					Ange namnet på den registrerade juridiska personen här							
Dokumentnummer: P04					Dokumenttitel: **Åtkomstkontrollpolicy**							
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 regelverk där tillämpligt

Standard/regelverk	Klausul/artikel	Kommentar
ISO/IEC 27001:2022	Klausul 5.15, 5.17, 5.18	Hantering av logisk och fysisk åtkomst
ISO/IEC 27002:2022	Kontrollerna 8.2, 8.3	Rollbaserad åtkomst och identitetshantering
NIST SP 800-53 Rev. 5	AC-1 till AC-20, IA-1 till IA-8	Konto- och åtkomstkontroller, identitet och autentisering
EU:s dataskyddsförordning (GDPR)	Artiklarna 5.1 f, 32.1 b; skäl 39	Dataskydd och uppgiftsminimering
EU:s NIS2-direktiv	Artikel 21.2 c–e	Åtkomstkontroll, användarautentisering och skydd av tillgångar
EU:s DORA-förordning	Artiklarna 6, 9.2	IKT- och användaråtkomst samt förstärkta kontroller för tredje part
COBIT 2019	APO07, BAI03, DSS01, DSS05, MEA03	Introduktion, drift, övervakning och regelefterlevnad

1. Syfte

1.1 Denna policy fastställer obligatoriska principer, ansvar och kontrollkrav för hantering av åtkomst till informationssystem, applikationer, fysiska anläggningar och datatillgångar i hela organisationen.

1.2 Den säkerställer att åtkomst beviljas utifrån verksamhetsbehov, arbetsuppgift och risknivå samt tillämpar principen om minsta privilegium, need-to-know-principen och funktionsåtskillnad.

1.3 Policyn stöder genomförandet av ISO/IEC 27001:2022 klausul 5.15 och relaterade kontroller för logisk och fysisk åtkomst, användarautentisering och livscykelhantering av behörigheter.

1.4 Denna policy utgör grunden för skydd av digitala och fysiska resurser mot obehörig användning, missbruk eller kompromettering.

2. Omfattning

2.1 Denna policy gäller för alla användare, system och anläggningar inom ISMS omfattning, inklusive:

2.1.1 Anställda, konsulter, tredjepartsleverantörer och tillfälligt anställda

2.1.2 Lokal IT-infrastruktur, molnsystem och hybrida miljöer

2.1.3 Samtliga organisationens tillgångar – hårdvara, programvara, data och säkra områden

2.1.4 Logisk åtkomst (t.ex. system, nätverk, applikationer, API:er) och fysiskt tillträde (t.ex. byggnader, datacenter)

2.2 Den reglerar åtkomst under hela identitetslivscykeln och vid all resursinteraktion, från introduktion och behörighetstilldelning till rolländringar och avslut.

2.3 Policyn omfattar även privata enheter i tjänsten (BYOD) och fjärråtkomst (VPN, hantering av mobila enheter) och säkerställer att kontroller tillämpas konsekvent oavsett plats och enheternas ägarförhållande.

3. Mål

3.1 Att införa säkra, rollbaserade åtkomstkontroller som stöder operativ integritet och regelefterlevnad.

3.2 Att säkerställa att behörigheter godkänns, övervakas och återkallas i rätt tid.

3.3 Att förhindra obehörig åtkomst, eskalering av systemprivilegier och kvarstående inaktuella behörigheter.

3.4 Att stödja zero trust genom att som standard neka åtkomst om den inte uttryckligen har godkänts och motiverats.

3.5 Att ge revisorer och intressenter underlag genom evidensbaserad, automatiserad åtkomstgranskning och tillämpning av policyn.

3.6 Att integrera åtkomstkontroll i verksamhetsprocesser, HR-processer och tekniska arkitekturer.

4. Roller och ansvar

4.1 Verkställande ledning

4.1.1 Godkänner åtkomstkontrollpolicyn och säkerställer lämplig budget och bemanning för dess genomförande.

4.1.2 Granskar åtkomstkontrollrisker inom ramen för ledningens genomgång och tilldelar ansvar på strategisk nivå.

4.2 Informationssäkerhetschef (CISO) / ISMS-ansvarig

4.2.1 Äger ramverket för åtkomstkontroll och säkerställer anpassning till ISO/IEC 27001 och relaterade standarder.

4.2.2 Samordnar tillämpning av policyn, kontrolltestning och rapportering av mätetal för åtkomstkontroll.

4.2.3 Övervakar riskbaserad åtkomstmodellering och följer upp systematiska kontrollbrister.

[... 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 Utlösande faktorer och granskningsfrekvens

9.1.1 Denna policy ska granskas:

9.1.1.1 Årligen, eller

9.1.1.2 Efter större förändringar i IT-infrastruktur, regulatoriska krav eller risknivå

9.1.1.3 Efter incidenter som visar på svagheter i åtkomstkontroller

9.1.1.4 När betydande förändringar sker i autentiseringsteknik eller identitetsplattformar

9.2 Ansvar och granskningsprocess

9.2.1 Informationssäkerhetschef (CISO) eller utsedd ISMS-ansvarig ska hantera granskningscykeln och beakta:

9.2.1.1 Internrevisionsresultat

9.2.1.2 Resultat och mätetal från åtkomstgranskningar

9.2.1.3 Juridiska och regulatoriska uppdateringar

9.2.1.4 Förändringar i teknikplattformar

9.2.2 Alla revideringar ska godkännas av verkställande ledning och kommuniceras till samtliga intressenter.

9.2.3 Berörda användare kan behöva lämna en ny policybekräftelse vid väsentliga uppdateringar.

9.3 Versionsstyrning och dokumentation

9.3.1 Huvudversionen ska lagras i ISMS-dokumentregistret med följande metadata:

9.3.1.1 Versionsnummer och ändringslogg

9.3.1.2 Ikraftträdandedatum och nästa granskningsdatum

9.3.1.3 Ägare och godkännandeinstans

9.3.1.4 Distributions- och bekräftelseposter

9.3.2 Ersatta versioner ska arkiveras och vara tillgängliga i minst 3 år.

10. Relaterade policyer och kopplingar

10.1 Denna policy är funktionellt beroende av och ska tolkas tillsammans med:

10.1.1 P01 – Informationssäkerhetspolicy: Definierar organisationens säkerhetsåtagande och övergripande förväntningar på åtkomstkontroll.

10.1.2 P03 – Policy för godtagbar användning: Anger beteendemässiga villkor för åtkomst och användaransvar för ansvarsfull användning av system.

10.1.3 P05 – Ändringshanteringspolicy: Reglerar hur ändringar i åtkomstkonfigurationer, roller eller gruppstrukturer ska genomföras och testas på ett säkert sätt.

10.1.4 P07 – Policy för introduktion och avslut: Styr initiering och återkallelse av behörigheter i enlighet med händelser i användarens livscykel.

10.1.5 P11 – Policy för hantering av användarkonton och privilegier: Operationaliserar kontroller på kontonivå och kompletterar denna policy med riktlinjer för tekniskt genomförande av åtkomstkontroller.

10.2 Tillsammans utgör dessa policyer ett sammanhållet och bindande ramverk för behörighetsstyrning i olika verksamhetsenheter och tekniska miljöer.

11. Referensstandarder och ramverk

11.1 ISO/IEC 27001:2022:

11.1.1 Klausul 5.15 – Åtkomstkontroll: Denna policy uppfyller kravet på att styra åtkomst till information och andra relaterade tillgångar utifrån verksamhetens behov och krav på informationssäkerhet.

11.1.2 Klausul 5.17 – Identitetshantering och klausul 5.18 – Autentiseringsinformation: Dessa omsätts genom identitetsprovisionering, autentiseringsmekanismer och tilldelning av privilegier.

11.1.3 Bilaga A, kontrollerna 8.2 (Åtkomst till nätverk och nätverkstjänster) och 8.3 (Informationsåtkomstbegränsning): Utgör grunden för denna policys kontrollmål, inklusive rollbaserad åtkomst, integration med användarlivscykeln och skydd av privilegierad åtkomst.

11.2 NIST SP 800-53 Rev. 5:

11.2.1 AC-familjen (AC-1 till AC-20): Denna policy stöder NIST:s krav på åtkomstkontroll för både fysiska och logiska system, inklusive policydefinition (AC-1), kontohantering (AC-2) och funktionsåtskillnad (AC-5).

11.2.2 IA-familjen (IA-1 till IA-8): Ger vägledning för identitetsautentisering, skydd av autentiseringsuppgifter och MFA.

11.2.3 AU-2, AU-12: Krav på loggning och revision som tillämpas genom denna policy stöder användaransvar och incidentutredning.

11.2.4 PE-2 till PE-6: Avser begränsningar för fysiskt tillträde, vilka denna policy delvis upprätthåller genom passerkontroller och behörigheter till byggnader.

11.3 EU:s dataskyddsförordning (GDPR) (2016/679):

11.3.1 Artikel 5.1 f: Personuppgifter ska skyddas mot obehörig åtkomst. Denna policy säkerställer tekniskt och processmässigt genomförande av den principen.

11.3.2 Artikel 32.1 b: Kräver införande av åtkomstkontroller, pseudonymisering och kryptering för att förhindra obehörig behandling av personuppgifter.

11.3.3 Skäl 39: Kräver minimering av åtkomst till personuppgifter, vilket här tillämpas genom principen om minsta privilegium och krav på åtkomstmotivering.

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

11.4.1 Artikel 21.2 c–e: Denna policy möjliggör tekniska och organisatoriska åtgärder för åtkomstkontroll, användarautentisering och skydd av tillgångar hos väsentliga och viktiga verksamhetsutövare.

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

11.5.1 Artikel 6: Kräver policyer för hantering av IKT-risker som uttryckligen omfattar hantering av användaråtkomst och kontroller för identitetslivscykeln. Denna policy uppfyller det kravet för finanssektorn och sektorn för IKT-tjänster.

11.5.2 Artikel 9.2: Denna policy stöder tillämpningen av starka åtkomstkontroller som en del av hanteringen av IKT-tjänster från tredje part och inom koncerner.

11.6 COBIT 2019:

11.6.1 APO07 – Managed Human Resources: Upprätthåller kontroller för introduktion och avslut för att stödja behörighetsstyrning.

11.6.2 BAI03 – Managed Solutions Identification and Build: Integrerar krav på åtkomstkontroll i systemdesign och ändringsprocesser.

11.6.3 DSS01 – Managed Operations och DSS05 – Managed Security Services: Styr tillämpning av begränsningar för logisk åtkomst och övervakning av överträdelser.

11.6.4 MEA03 – Monitor, Evaluate, and Assess Compliance: Stöder revisions- och säkerställandemekanismer för att validera åtkomstkontrollens effektivitet.