					Ange namnet på den registrerade juridiska personen här							
Dokumentnummer: P11					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**

Anpassad till standarder och regelverk

Standard/reglering	Klausul/artikel	Kommentar
ISO/IEC 27001:2022	Klausul 6.1.3, klausul 8	-
ISO/IEC 27002:2022	Kontroller 5.15-5.18	-
NIST SP 800-53 Rev.5	AC-1, AC-2, AC-5, AC-6, IA-2-IA-5, AU-2, AU-12	-
EU:s GDPR	Artiklarna 5.1(f), 32; skäl 39	-
EU:s NIS2-direktiv	Artiklarna 21.2(a, d), 21.3	-
EU:s DORA-förordning	Artiklarna 5, 9	-
COBIT 2019	DSS01, DSS05, APO13	-

1. Syfte

1 Denna policy fastställer obligatoriska kontroller för hantering av användarkonton och privilegier i alla informationssystem och tjänster. Den säkerställer att åtkomst till organisationens resurser beviljas utifrån verifierad identitet, behov enligt roll samt principen om minsta privilegium och funktionsåtskillnad.

1.1 Den stödjer organisationens åtagande inom informationssäkerhet genom att införa strukturerade, granskningsbara processer för åtkomsttilldelning, tilldelning av privilegier, övervakning av användning och avveckling av behörigheter.

1.2 Denna policy är avgörande för att minska risken för obehörig åtkomst, missbruk av privilegier, insiderhot och bristande efterlevnad av tillämpliga regulatoriska ramverk.

2. Omfattning

2.1 Denna policy gäller för alla anställda, entreprenörer, tredjepartstjänsteleverantörer, konsulter och andra personer som beviljats åtkomst till organisationens IT-resurser, applikationer eller data.

2.2 Den omfattar alla system och miljöer där användarautentisering och åtkomstkontrollmekanismer tillämpas, inklusive men inte begränsat till:

2.2.1 Verksamhetsapplikationer och databaser

2.2.2 Molnplattformar och SaaS-miljöer

2.2.3 Operativsystem och administrativa konsoler

2.2.4 Verktyg för fjärråtkomst och VPN

2.2.5 System för identitets- och åtkomsthantering (IAM)

2.3 Policyn omfattar både standardkonton och privilegierade användarkonton och inkluderar kontroller för:

2.3.1 Skapande, ändring och avaktivering av konton

2.3.2 Privilegieeskalering och delegering

2.3.3 Sessionsstyrning och övervakning

2.3.4 Autentiseringsmetoder och hantering av autentiseringsuppgifter

3. Mål

3.1 Att säkerställa att alla användarkonton är unikt identifierbara, korrekt auktoriserade och endast tilldelas efter formell validering av behov.

3.2 Att tillämpa principen om minsta privilegium och förhindra onödig eller alltför omfattande åtkomst genom att upprätthålla strikta kontroller för tilldelning och användning av privilegierade konton.

3.3 Att kräva skyndsamma uppdateringar av kontostatus vid förändringar i anställning eller roll, inklusive omedelbar avaktivering vid avslut.

3.4 Att möjliggöra proaktiv upptäckt och åtgärd av inaktiva, felanvända eller obehöriga konton genom loggning, granskningar och automatisering.

3.5 Att upprätthålla överensstämmelse med ISO/IEC 27001:2022 och tillhörande standarder samt uppfylla skyldigheter enligt relevanta rättsliga och regulatoriska ramverk såsom GDPR, NIS2, DORA och COBIT 2019.

4. Roller och ansvar

4.1 Informationssäkerhetschef (CISO)

4.1.1 Är policyägare för denna policy och säkerställer dess tillämpning i hela organisationen.

4.1.2 Granskar och godkänner formella undantag eller fall av akut åtkomst.

4.1.3 Rapporterar kontorelaterade revisionsiakttagelser och eskalerar risker till verkställande ledning.

4.2 Chef för åtkomsthantering / IT-administratör

4.2.1 Underhåller och driver de tekniska kontrollerna för livscykelhantering av behörigheter för användarkonton.

4.2.2 Verkställer åtkomsttilldelning, avveckling av behörigheter och åtgärder för privilegiehantering efter godkänd begäran.

4.2.3 Upprätthåller ett auktoritativt register över alla användarkonton, deras status och privilegienivå.

4.2.4 Stödjer revisioner och regelefterlevnadsgranskningar med loggar och aktivitetsrapporter.

[... 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 Denna policy ska granskas minst årligen eller vid väsentliga förändringar av:

9.1.1 Organisationsstruktur eller verksamhetsprocesser

9.1.2 IT-system, identitetsplattformar eller åtkomstmetoder

9.1.3 Regulatoriska krav eller avtalskrav relaterade till identitets- och åtkomsthantering

9.2 Informationssäkerhetschef (CISO) ska tillsammans med chefen för åtkomsthantering ansvara för att initiera granskningsprocessen och samordna återkoppling från intressenter.

9.3 Extra granskningar kan utlösas av:

9.3.1 Säkerhetsincidenter relaterade till missbruk av konton

9.3.2 Revisionsiakttagelser som påvisar brister i livscykelhantering av behörigheter

9.3.3 Driftsättning av nya verktyg för identitetshantering eller hantering av privilegierad åtkomst

9.4 Uppdateringar av denna policy ska:

9.4.1 Versionshanteras och registreras i ISMS-dokumentbiblioteket

9.4.2 Kommuniceras till alla relevanta intressenter, inklusive avdelningschefer, IT-drift och HR

9.4.3 Stödjas av uppdaterat utbildningsmaterial och rutinbeskrivningar

9.5 Alla ändringar ska godkännas av verkställande ledning eller styrgruppen för informationssäkerhet (ISSC) och loggas för revisionsändamål.

10. Relaterade policyer och kopplingar

10.1 Denna policy är operativt kopplad till och stöds av följande relaterade policyer inom ISMS:

10.1.1 P4 Åtkomstkontrollpolicy: Fastställer övergripande principer och mekanismer för åtkomstkontroll, inklusive regelbaserade och rollbaserade kontroller.

10.1.2 P7 Policy för onboarding och offboarding: Tillhandahåller rutinmässiga steg för att initiera och avsluta användaråtkomst i linje med åtgärder från HR.

10.1.3 P8 Policy för informationssäkerhetsmedvetenhet och utbildning: Förstärker användarnas ansvar för kontosäkerhet och skydd av autentiseringsuppgifter.

10.1.4 P13 Policy för dataklassificering och märkning: Vägledande för åtkomstnivåer baserat på dataklassificering så att privilegiegränser anpassas till känslighetsnivåer.

10.1.5 P22 Policy för loggning och övervakning: Säkerställer att revisionsspår samlas in för alla kontorelaterade aktiviteter och granskas för att upptäcka avvikelser eller obehörig användning.

10.1.6 P30 Policy för incidenthantering: Reglerar eskalering, begränsning och åtgärder efter incidenter vid missbruk av privilegier eller obehörig kontoaktivitet.

10.2 Var och en av dessa policyer samverkar för att upprätthålla ett sammanhållet, riskbaserat ramverk för identitets- och åtkomsthantering i hela organisationen.

11. Referensstandarder och ramverk

11.1 Denna policy är anpassad till globalt erkända cybersäkerhetsstandarder och regulatoriska ramverk som kräver säker hantering av identitet, åtkomst och privilegier som en central del av organisationens informationssäkerhet.

11.2 ISO/IEC 27001:

11.2.1 Klausul 6.1.3 kräver att organisationer identifierar, utvärderar och behandlar informationssäkerhetsrisker, vilket gör hantering av åtkomst och privilegier till en formell, riskbaserad kontroll som är inbyggd i ISMS-planeringen.

11.2.2 Klausul 8.1 - Operativ planering och styrning: Förstärker genomförandet av tekniska och administrativa skyddsåtgärder som styr användaråtkomst och privilegierad åtkomst.

11.3 ISO/IEC 27002:2022 - kontroller 5.15 till 5.18:

11.3.1 Kontroll 5.15 - Användaråtkomsthantering: Stödjer formella processer för åtkomsttilldelning, åtkomstauktorisering och periodisk granskning av åtkomsträttigheter.

11.3.2 Kontroll 5.16 - Identitetshantering: Fastställer unik identitet, livscykelkontroller och säker tillämpning av autentisering.

11.3.3 Kontroll 5.17 säkerställer att tilldelning och användning av privilegierade åtkomsträttigheter är strikt kontrollerad, spårbar och anpassad till principen om minsta privilegium genom hela användarkontots livscykel.

11.3.4 Kontroll 5.18 - Privilegierade åtkomsträttigheter: Hanteras fullt ut genom rollbaserad tilldelning av privilegier, granskning och krav på godkännande av förhöjd åtkomst.

11.4 Dessa kontroller vägleder ett strukturerat genomförande av kontoregistrering, avregistrering, åtskillnad av privilegier och användning av autentiseringsinformation. Policyn upprätthåller styrning av identitetslivscykeln, just-in-time-åtkomst och övervakning av förhöjda sessioner för att förhindra obehörig systemanvändning.

11.5 NIST SP 800-53 Rev.5:

11.5.1 AC-1 (Access Control Policy) och AC-2 (Account Management): Mappas till policykrav för åtkomstgodkännanden, rollmappning och revision av användarkonton.

11.5.2 AC-5 (Separation of Duties) och AC-6 (Least Privilege): Uppfylls genom begränsning av privilegier, anpassning till arbetsroll och dubbelgodkännande för uppgifter med hög risk.

11.5.3 IA-2 till IA-5 (Identification and Authentication): Upprätthålls genom starka autentiseringsmekanismer, regler för autentiseringsuppgifters livscykel och krav på MFA.

11.5.4 AU-2, AU-12 (Audit Logging and Analysis): Hanteras genom sessionsloggning och övervakning av privilegierad aktivitet i känsliga miljöer.

11.6 EU:s GDPR (2016/679):

11.6.1 Artikel 32 - Säkerhet i behandlingen: Kräver åtkomstkontroller och mekanismer för identitetsverifiering för att skydda personuppgifter. Uppfylls genom krav på kontogodkännanden, granskning av privilegier och starka autentiseringsskydd.

11.6.2 Artikel 5.1(f) - Integritet och konfidentialitet: Säkerställer att personuppgifter endast är tillgängliga för behöriga användare med legitima roller, förstärkt genom tillämpning av kontohantering.

11.6.3 Skäl 39: Efterfrågar tydlig åtkomstbegränsning och ansvarsskyldighet – denna policy stödjer full spårbarhet för användaridentiteter och tilldelning av privilegier.

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

11.7.1 Artikel 21.2(a, d): Kräver att entiteter tillämpar policyer för åtkomsthantering och säker hantering av autentiseringsuppgifter och privilegierade sessioner, vilket stöds genom denna policys kontroller för åtkomsttilldelning, övervakning och undantag.

11.7.2 Artikel 21.3: Främjar åtkomstdisciplin och stark identitetssäkring i kritiska sektorer, vilket uppfylls genom användning av unika identifierare, RBAC och tidsbegränsad förhöjd åtkomst.

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

11.8.1 Artikel 5 - IKT-styrning och kontroll: Kräver formaliserade processer för hantering av IKT-användare, vilket täcks genom dokumenterad åtkomsttilldelning, avaktivering och undantagshantering.

11.8.2 Artikel 9 - IKT-riskhantering: Styr organisationer att säkra system genom åtkomstbegränsningar och övervakning, vilket hanteras genom MFA, loggning av privilegierad åtkomst och centraliserade granskningar.

11.9 COBIT 2019:

11.9.1 DSS01 - Managed Operations: Främjar tillämpning av standardiserade operativa kontroller, inklusive livscykelhantering av behörigheter för användarkonton och dokumentation av åtkomst.

11.9.2 DSS05 - Managed Security Services: Återspeglar säker administration av privilegier för användare och system och stödjer riskreducering genom principen om minsta privilegium och validering av revisionsspår.

11.9.3 APO13 - Managed Security: Kräver behörighetsstyrning för digitala tillgångar, vilket uppfylls genom formaliserad praxis för auktorisering av konton och roller med krav på periodisk granskning.