					Ange namnet på den registrerade juridiska personen här							
Dokumentnummer: P04S					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**

Anpassad till standarder och regelverk

Standard/regelverk	Klausul/artikel	Kommentar
ISO/IEC 27001:2022	Klausul 5	
ISO/IEC 27002:2022	Kontroller: 5.15, 5.16, 5.17	
NIST SP 800-53 Rev. 5	AC-1 till AC-5	
EU:s dataskyddsförordning (GDPR)	Artikel 32	
EU:s NIS2-direktiv	Artikel 21.2(b)	
EU:s DORA-förordning	Artikel 9	
COBIT 2019	APO07, DSS01	

1. Syfte

1.1. Denna policy anger hur organisationen hanterar åtkomst till system, data och anläggningar för att säkerställa att endast behöriga personer får tillgång till information utifrån verksamhetens behov.

1.2. Den fastställer tydliga regler för tilldelning, ändring, övervakning och borttagning av användarbehörigheter för att minimera risken för obehörig åtkomst och stödja efterlevnad av tillämpliga lagkrav och standarder.

1.3. Policyn tillämpar principen om minsta privilegium, vilket innebär att åtkomst ska begränsas till det minimum som krävs för att utföra arbetsuppgifter.

2. Omfattning

2.1. Denna policy gäller för alla personer som använder eller hanterar åtkomst till organisationens IT-system, nätverk, data eller lokaler, inklusive:

2.1.1. Anställda

2.1.2. Konsulter

2.1.3. Tillfälligt anställda

2.1.4. Externa IT-tjänsteleverantörer

2.2. Den omfattar åtkomst till:

2.2.1. Verksamhetsapplikationer, fildelningar och databaser

2.2.2. E-post, VPN och fjärråtkomstsystem

2.2.3. Molntjänster som används för verksamhetsändamål

2.2.4. Fysiskt tillträde till skyddade anläggningar, såsom kontor eller serverrum

2.3. Denna policy ska tillämpas på alla enheter (företagsägda eller godkända personliga enheter (BYOD)), plattformar och platser.

3. Mål

3.1. Säkerställa att behörigheter endast beviljas efter formellt godkännande baserat på roll och verksamhetsmässig motivering.

3.2. Förhindra obehörig eller alltför omfattande åtkomst till känsliga data, system eller infrastruktur.

3.3. Fastställa tydliga rutiner för tilldelning, ändring och avslut av användarbehörigheter.

3.4. Kräva regelbundna behörighetsgranskningar samt automatiserad eller manuell loggning för att stödja revision.

3.5. Stödja tekniskt genomdrivande av åtkomstbegränsningar genom konfiguration och övervakning.

4. Roller och ansvar

4.1. Verkställande direktör

4.1.1. Godkänner denna policy och säkerställer att resurser finns tillgängliga för att införa effektiva åtkomstkontroller.

4.1.2. Godkänner undantag och granskar årliga åtkomstrevisioner.

4.2. IT-chef / extern IT-tjänsteleverantör

4.2.1. Hanterar tilldelning, ändring och avslut av användarkonton.

4.2.2. Upprätthåller ett register över åtkomstkontroll med all aktivitet (skapande, ändring, borttagning).

4.2.3. Inför rollbaserad åtkomstkontroll (RBAC) och tillämpar stark autentisering, till exempel flerfaktorsautentisering (MFA).

4.2.4. Granskar åtkomstloggar avseende misstänkt aktivitet och rapporterar avvikelser till verkställande direktören.

[... 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. Årlig policygranskning

9.1.1. IT-chefen ska granska denna policy årligen. Ändringar i rättsliga, tekniska eller organisatoriska förhållanden ska utlösa en omedelbar uppdatering.

9.2. Utlösande faktorer för granskning

9.2.1. Policyn ska även granskas om något av följande inträffar:

9.2.2. Större systemändringar eller migrering till molnmiljö

9.2.3. Ändringar i roller eller organisationsstruktur

9.2.4. En säkerhetsincident som rör obehörig åtkomst

9.2.5. Regulatoriska ändringar, till exempel uppdateringar av GDPR, NIS2 eller DORA

9.3. Dokumentation och kommunikation av ändringar

9.3.1. Revideringar ska loggas i versionshistorik, godkännas av verkställande direktören och kommuniceras till all berörd personal.

9.4. Tillgänglighet och utbildning

9.4.1. Denna policy ska göras tillgänglig för all personal, och relevant utbildning ska ges som en del av introduktionen och därefter årligen.

10. Relaterade policyer och kopplingar

10.1. Denna policy ska tillämpas tillsammans med följande SME-policyer för att säkerställa fullständig tillämpning av säker åtkomstpraxis:

10.1.1. P3S – Policy för godtagbar användning: Säkerställer att användare förstår godtagbart beteende vid beviljad åtkomst.

10.1.2. P5S – Ändringshanteringspolicy: Säkerställer att behörigheter är anpassade till godkända systemändringar.

10.1.3. P7S – Policy för introduktion och avslut: Definierar utlösande händelser för behörighetstilldelning och avveckling av användarbehörigheter.

10.1.4. P17S – Policy för dataskydd och integritet: Säkerställer att åtkomstkontroller är anpassade till skyddsåtgärder för personuppgifter.

10.1.5. P30S – Policy för incidenthantering (P30): Definierar hur åtkomstrelaterade incidenter, till exempel missbruk eller överträdelser, hanteras och utreds.

11. Referensstandarder och ramverk

11.1. ISO/IEC 27001

11.1.1. Klausul 5.15 – Kräver formaliserade policyer och processer för åtkomstkontroll.

11.2. ISO/IEC 27002

11.2.1. Kontroller 5.15–5.17 – Anger detaljerad vägledning för rollbaserad åtkomst, hantering av användares livscykel och hantering av privilegierad åtkomst.

11.3. NIST SP 800-53 Rev. 5

11.3.1. AC-1 till AC-5 – Kräver strukturerade policyer för åtkomsthantering, inklusive auktorisering av konton, granskning och övervakning.

11.4. EU:s dataskyddsförordning (GDPR)

11.4.1. Artikel 32 – Kräver tekniska och organisatoriska åtgärder, såsom åtkomsthantering, för att säkerställa säkerhet och konfidentialitet för personuppgifter.

11.5. EU:s NIS2-direktiv

11.5.1. Artikel 21.2(b) – Kräver operativ åtkomstkontroll och system för identitets- och åtkomsthantering för att förhindra obehörig systemåtkomst.

11.6. EU:s DORA-förordning

11.6.1. Artikel 9 – Betonar säker hantering av IKT-risker, inklusive robust åtkomstkontroll för finansiella entiteter.

11.7. COBIT 2019

11.7.1. APO07 – Managed Security: Kräver definierat och tillämpat ansvar för åtkomst.

11.7.2. DSS01 – Manage Operations: Omfattar rutiner för hantering av logisk åtkomst och upprätthållande av säkra driftsmiljöer.