					Ange namnet på den registrerade juridiska personen här							
Dokumentnummer: P11S					Dokumenttitel: **Policy för hantering av användarkonton och privilegier**							
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**

I linje med standarder och regleringar

Standard/reglering	Klausul/artikel	Kommentar
ISO/IEC 27001:2022	Klausul 5.3, 8	Roller, ansvar samt operativ planering och styrning för hantering av användaråtkomst
ISO/IEC 27002:2022	Kontroll 8	Kontroller för tilldelning, granskning och borttagning av förhöjda privilegier
NIST SP 800-53 Rev.5	AC-2, AC-5, AC-6	Kontohantering, övervakning, principen om minsta privilegium samt funktionsseparering
EU:s NIS2-direktiv	Artikel 21(2)(d)	Hantering av användaråtkomst för väsentliga och viktiga verksamhetsutövare
EU:s DORA-förordning	Artikel 9(2)(b)	Kontroll av privilegierad åtkomst i finansiella entiteter
COBIT 2019	DSS05.03, DSS05.04	Tilldelning av åtkomst, avveckling av behörigheter och periodisk granskning av användaråtkomst
EU:s GDPR	Artikel 32	Lämpliga åtkomstkontroller för skydd av personuppgifter

1. Syfte

1.1 Denna policy fastställer regler för hantering av användarkonton och åtkomsträttigheter på ett säkert, konsekvent och spårbart sätt. Den säkerställer att endast behöriga personer har åtkomst till system och data samt att åtkomsten är anpassad till deras roller och ansvar.

1.2 Effektiv hantering av konton och privilegier är avgörande för att förhindra obehörig åtkomst, minska insiderhot och säkerställa efterlevnad av ISO/IEC 27001, GDPR och andra regulatoriska krav.

1.3 Denna policy gör det möjligt för organisationen att tilldela ägarskap och ansvar för användning av konton, övervaka och granska privilegiehöjningar samt på ett säkert sätt inaktivera eller återkalla åtkomst när den inte längre behövs.

1.4 Den skyddar även verksamheten mot operativa fel eller missbruk som orsakas av alltför omfattande eller otillräckligt övervakad åtkomst och bidrar till att minska risken för oavsiktligt dataläckage, missbruk av privilegier eller bristande regelefterlevnad.

2. Omfattning

2.1 Denna policy gäller för:

2.1.1 alla anställda, praktikanter, konsulter och tredjepartsanvändare med åtkomst till organisationens IT-system

2.1.2 alla system, enheter, tjänster och plattformar som hanteras av eller för organisationens räkning, inklusive molnplattformar, lokal IT-infrastruktur och verktyg från tredje part

2.2 Den omfattar alla typer av användarkonton, inklusive:

2.2.1 personliga användarkonton knutna till namngiven användare (t.ex. e-postkonton, systeminloggningar)

2.2.2 administratörskonton och systemkonton

2.2.3 tillfälliga inloggningsuppgifter, gästkonton eller tredjepartsåtkomst

2.2.4 tjänstekonton som används av applikationer eller automatiseringssystem

2.3 Policyn gäller under hela kontots livscykel – från skapande och godkännande till ändring, övervakning och avaktivering. Detta omfattar initial tilldelning av åtkomst vid introduktion, åtkomstgranskning vid rolländringar samt borttagning av behörigheter vid avslut.

3. Mål

3.1 Tilldela unika och spårbara användaridentiteter till alla systemanvändare för att säkerställa ansvarsskyldighet och eliminera beroendet av delade autentiseringsuppgifter.

3.2 Tillämpa principen om minsta privilegium så att användare endast beviljas den lägsta åtkomstnivå som krävs för att utföra sina arbetsuppgifter.

3.3 Förhindra obehörig åtkomst till känsliga system eller data genom tydligt dokumenterade processer för godkännande och granskning.

3.4 Säkerställa att användarkonton inaktiveras utan dröjsmål när de inte längre behövs, till exempel vid avslutad anställning, kontraktsslut eller rolländringar.

3.5 Upprätthålla en säker miljö med revisionsberedskap genom att dokumentera alla kontoändringar, godkännanden och periodiska granskningar.

3.6 Säkerställa att privilegiehöjning är strikt styrd, godkänns oberoende och loggas, samt att förhöjd åtkomst återkallas utan dröjsmål när den inte längre behövs.

4. Roller och ansvar

4.1 Verkställande direktör (GM)

4.1.1 Har det övergripande ansvaret för att denna policy tillämpas.

4.1.2 Säkerställer att praxis för kontohantering överensstämmer med kraven för certifiering enligt ISO/IEC 27001 och relevanta rättsliga skyldigheter (t.ex. GDPR).

4.1.3 Ska omedelbart informeras om obehörig åtkomst, säkerhetsincidenter eller policyöverträdelser som rör användarkonton.

4.1.4 Utövar tillsyn över policygranskningar, revisioner och åtgärder vid överträdelser.

4.2 IT-chef eller extern IT-tjänsteleverantör

4.2.1 Ansvarar för det tekniska genomförandet av konto- och privilegiekontroller i de system som organisationen använder.

4.2.2 Får endast utföra tilldelning av åtkomst, ändringar och avaktivering av användarkonton på grundval av dokumenterade godkännanden.

4.2.3 Ska tillämpa krav på lösenordskomplexitet, skärmlås vid inaktivitet, flerfaktorsautentisering (MFA) där detta är tillgängligt samt systemloggning.

4.2.4 Ska upprätthålla säkra register över alla åtkomstgodkännanden, kontoägarskap, privilegiehöjningar och borttagning av behörigheter.

4.2.5 Ska övervaka förekomsten av obehöriga eller herrelösa konton och rapportera avvikelser till GM.

[... 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 Denna policy ska granskas minst årligen av GM och IT-chefen för att säkerställa efterlevnad av:

9.1.1 gällande kontroller och vägledning enligt ISO/IEC 27001:2022

9.1.2 regulatoriska uppdateringar (t.ex. GDPR, DORA, NIS2)

9.1.3 förändringar i system, tjänster eller verksamhetsstruktur

9.2 Granskning ska även genomföras efter:

9.2.1 betydande säkerhetsincidenter eller revisionsiakttagelser

9.2.2 större förändringar i IT-system eller kontoarkitektur

9.2.3 införande av nya plattformar som kräver integration med åtkomstkontroll

9.3 Alla ändringar ska godkännas av GM och kommuniceras tydligt till berörd personal.

10. Relaterade policyer och kopplingar

10.1 P2S – Policy för styrningsroller och ansvar: Fastställer ansvarsskyldighet och beslutsbefogenheter för åtkomstgodkännanden och tillsyn.

10.2 P4S – Policy för åtkomstkontroll: Styr tillämpningen av åtkomstkontroll i hela systemmiljön samt autentiseringsmetoder.

10.3 P7S – Policy för introduktion och avslut: Säkerställer att skapande och borttagning av konton ingår i HR-hanterade personalförändringar.

10.4 P8S – Policy för informationssäkerhetsmedvetenhet och utbildning: Utbildar användare i säker kontohantering och förväntad användning.

10.5 P30S – Policy för incidenthantering: Definierar åtgärder som ska vidtas om missbruk av konto leder till en säkerhetsincident eller obehörigt röjande.

11. Referensstandarder och ramverk

11.1 ISO/IEC 27001

11.1.1 Klausul 5.3: Kräver att roller och ansvar för informationssäkerhet tydligt tilldelas och tillämpas.

11.1.2 Klausul 8.1: Operativ planering och styrning ska omfatta hantering av användaråtkomst.

11.2 ISO/IEC 27002

11.2.1 Kontroll 8.2: Anger tekniska och administrativa kontroller för tilldelning, granskning och borttagning av förhöjda privilegier.

11.3 NIST SP 800-53 Rev.5

11.3.1 AC-2: Kräver kontohantering, övervakning och borttagning av behörigheter utifrån definierade roller och processer.

11.3.2 AC-5: Avser funktionsseparering för att förhindra intressekonflikter eller missbruk av privilegier.

11.3.3 AC-6: Kräver att principen om minsta privilegium tillämpas på alla åtkomsträttigheter.

11.4 EU:s GDPR

11.4.1 Artikel 32: Kräver lämpliga åtkomstkontroller för att skydda personuppgifter mot obehörig åtkomst eller ändring.

11.5 EU:s NIS2-direktiv

11.5.1 Artikel 21(2)(d): Kräver hantering av användaråtkomst som en del av centrala säkerhetskontroller för väsentliga och viktiga verksamhetsutövare.

11.6 EU:s DORA-förordning

11.6.1 Artikel 9(2)(b): Kräver att finansiella entiteter inför åtkomstkontroller som begränsar och övervakar privilegierade rättigheter.

11.7 COBIT 2019

11.7.1 DSS05.03: Anger tilldelning av åtkomst och avveckling av behörigheter som en del av IT-styrning.

11.7.2 DSS05.04: Kräver löpande granskning och anpassning av användaråtkomst till organisationens roller.