					Indsæt navnet på den registrerede juridiske enhed her						
Dokumentnummer: P11S					Dokumenttitel: **Politik for brugeradgangsstyring og privilegeret adgang**						
Version: 1.0		Ikrafttrædelsesdato: 01.01.2025			Dokumentejer:						
X	Politik		Standard		Procedure		Formular		Register		Andet

Revisionshistorik				
Revisionsnummer	**Revisionsdato**	**Ændringer**	**Gennemgået af**	**Procesejer**

Godkendelser			
Navn	**Stilling**	**Dato**	**Underskrift**

Tilpasset relevante standarder og regler

Standard/regulering	Klausul/artikel	Kommentar
ISO/IEC 27001:2022	Klausul 5.3, 8	Roller, ansvar samt operationel planlægning og kontrol for brugeradgangsstyring
ISO/IEC 27002:2022	Kontrol 8	Kontroller for tildeling, gennemgang og fjernelse af privilegerede rettigheder
NIST SP 800-53 Rev.5	AC-2, AC-5, AC-6	Oprettelse af konti, overvågning, princippet om mindst privilegium og funktionsadskillelse
EU NIS2	Artikel 21(2)(d)	Brugeradgangsstyring for væsentlige og vigtige enheder
EU DORA	Artikel 9(2)(b)	Styring af privilegeret adgang i finansielle enheder
COBIT 2019	DSS05.03, DSS05.04	Tildeling af adgang, fjernelse af adgang og periodisk gennemgang af brugeradgang
EU GDPR	Artikel 32	Passende adgangskontroller til beskyttelse af personoplysninger

1. Formål

1.1 Denne politik fastsætter krav til styring af brugerkonti og adgangsrettigheder på en sikker, ensartet og sporbar måde. Den sikrer, at kun autoriserede brugere har adgang til systemer og data, og at adgangen er passende i forhold til deres rolle og ansvar.

1.2 Effektiv styring af konti og privilegier er afgørende for at forebygge uautoriseret adgang, minimere insidertrusler og sikre overholdelse af ISO/IEC 27001, GDPR og øvrige regulatoriske krav.

1.3 Denne politik gør det muligt for organisationen at fastlægge ejerskab og ansvar for brug af konti, overvåge og revidere rettighedseskalering samt deaktivere eller tilbagekalde adgang sikkert, når der ikke længere er et forretningsmæssigt behov.

1.4 Den beskytter desuden forretningsdriften mod driftsfejl eller misbrug som følge af for omfattende eller utilstrækkeligt overvåget adgang og bidrager til at reducere risikoen for utilsigtet datalækage, misbrug af privilegier eller manglende regulatorisk efterlevelse.

2. Omfang

2.1 Denne politik gælder for:

2.1.1 Alle medarbejdere, praktikanter, kontraktansatte og tredjepartsbrugere med adgang til organisationens IT-systemer

2.1.2 Alle systemer, enheder, tjenester og platforme, som administreres af eller på vegne af organisationen, herunder cloudplatforme, on-premises-infrastruktur og tredjepartsværktøjer

2.2 Den omfatter alle typer brugerkonti, herunder:

2.2.1 Personlige brugerkonti (f.eks. e-mailkonti, systemlogin)

2.2.2 Administratorkonti og systemkonti

2.2.3 Midlertidige legitimationsoplysninger til gæste- eller tredjepartsadgang

2.2.4 Tjenestekonti, der anvendes af applikationer eller automatiseringssystemer

2.3 Politikken gælder for hele kontoens livscyklus – fra oprettelse og godkendelse til ændring, overvågning og deaktivering. Dette omfatter den indledende tildeling af adgang under onboarding, gennemgang af adgangsrettigheder ved rolleændringer og tilbagekaldelse som led i fratrædelsesprocessen.

3. Mål

3.1 At tildele unikke og sporbare brugeridentiteter til alle systembrugere for at sikre ansvarlighed og eliminere afhængighed af delte legitimationsoplysninger.

3.2 At håndhæve princippet om mindst privilegium, så brugere kun tildeles det minimumsniveau af adgang, der er nødvendigt for at udføre deres arbejdsopgaver.

3.3 At forebygge uautoriseret adgang til følsomme systemer eller data gennem klart dokumenterede processer for godkendelse og gennemgang.

3.4 At sikre rettidig deaktivering af brugerkonti, når de ikke længere er nødvendige, f.eks. ved fratrædelse, kontraktophør eller rolleændringer.

3.5 At opretholde et sikkert og revisionsklart miljø ved at dokumentere alle kontoændringer, godkendelser og periodiske gennemgange.

3.6 At sikre, at rettighedseskalering er strengt kontrolleret, godkendt uafhængigt og logget, og at privilegeret adgang tilbagekaldes straks, når der ikke længere er behov for den.

4. Roller og ansvar

4.1 Direktør (GM)

4.1.1 Har det overordnede ansvar for håndhævelse af denne politik.

4.1.2 Sikrer, at praksis for kontostyring er afstemt med kravene til ISO/IEC 27001-certificering og relevante retlige forpligtelser (f.eks. GDPR).

4.1.3 Skal straks orienteres om enhver uautoriseret adgang, sikkerhedshændelse eller overtrædelse af politikken relateret til brugerkonti.

4.1.4 Fører tilsyn med gennemgang af politikken, revisioner og håndhævelsestiltag.

4.2 IT-ansvarlig eller ekstern IT-leverandør

4.2.1 Er ansvarlig for den tekniske implementering af konto- og privilegiekontroller på tværs af de systemer, organisationen anvender.

4.2.2 Må kun tildele, ændre og deaktivere brugerkonti på grundlag af dokumenterede godkendelser.

4.2.3 Skal håndhæve krav til adgangskodekompleksitet, automatisk skærmlås ved inaktivitet, multifaktorautentifikation (MFA), hvor det er tilgængeligt, samt systemlogning.

4.2.4 Skal opretholde sikre registreringer af alle adgangsgodkendelser, kontoejerskab, rettighedseskaleringer og tilbagekaldelser.

4.2.5 Skal overvåge for uautoriserede eller forældreløse konti og rapportere afvigelser til direktøren.

[... Afsnit 4.3–8 er ikke inkluderet i denne forhåndsvisning. Køb det fulde dokument for at få adgang til det komplette indhold. ...]

9. Krav til gennemgang og opdatering

9.1 Denne politik skal gennemgås mindst én gang årligt af direktøren og den IT-ansvarlige for at sikre overholdelse af:

9.1.1 Gældende kontroller og vejledning i ISO/IEC 27001:2022

9.1.2 Regulatoriske opdateringer (f.eks. GDPR, DORA, NIS2)

9.1.3 Ændringer i systemer, tjenester eller forretningsstruktur

9.2 Gennemgang skal også gennemføres efter:

9.2.1 Væsentlige sikkerhedshændelser eller revisionskonstateringer

9.2.2 Større ændringer i IT-systemer eller kontoarkitektur

9.2.3 Indførelse af nye platforme, der kræver integration med adgangsstyring

9.3 Alle ændringer skal godkendes af direktøren og kommunikeres klart til berørte medarbejdere.

10. Relaterede politikker og sammenhænge

10.1 P2S – Politik for styringsroller og ansvarsområder: Fastlægger ansvar og beslutningskompetence for adgangsgodkendelser og tilsyn.

10.2 P4S – Politik for adgangskontrol: Regulerer håndhævelse af adgangsstyring på tværs af systemer og autentifikationsmetoder.

10.3 P7S – Politik for onboarding og fratrædelse: Sikrer, at oprettelse og fjernelse af konti indgår i HR-styrede personaleændringer.

10.4 P8S – Politik for informationssikkerhedsbevidsthed og -uddannelse: Uddanner brugere i sikker praksis for konti og forventninger til anvendelse.

10.5 P30S – Politik for hændelsesrespons: Definerer de handlinger, der skal iværksættes, hvis misbrug af konti fører til et sikkerhedsbrud eller uautoriseret videregivelse.

11. Referencestandarder og rammeværk

11.1 ISO/IEC 27001

11.1.1 Klausul 5.3: Kræver, at roller og ansvar for informationssikkerhed er klart tildelt og håndhævet.

11.1.2 Klausul 8.1: Operationel planlægning og kontrol skal omfatte brugeradgangsstyring.

11.2 ISO/IEC 27002

11.2.1 Kontrol 8.2: Beskriver tekniske og proceduremæssige kontroller for tildeling, gennemgang og fjernelse af privilegerede rettigheder.

11.3 NIST SP 800-53 Rev.5

11.3.1 AC-2: Kræver oprettelse, overvågning og tilbagekaldelse af konti på grundlag af definerede roller og processer.

11.3.2 AC-5: Omhandler funktionsadskillelse for at forebygge konflikter eller misbrug af privilegier.

11.3.3 AC-6: Kræver anvendelse af princippet om mindst privilegium på alle adgangsrettigheder.

11.4 EU GDPR

11.4.1 Artikel 32: Kræver passende adgangskontroller for at beskytte personoplysninger mod uautoriseret adgang eller ændring.

11.5 EU NIS

11.5.1 Artikel 21(2)(d): Kræver brugeradgangsstyring som en del af de centrale sikkerhedskontroller for væsentlige og vigtige enheder.

11.6 EU DORA

11.6.1 Artikel 9(2)(b): Kræver, at finansielle enheder implementerer adgangskontroller, der begrænser og overvåger privilegerede rettigheder.

11.7 COBIT 2019

11.7.1 DSS05.03: Specificerer tildeling og fjernelse af adgang som en del af IT-styring.

11.7.2 DSS05.04: Kræver løbende gennemgang og tilpasning af brugeradgang i forhold til organisatoriske roller.