					Indsæt navnet på den registrerede juridiske enhed her							
Dokumentnummer: P04					Dokumenttitel: **Politik for adgangskontrol**							
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 reguleringer

Standard/regulering	Klausul/artikel	Kommentar
ISO/IEC 27001:2022	Klausul 5.15, 5.17, 5.18	Logisk og fysisk adgangskontrol
ISO/IEC 27002:2022	Kontrol 8.2, 8.3	Rollebaseret adgangskontrol og identitetsstyring
NIST SP 800-53 Rev. 5	AC-1 til AC-20, IA-1 til IA-8	Konto- og adgangskontroller, identitet og autentifikation
EU GDPR	Artikel 5(1)(f), 32(1)(b); betragtning 39	Databeskyttelse og dataminimering
EU NIS2	Artikel 21(2)(c–e)	Adgangskontrol, brugergodkendelse og beskyttelse af aktiver
EU DORA	Artikel 6, 9(2)	IKT- og brugeradgang samt stærke kontroller for tredjeparter
COBIT 2019	APO07, BAI03, DSS01, DSS05, MEA03	Onboarding, drift, overvågning og efterlevelse

1. Formål

1.1 Denne politik fastsætter obligatoriske principper, ansvarsforhold og kontrolkrav for styring af adgang til informationssystemer, applikationer, fysiske faciliteter og dataaktiver i hele organisationen.

1.2 Den sikrer, at adgang tildeles på baggrund af forretningsmæssigt behov, jobfunktion og risikoprofil og håndhæver principperne om mindst privilegium, need-to-know og funktionsadskillelse.

1.3 Politikken understøtter implementeringen af ISO/IEC 27001:2022, klausul 5.15, og relaterede kontroller for logisk og fysisk adgang, brugergodkendelse og styring af adgangens livscyklus.

1.4 Denne politik danner grundlag for beskyttelse af digitale og fysiske ressourcer mod uautoriseret brug, misbrug eller kompromittering.

2. Omfang

2.1 Denne politik gælder for alle brugere, systemer og faciliteter inden for ISMS'ets omfang, herunder:

2.1.1 Medarbejdere, konsulenter, leverandører og midlertidigt personale

2.1.2 Lokal infrastruktur, cloud-hostede systemer og hybride miljøer

2.1.3 Alle virksomhedens aktiver – hardware, software, data og sikrede fysiske områder

2.1.4 Logisk adgang (f.eks. systemer, netværk, applikationer, API'er) og fysisk adgang (f.eks. bygninger, datacentre)

2.2 Den regulerer adgang gennem hele identitets- og ressourceinteraktionens livscyklus, fra onboarding og tildeling af adgang til rolleændringer og fratrædelse.

2.3 Politikken omfatter også Bring Your Own Device (BYOD) og fjernadgang, så kontrollerne er ensartede på tværs af lokationer og modeller for enhedsejerskab.

3. Mål

3.1 At implementere sikre, rollebaserede adgangskontroller, der understøtter operationel integritet og regulatorisk efterlevelse.

3.2 At sikre, at adgangsrettigheder godkendes, overvåges og tilbagekaldes rettidigt.

3.3 At forhindre uautoriseret adgang, eskalering af rettigheder eller fortsat eksistens af forældede adgangsrettigheder.

3.4 At understøtte zero trust-principper ved som udgangspunkt at afvise adgang, medmindre den er udtrykkeligt godkendt og begrundet.

3.5 At give auditorer og interessenter sikkerhed gennem evidensbaserede, automatiserede adgangsgennemgange og håndhævelse af politikken.

3.6 At indarbejde adgangskontrol i forretningsprocesser, HR-livscyklushændelser og tekniske arkitekturer.

4. Roller og ansvar

4.1 Øverste ledelse

4.1.1 Godkender politikken for adgangskontrol og sikrer passende budget og bemanding til håndhævelse.

4.1.2 Gennemgår risici vedrørende adgangskontrol som led i ledelsens gennemgang og forankrer ansvaret på strategisk niveau.

4.2 CISO / ISMS-ansvarlig

4.2.1 Ejer styringsrammen for adgangskontrol og sikrer overensstemmelse med ISO/IEC 27001 og relaterede standarder.

4.2.2 Koordinerer håndhævelse af politikken, kontroltest og rapportering af målepunkter for adgangskontrol.

4.2.3 Fører tilsyn med risikobaseret modellering af adgang og overvåger systemiske kontrolsvagheder.

[... 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 Udløsende forhold og hyppighed for gennemgang

9.1.1 Denne politik skal gennemgås:

9.1.1.1 Årligt, eller

9.1.1.2 Efter en væsentlig ændring i IT-infrastruktur, regulatoriske krav eller risikoprofil

9.1.1.3 Efter hændelser, der afdækker svagheder i adgangskontroller

9.1.1.4 Når der sker væsentlige ændringer i autentifikationsteknologier eller identitetsplatforme

9.2 Ansvar og proces for gennemgang

9.2.1 CISO eller udpeget ISMS-ansvarlig skal styre gennemgangscyklussen og inddrage:

9.2.1.1 Konklusioner fra intern revision

9.2.1.2 Resultater og målepunkter fra adgangsgennemgange

9.2.1.3 Juridiske og regulatoriske opdateringer

9.2.1.4 Ændringer i teknologiplatforme

9.2.2 Alle ændringer skal godkendes af den øverste ledelse og kommunikeres til alle interessenter.

9.2.3 Berørte brugere kan blive pålagt at bekræfte politikken på ny ved væsentlige opdateringer.

9.3 Versionsstyring og dokumentation

9.3.1 Hovedversionen skal opbevares i ISMS-dokumentarkivet med følgende metadata:

9.3.1.1 Versionsnummer og ændringslog

9.3.1.2 Ikrafttrædelsesdato og dato for næste gennemgang

9.3.1.3 Ejer og godkendelsesmyndighed

9.3.1.4 Registrering af distribution og bekræftelse

9.3.2 Erstattede versioner skal arkiveres og være tilgængelige i mindst 3 år.

10. Relaterede politikker og sammenhænge

10.1 Denne politik er funktionelt afhængig af og skal fortolkes sammen med:

10.1.1 P01 – Informationssikkerhedspolitik: Definerer organisationens sikkerhedsforpligtelse og overordnede forventninger til adgangskontrol.

10.1.2 P03 – Politik for acceptabel brug: Fastlægger adfærdsmæssige vilkår for adgang og brugeransvar for forsvarlig brug af systemer.

10.1.3 P05 – Politik for ændringsstyring: Regulerer, hvordan ændringer i adgangskonfigurationer, roller eller gruppestrukturer skal implementeres og testes sikkert.

10.1.4 P07 – Politik for onboarding og fratrædelse: Regulerer initiering og tilbagekaldelse af adgangsrettigheder i overensstemmelse med hændelser i brugerens livscyklus.

10.1.5 P11 – Politik for styring af brugerkonti og privilegier: Operationaliserer kontonære kontroller og supplerer denne politik med tekniske retningslinjer for håndhævelse af adgang.

10.2 Samlet udgør disse politikker en sammenhængende og håndhævelig styringsramme for adgang på tværs af forretningsenheder og teknologier.

11. Referencestandarder og rammeværker

11.1 ISO/IEC 27001:2022:

11.1.1 Klausul 5.15 – Adgangskontrol: Denne politik opfylder kravet om at kontrollere adgang til information og andre tilknyttede aktiver på baggrund af forretningsmæssige behov og krav til informationssikkerhed.

11.1.2 Klausul 5.17 – Identitetsstyring og klausul 5.18 – Autentifikationsoplysninger: Disse operationaliseres gennem identitetstildeling, autentifikationsmekanismer og tildeling af privilegier.

11.1.3 Bilag A, kontroller 8.2 (adgangskontrol) og 8.3 (identitetsstyring): Danner grundlag for denne politiks kontrolmål, herunder rollebaseret adgang, integration med brugerens livscyklus og beskyttelse af privilegeret adgang.

11.2 NIST SP 800-53 Rev. 5:

11.2.1 AC-familien (AC-1 til AC-20): Denne politik understøtter NIST's krav til adgangskontrol for både fysiske og logiske systemer, herunder politikdefinition (AC-1), kontostyring (AC-2) og funktionsadskillelse (AC-5).

11.2.2 IA-familien (IA-1 til IA-8): Giver vejledning om identitetsgodkendelse, beskyttelse af legitimationsoplysninger og MFA.

11.2.3 AU-2, AU-12: Krav til logning og revision, der håndhæves under denne politik, understøtter brugeransvarlighed og undersøgelse af hændelser.

11.2.4 PE-2 til PE-6: Omhandler begrænsninger i fysisk adgang, som denne politik delvist håndhæver gennem badgekontroller og bygningstilladelser.

11.3 EU GDPR (2016/679):

11.3.1 Artikel 5(1)(f): Personoplysninger skal beskyttes mod uautoriseret adgang. Denne politik sikrer teknisk og proceduremæssig håndhævelse af dette princip.

11.3.2 Artikel 32(1)(b): Kræver implementering af adgangskontroller, pseudonymisering og kryptering for at forhindre uautoriseret behandling af personoplysninger.

11.3.3 Betragtning 39: Kræver minimering af adgang til personoplysninger, hvilket her håndhæves gennem mindst privilegium og krav om begrundelse for adgang.

11.4 EU NIS2-direktivet (2022/2555):

11.4.1 Artikel 21(2)(c–e): Denne politik muliggør tekniske og organisatoriske foranstaltninger for adgangskontrol, brugergodkendelse og beskyttelse af aktiver på tværs af væsentlige og vigtige enheder.

11.5 EU DORA (2022/2554):

11.5.1 Artikel 6: Kræver politikker for styring af IKT-risici, som udtrykkeligt omfatter styring af brugeradgang og kontroller for identitetens livscyklus. Denne politik opfylder dette krav for den finansielle sektor og IKT-tjenestesektoren.

11.5.2 Artikel 9(2): Denne politik understøtter håndhævelse af stærke adgangskontroller som led i styring af tredjeparts- og koncerninterne IKT-tjenester.

11.6 COBIT 2019:

11.6.1 APO07 – Managed Human Resources: Håndhæver kontroller for onboarding og fratrædelse til understøttelse af adgangsstyring.

11.6.2 BAI03 – Managed Solutions Identification and Build: Indarbejder krav til adgangskontrol i systemdesign og ændringsprocesser.

11.6.3 DSS01 – Managed Operations og DSS05 – Managed Security Services: Regulerer håndhævelse af begrænsninger i logisk adgang og overvågning af overtrædelser.

11.6.4 MEA03 – Monitor, Evaluate, and Assess Compliance: Understøtter revisions- og sikkerhedsmekanismer til validering af adgangskontrollernes effektivitet.