					Indsæt navnet på den registrerede juridiske enhed her							
Dokumentnummer: P11					Dokumenttitel: **Politik for styring af brugerkonti og privilegier**							
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	Bemærkning
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 GDPR	Artikel 5(1)(f), 32; betragtning 39	-
EU NIS2	Artikel 21(2)(a, d), 21(3)	-
EU DORA	Artikel 5, 9	-
COBIT 2019	DSS01, DSS05, APO13	-

1. Formål

1. Denne politik fastsætter obligatoriske kontroller for styring af brugerkonti og privilegier på tværs af alle informationssystemer og tjenester. Den sikrer, at adgang til organisationens ressourcer tildeles på grundlag af valideret identitet, rollebaseret behov samt princippet om mindst privilegium og funktionsadskillelse.

1.1 Den understøtter organisationens forpligtelse til informationssikkerhed ved at implementere strukturerede og revisionsbare processer for tildeling af adgang, tildeling af privilegier, overvågning af brug og tilbagekaldelse af konti.

1.2 Denne politik er afgørende for at reducere risikoen for uautoriseret adgang, misbrug af privilegier, insidertrusler og manglende efterlevelse af gældende regulatoriske rammer.

2. Omfang

2.1 Denne politik gælder for alle medarbejdere, kontraktansatte, tredjepartsleverandører, konsulenter og andre personer, der har fået adgang til organisationens IT-ressourcer, applikationer eller data.

2.2 Den omfatter alle systemer og miljøer, hvor mekanismer til brugergodkendelse og adgangsstyring anvendes, herunder, men ikke begrænset til:

2.2.1 Virksomhedsapplikationer og databaser

2.2.2 Cloudplatforme og SaaS-miljøer

2.2.3 Operativsystemer og administrative konsoller

2.2.4 Værktøjer til fjernadgang og VPN

2.2.5 IAM-systemer

2.3 Politikken omfatter både standardbrugerkonti og privilegerede brugerkonti og inkluderer kontroller for:

2.3.1 Oprettelse, ændring og deaktivering af konti

2.3.2 Eskalering af rettigheder og delegering

2.3.3 Sessionsstyring og overvågning

2.3.4 Autentifikationsmetoder og styring af legitimationsoplysninger

3. Mål

3.1 At sikre, at alle brugerkonti er entydigt identificerbare, korrekt autoriserede og kun tildeles efter formel validering af behov.

3.2 At implementere princippet om mindst privilegium og forhindre unødvendig eller overdreven adgang ved at håndhæve strenge kontroller for tildeling og brug af privilegerede konti.

3.3 At kræve rettidige opdateringer af kontostatus på baggrund af ændringer i ansættelse eller rolle, herunder øjeblikkelig deaktivering ved fratrædelse.

3.4 At muliggøre proaktiv detektion og afhjælpning af inaktive, misbrugte eller uautoriserede konti via logning, gennemgange og automatisering.

3.5 At opretholde overensstemmelse med ISO/IEC 27001:2022 og tilknyttede standarder samt opfylde forpligtelser efter relevante lovgivningsmæssige og regulatoriske rammer såsom GDPR, NIS2, DORA og COBIT 2019.

4. Roller og ansvar

4.1 Chief Information Security Officer (CISO)

4.1.1 Er ansvarlig for denne politik og sikrer dens håndhævelse i hele organisationen.

4.1.2 Gennemgår og godkender eventuelle formelle undtagelser eller tilfælde af nødadgang.

4.1.3 Rapporterer revisionsresultater vedrørende konti og eskalerer risici til direktionen.

4.2 Ansvarlig for adgangsstyring / IT-administrator

4.2.1 Vedligeholder og driver de tekniske kontroller for styring af brugerkontis adgangslivscyklus.

4.2.2 Udfører tildeling af adgang, fjernelse af adgang og styring af privilegeret adgang på grundlag af godkendte anmodninger.

4.2.3 Vedligeholder et autoritativt register over alle brugerkonti, deres status og privilegieniveau.

4.2.4 Understøtter revisioner og compliance-gennemgange med logfiler og aktivitetsrapporter.

[... 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 årligt eller ved væsentlige ændringer i:

9.1.1 Organisationsstruktur eller forretningsprocesser

9.1.2 IT-systemer, identitetsplatforme eller adgangsmetoder

9.1.3 Regulatoriske eller kontraktuelle krav vedrørende identitets- og adgangsstyring

9.2 Chief Information Security Officer (CISO) er sammen med den ansvarlige for adgangsstyring ansvarlig for at igangsætte gennemgangsprocessen og koordinere feedback fra interessenter.

9.3 Mellemliggende gennemgange kan udløses af:

9.3.1 Sikkerhedshændelser relateret til misbrug af konti

9.3.2 Revisionsresultater, der påviser mangler i styring af adgangslivscyklussen

9.3.3 Implementering af nye værktøjer til identitetsstyring eller privilegeret adgangsstyring (PAM)

9.4 Opdateringer til denne politik skal være:

9.4.1 Underlagt versionsstyring og registreret i ISMS-dokumentationsbiblioteket

9.4.2 Kommunikeret til alle relevante interessenter, herunder afdelingsledere, IT-drift og HR

9.4.3 Understøttet af opdateret træningsmateriale og procedurevejledninger

9.5 Alle ændringer skal godkendes af direktionen eller styregruppen for informationssikkerhed og logges til revisionsformål.

10. Relaterede politikker og sammenhænge

10.1 Denne politik er operationelt forbundet med og understøttet af følgende relaterede politikker i ISMS-porteføljen:

10.1.1 P4 politik for adgangskontrol: Fastlægger de overordnede principper og mekanismer for adgangsstyring, herunder regelbaserede og rollebaserede kontroller.

10.1.2 P7 politik for onboarding og offboarding: Angiver de proceduremæssige trin for initiering og afslutning af brugeradgang i overensstemmelse med HR-handlinger.

10.1.3 P8 politik for informationssikkerhedsbevidsthed og -uddannelse: Understøtter brugeransvar for kontosikkerhed og beskyttelse af legitimationsoplysninger.

10.1.4 P13 politik for dataklassifikation og mærkning: Vejleder om adgangsniveauer på baggrund af dataklassifikation og sikrer, at privilegiegrænser er i overensstemmelse med følsomhedsniveauer.

10.1.5 P22 lognings- og overvågningspolitik: Sikrer, at revisionsspor indsamles for alle kontorelaterede aktiviteter og gennemgås for at detektere anomalier eller uautoriseret brug.

10.1.6 P30 politik for hændelsesrespons: Regulerer eskalering, inddæmning og efterfølgende handlinger ved misbrug af privilegier eller uautoriseret kontoaktivitet.

10.2 Hver af disse politikker virker sammen for at håndhæve en sammenhængende, risikobaseret ramme for identitets- og adgangsstyring på tværs af organisationen.

11. Referencestandarder og rammeværk

11.1 Denne politik er tilpasset globalt anerkendte cybersikkerhedsstandarder og regulatoriske rammer, der stiller krav om sikker styring af identitet, adgang og privilegier som en central del af organisationens informationssikkerhed.

11.2 ISO/IEC 27001:

11.2.1 Klausul 6.1.3 kræver, at organisationer identificerer, evaluerer og behandler informationssikkerhedsrisici, hvilket gør styring af adgang og privilegier til en formel, risikobaseret kontrol forankret i ISMS'ets planlægningsproces.

11.2.2 Klausul 8.1 - driftsplanlægning og kontrol: Understøtter implementering af tekniske og proceduremæssige sikkerhedsforanstaltninger, der regulerer brugeradgang og privilegeret adgang.

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

11.3.1 Kontrol 5.15 - brugeradgangsstyring: Understøtter formelle processer for tildeling af adgang, adgangsautorisation og periodisk gennemgang af adgangsrettigheder.

11.3.2 Kontrol 5.16 - identitetsstyring: Fastlægger entydighed af identiteter, livscykluskontroller og håndhævelse af sikker autentifikation.

11.3.3 Kontrol 5.17 sikrer, at tildeling og brug af privilegerede adgangsrettigheder er strengt kontrolleret, sporbar og i overensstemmelse med princippet om mindst privilegium gennem hele brugerkontoens livscyklus.

11.3.4 Kontrol 5.18 - privilegerede adgangsrettigheder: Er fuldt adresseret gennem rollebaseret tildeling af privilegier, revision og krav om godkendelse af forhøjet adgang.

11.4 Disse kontroller understøtter en struktureret implementering af kontoregistrering, afregistrering, adskillelse af privilegier og brug af autentifikationsoplysninger. Politikken håndhæver styring af identitetslivscyklussen, just-in-time-adgang og overvågning af forhøjede sessioner for at forhindre uautoriseret systembrug.

11.5 NIST SP 800-53 Rev. 5:

11.5.1 AC-1 (politik for adgangskontrol) og AC-2 (kontostyring): Er kortlagt gennem politikkrav til adgangsgodkendelser, rolletildeling og revision af brugerkonti.

11.5.2 AC-5 (funktionsadskillelse) og AC-6 (princippet om mindst privilegium): Opfyldes gennem begrænsning af privilegier, tilpasning til jobroller og dobbeltgodkendelse ved højrisikoopgaver.

11.5.3 IA-2 til IA-5 (identifikation og autentifikation): Håndhæves via stærke autentifikationsmekanismer, regler for legitimationsoplysningers livscyklus og krav om MFA.

11.5.4 AU-2, AU-12 (revisionslogning og analyse): Adresseres gennem logning af sessioner og overvågning af privilegeret aktivitet på tværs af følsomme miljøer.

11.6 EU GDPR (2016/679):

11.6.1 Artikel 32 - behandlingssikkerhed: Kræver adgangskontroller og mekanismer til identitetsverifikation for at beskytte personoplysninger. Dette opfyldes ved at kræve kontogodkendelser, gennemgang af privilegier og stærke autentifikationsforanstaltninger.

11.6.2 Artikel 5(1)(f) - integritet og fortrolighed: Sikrer, at personoplysninger kun tilgås af autoriserede brugere med legitime roller, understøttet af håndhævelse af kontostyring.

11.6.3 Betragtning 39: Kræver klare begrænsninger i adgang og ansvarlighed - denne politik understøtter fuld sporbarhed af brugeridentiteter og tildeling af privilegier.

11.7 EU NIS2-direktivet (2022/2555):

11.7.1 Artikel 21(2)(a, d): Kræver, at enheder håndhæver politikker for adgangsstyring og sikker håndtering af legitimationsoplysninger og privilegerede sessioner, understøttet gennem denne politiks kontroller for tildeling af adgang, overvågning og undtagelser.

11.7.2 Artikel 21(3): Fremmer adgangsdisciplin og høj sikkerhed for identitetsbekræftelse i kritiske sektorer, opfyldt gennem brug af unikke ID'er, RBAC og tidsbegrænset forhøjet adgang.

11.8 EU DORA (2022/2554):

11.8.1 Artikel 5 - IKT-styring og kontrol: Kræver formaliserede processer for styring af IKT-brugere, dækket gennem dokumenteret tildeling af adgang, deaktivering og undtagelseshåndtering.

11.8.2 Artikel 9 - styring af IKT-risiko: Påbyder organisationer at sikre systemer gennem adgangsbegrænsninger og overvågning, adresseret via MFA, logning af privilegeret adgang og centraliserede gennemgange.

11.9 COBIT 2019:

11.9.1 DSS01 - styrede driftsaktiviteter: Fremmer håndhævelse af standardiserede driftskontroller, herunder styring af brugerkontienes livscyklus og dokumentation af adgang.

11.9.2 DSS05 - styrede sikkerhedstjenester: Afspejler sikker administration af bruger- og systemprivilegier og understøtter risikoafdækning gennem princippet om mindst privilegium og validering af revisionsspor.

11.9.3 APO13 - styret sikkerhed: Kræver governance for adgang på tværs af digitale aktiver, opfyldt gennem formaliseret autorisation af konti og roller med krav om periodisk gennemgang.