar (HR, IT, fastighet, säkerhet och ledning) ansvarar för att utföra sin del i arbetsflöden för introduktion och avslut.

3. Mål

3.1 Att säkerställa att all personal endast beviljas åtkomst efter att säkerhetsmässiga, utbildningsrelaterade och avtalsmässiga förutsättningar har uppfyllts.

3.2 Att återkalla åtkomsträttigheter och återta organisationens tillgångar omedelbart vid rolländringar eller avslut.

3.3 Att bevara konfidentialitet, riktighet och tillgänglighet för organisationens tillgångar vid personalövergångar.

3.4 Att stödja revisionsbarhet och rättslig hållbarhet genom fullständig dokumentation av händelser avseende introduktion och avslut.

3.5 Att minska exponeringen för insiderhot genom att validera och dokumentera alla personalrelaterade åtkomsthändelser.

3.6 Att anpassa organisationens personallivscykel till riskbaserad säkerhetspraxis och regulatoriska krav.

4. Roller och ansvar

4.1 Verkställande ledning

4.1.1 Godkänner denna policy och tilldelar befogenheter och resurser för processer för introduktion, avslut och åtkomstkontroll.

4.1.2 Säkerställer att personalövergångar inte utsätter organisationen för otillbörlig säkerhetsrisk eller rättslig risk.

4.2 HR

4.2.1 Initierar arbetsflöden för introduktion och avslut för anställda och underrättar relevanta avdelningar om förändringar.

4.2.2 Säkerställer att bakgrundskontroller, avtal, sekretessavtal (NDA) och policybekräftelser är slutförda innan åtkomst beviljas.

4.2.3 Informerar IT och fastighets- och tillgångsförvaltning om personalavgångar i enlighet med SLA för aviseringar.

4.2.4 Samordnar med juridisk funktion för att säkerställa efterlevnad av förpliktelser efter anställningens upphörande (t.ex. sekretessklausuler).

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

9. Krav på granskning och uppdatering

9.1 Frekvens för policygranskning

9.1.1 Denna policy ska granskas:

9.1.1.1 årligen, eller

9.1.1.2 efter varje väsentlig incident som rör missbruk av åtkomst, förlust av tillgångar eller processfel

9.1.1.3 vid genomförande av större förändringar i HR-system eller IAM-plattform

9.1.1.4 vid regulatoriska eller rättsliga uppdateringar som påverkar personaluppgifter eller skyldigheter

9.2 Granskningsprocess och ägarskap

9.2.1 ISMS-ansvarig och HR-direktör ska samordna granskningen med bidrag från IT-säkerhet, juridisk funktion och regelefterlevnad.

9.2.2 Samtliga ändringar ska godkännas av verkställande ledning och styrgruppen för informationssäkerhet (ISSC).

9.2.3 Reviderade versioner ska distribueras på nytt till berörda avdelningar och berörd personal för förnyad bekräftelse.

9.3 Dokumentstyrning och bevarande

9.3.1 Denna policy ska innehålla:

9.3.2 versionshantering, ändringshistorik och ikraftträdandedatum

9.3.3 ansvarig ägare och granskare

9.3.4 policyklassificering och godkännandepost

9.3.5 Utgångna versioner ska arkiveras i minst 3 år i enlighet med policyn för dokumenthantering.

10. Relaterade policyer och kopplingar

10.1.1 Denna policy är direkt integrerad med:

10.1.2 P1 – Informationssäkerhetspolicy: Fastställer organisationens säkerhetsmål, inklusive styrning av personalrelaterad åtkomst.

10.1.3 P4 – Åtkomstkontrollpolicy: Anger operativa krav för tilldelning och återkallelse av systemåtkomst och fysiskt tillträde utifrån utlösande händelser vid introduktion och avslut.

10.1.4 P3 – Policy för godtagbar användning: Kräver bekräftelse vid introduktion och stödjer tillämpning efter avslut.

10.1.5 P6 – Riskhanteringspolicy: Säkerställer att risker relaterade till användaråtkomst och personalövergångar utvärderas och reduceras i linje med ISMS-principer.

10.1.6 P11 – Policy för hantering av användarkonton och privilegier: Reglerar de tekniska kontrollerna för tilldelning av åtkomst och behörighetsavveckling till stöd för denna policy.

10.2 Dessa policyer utgör tillsammans ett integrerat kontrollsystem för att hantera händelser i personalens livscykel på ett säkert sätt och med tydlig ansvarsskyldighet.

11. Referensstandarder och ramverk

11.1 Denna policy är anpassad till internationellt erkända ramverk för säkerhet, integritet och IT-styrning för att säkerställa att processer för introduktion och avslut är säkra, spårbara och förenliga med rättsliga och organisatoriska krav.

11.2 ISO/IEC 27001:

11.2.1 Klausul 7.2 – Kompetens och klausul 6.2 – Informationssäkerhetsmål: Denna policy stödjer etablering av personalkompetens och säker integrering av individer i roller där de påverkar ISMS-mål.

11.2.2 Bilaga A kontroll 6.5 – Ansvar efter avslut eller förändring av anställning: Denna policy implementerar fullt ut kontroller för kvarstående åtkomsträttigheter, datahantering och avtalsmässiga skyldigheter vid avgång.

11.2.3 Bilaga A kontroll 5.9 – Screening och 6.2 – Anställningsvillkor: Introduktionsrutinerna omfattar bakgrundsverifiering och mekanismer för policybekräftelse i enlighet med dessa krav.

11.3 NIST SP 800-53 Rev.5:

11.3.1 PS-4 (avslut av personal) och PS-5 (intern personalförflyttning): Denna policy säkerställer strukturerad borttagning eller ändring av åtkomsträttigheter, fysiska passerkort och tillgångar.

11.3.2 AC-2 (kontohantering) och AC-6 (principen om minsta privilegium): Bestämmelserna säkerställer att åtkomst är rollanpassad och omedelbart återkallas när den inte längre behövs.

11.3.3 IA-4 (hantering av identifierare) och IA-5 (hantering av autentiseringsuppgifter): Stödjer säker hantering av autentiseringsuppgifter under och efter personalförändringar.

11.3.4 CM-5 (åtkomstbegränsningar för ändringar): Förhindrar otillåtna ändringar efter avslut genom att förhöjda åtkomsträttigheter återkallas.

11.3.5 AU-2 och AU-6: Loggning och spårbarhet för åtkomsthändelser förstärks genom integration mellan IAM och revisionsspår.

11.4 EU:s GDPR (2016/679):

11.4.1 Artikel 5(1)(f): Skyddar personuppgifter mot obehörig åtkomst, vilket här upprätthålls genom att användaråtkomst återkallas vid avslut.

11.4.2 Artikel 32: Kräver lämpliga tekniska och organisatoriska kontroller för att skydda personuppgifter under hela anställningslivscykeln.

11.4.3 Artikel 25 – Dataskydd genom inbyggt dataskydd och dataskydd som standard: Säkerställer att introduktion och avslut integrerar uppgiftsminimering, lagring och laglig åtkomstkontroll.

11.4.4 Skäl 39: Betonar begränsning av åtkomst och konfidentialitet, vilket stöds av denna policys struktur.

11.5 EU:s NIS2-direktiv (2022/2555):

11.5.1 Artikel 21(2)(b, c, d): Kräver personalrelaterade och operativa säkerhetsåtgärder för att hantera åtkomstkontroll, insiderhot och livscykelprocesser, vilket återspeglas i denna policy.

11.6 EU:s DORA-förordning (2022/2554):

11.6.1 Artikel 5 – Styrning och intern kontroll: Denna policy stöder intern IKT-styrning avseende mänskliga risker och åtkomsthantering.

11.6.2 Artikel 8 – IKT-riskhantering: Kräver tillämpning av kontroller på personalövergångar som kan exponera kritiska tillgångar eller reglerade miljöer.

11.6.3 Artikel 9 – Klassificering och hantering av incidenter: Säkerställer att överträdelser relaterade till avslut är rapporteringsbara och reduceras genom korrekt behörighetsavveckling och hantering av tillgångar.

11.7 COBIT 2019:

11.7.1 APO07 – Managed Human Resources: Definierar roller, ansvar och livscykelåtgärder för introduktion och avslut i linje med styrningsmål.

11.7.2 BAI08 – Knowledge Management: Förstärker dokumentation av rutiner, kunskapsbevarande och överföring av kontroller vid anställningens slut.

11.7.3 DSS05 – Managed Security Services: Säkerställer användardeaktivering, tillgångskontroll och ansvarsskyldighet vid rollövergångar.

11.7.4 MEA03 – Monitor, Evaluate, and Assess Compliance: Säkerställer att kontroller för introduktion och avslut bedöms vid intern och extern revision.