					Indsæt navnet på den registrerede juridiske enhed her							
Dokumentnummer: P03					Dokumenttitel: **Politik for acceptabel brug**							
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	Fastlægger adfærdsnormer og krav for politikken for acceptabel brug
ISO/IEC 27002:2022	Kontroller 6.1, 6.2, 8.1, 8.12	Vejleder om ansvar for informationssikkerhed, awareness og styring af enheder og data
NIST SP 800-53 Rev.5	AC-19, AC-20, AT-2	Adgangskontrol og awareness-/adfærdskontroller med relevans for brug af IT-aktiver
EU GDPR	Artikel 5, stk. 1, litra f, 32; betragtning 39	Fastsætter krav til fortrolighed og integritet samt tekniske og organisatoriske kontroller og lovligt grundlag for korrekt brug
EU NIS2	Artikel 21, stk. 2, litra a-d	Kræver operationelle politikker og oplæring i sikker brug
EU DORA	Artikel 5	Understøtter styring af IKT-risici ved at regulere brugeradfærd
COBIT 2019	APO07, BAI05, DSS05, MEA01	Menneskelige ressourcer, ændringsstyring, styrede sikkerhedstjenester samt overvågning af efterlevelse og performance

1. Formål

1.1 Denne politik fastlægger acceptabel og uacceptabel brug af organisationens informationssystemer, IT-ressourcer, kommunikationsværktøjer og praksis for databehandling.

1.2 Den sikrer, at alle brugere forstår deres ansvar ved brug af virksomhedens IT-aktiver, og at deres handlinger understøtter fortrolighed, integritet, tilgængelighed og lovlig behandling af oplysninger.

1.3 Politikken opfylder ISO/IEC 27001:2022, kontrol 5.10, ved at fastlægge adfærdsnormer for systembrug og anvende tekniske og proceduremæssige sikkerhedsforanstaltninger for at minimere risikoen for misbrug, forsømmelighed eller retsstridig anvendelse.

1.4 Den understøtter også undersøgelses- og håndhævelsesaktiviteter, herunder hændelsesrespons og disciplinære foranstaltninger ved overtrædelser.

2. Omfang

2.1 Denne politik gælder for alle personer og enheder, der har fået adgang til organisationens informationssystemer og aktiver, herunder, men ikke begrænset til:

2.1.1 Medarbejdere, kontraktansatte, konsulenter, praktikanter og vikarer

2.1.2 Tredjeparter med systemadgang eller delegerede administrative roller

2.1.3 Gæster eller partnere, der anvender organisationsejet eller godkendt IT-infrastruktur

2.2 Omfanget omfatter alle organisationens teknologi- og dataaktiver, herunder:

2.2.1 Arbejdsstationer, bærbare computere, mobile enheder og servere

2.2.2 Netværksinfrastruktur og cloudbaserede tjenester

2.2.3 E-mail, beskedtjenester, fillagring, samarbejdsplatforme og VPN-forbindelser

2.2.4 Data i hvile, under overførsel eller under behandling, uanset format eller placering

2.2.5 Enhver personlig enhed, der anvendes under en BYOD-ordning (Bring Your Own Device), og som opretter forbindelse til organisationens systemer

2.3 Denne politik håndhæves i alle arbejdsmiljøer, herunder:

2.3.1 Virksomhedens kontorer og produktionssteder

2.3.2 Hjemmearbejdspladser eller hybride arbejdsformer

2.3.3 Feltbaserede aktiviteter eller lokationer drevet af tredjepart

2.4 Alle brugere skal anerkende og overholde denne politik som betingelse for adgang til virksomhedens systemer eller håndtering af virksomhedens data.

3. Mål

3.1 At fastlægge og håndhæve regler for acceptabel brug af organisationens IT-ressourcer.

3.2 At forhindre uautoriseret adgang, datalækage eller skade som følge af forsømmelig eller ondsindet brug.

3.3 At beskytte virksomhedens netværk, aktiver og data mod trusler, der opstår som følge af brugeradfærd.

3.4 At understøtte juridiske og kontraktmæssige forpligtelser ved at dokumentere rettidig omhu i styringen af IT-ressourcer.

3.5 At sikre ensartethed og klarhed i anvendelsen af disciplinære foranstaltninger og processer for håndtering af undtagelser.

3.6 At fremme en kultur for etisk, sikker og ansvarlig brug af digitale og fysiske IT-ressourcer.

4. Roller og ansvar

4.1 Direktionen

4.1.1 Godkender politikken for acceptabel brug (AUP) og sikrer, at den er afstemt med forretningsmål, regulatoriske krav og organisationens værdier.

4.1.2 Afsætter ressourcer til håndhævelse, oplæring, overvågning og gennemgang af politikken.

4.1.3 Gennemgår status for efterlevelse og disciplinære foranstaltninger i forbindelse med politikovertrædelser som led i styringen af ISMS.

4.2 IT- og informationssikkerhedsteams

4.2.1 Implementerer tekniske sikkerhedsforanstaltninger til håndhævelse af denne politik, herunder:

4.2.2 Filtrering af indhold, malwarebeskyttelse, endepunktssikkerhed og værktøjer til netværksovervågning

4.2.3 Sikkerhedskonfigurationer for e-mail og løsninger til forebyggelse af datatab (DLP)

4.2.4 Bloklister og tilladelseslister for software, hardware og websteder

4.2.5 Vedligeholder en fortegnelse over godkendt og forbudt software, enheder og tjenester.

4.2.6 Undersøger mistanke om overtrædelser af AUP, indsamler digitale beviser og understøtter disciplinære eller retlige skridt, hvor det er relevant.

4.2.7 Samarbejder med HR og juridisk funktion om hændelseshåndtering, eskalering og rapporteringsforpligtelser.

[... 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 frekvens for gennemgang

9.1.1 Denne politik skal gennemgås:

9.1.1.1 Mindst én gang årligt

9.1.1.2 Efter væsentlige ændringer i teknologi eller infrastruktur

9.1.1.3 Efter hændelser eller revisionsresultater, der påviser mangler i håndhævelsen

9.1.1.4 Som reaktion på ændringer i gældende lovgivning eller kontrakter

9.2 Ejerskab og godkendelse

9.2.1 CISO eller den udpegede ISMS-manager er ansvarlig for gennemgangsprocessen.

9.2.2 Opdateringer skal godkendes af direktionen og kommunikeres i hele organisationen.

9.2.3 Anerkendelse af opdaterede vilkår skal indhentes på ny ved genudstedelse af politikken.

9.3 Dokumentstyring

9.3.1 Politikken skal indeholde følgende metadata og versionsoplysninger:

9.3.1.1 Titel, ID og klassifikationsniveau

9.3.1.2 Politikejer og dokumentansvarlig

9.3.1.3 Ændringshistorik og begrundelse for opdateringer

9.3.1.4 Datoer for gennemgang og næste planlagte opdatering

9.3.1.5 Referencer til distributions- og anerkendelseslog

9.3.2 Masterkopien skal opbevares i ISMS' dokumentrepository under versionsstyring.

10. Relaterede politikker og sammenhænge

10.1 Denne politik skal fortolkes i sammenhæng med følgende:

10.1.1 P1 – Informationssikkerhedspolitik: Fastlægger de grundlæggende forventninger til adfærd og den øverste ledelses forpligtelse til acceptabel brug.

10.1.2 P4 – Politik for adgangskontrol: Definerer tilladelser og rettigheder knyttet til brugere, systemer og dataadgang og håndhæver dermed direkte grænserne for acceptabel brug.

10.1.3 P6 – Risikostyringspolitik: Omhandler adfærdsrelaterede risici og understøtter overvågnings- og behandlingsaktiviteter forbundet med brugerudløste trusler.

10.1.4 P7 – Politik for onboarding og fratrædelse: Sikrer, at vilkår for acceptabel brug anerkendes ved tiltrædelse og tilbagekaldes ved fratrædelse.

10.1.5 P9 – Politik for fjernarbejde: Udvider bestemmelserne om acceptabel brug til fjernarbejde og hybride arbejdsmiljøer.

10.2 Disse relaterede politikker udgør tilsammen en lagdelt forsvarsmodel for adfærdsmæssig, teknisk og kontraktuel styring.

11. Referencestandarder og rammeværk

11.1 Denne politik for acceptabel brug (AUP) er afstemt med internationalt anerkendte standarder og retlige rammer for at sikre håndhævelige, reviderbare og risikobaserede adfærdskontroller på tværs af al brug af digitale og fysiske informationssystemer.

11.2 ISO/IEC 27001:2022

11.2.1 Kontrol 5.10 – Acceptabel brug af information og andre tilknyttede aktiver: Denne politik opfylder direkte kravet om at definere, kommunikere og håndhæve regler for korrekt brug af IT-ressourcer.

11.2.2 Bilag A, kontrol 6.1 – Ansvar for informationssikkerhed: Tildeler tydeligt ansvar for brugeradfærd og tilsyn med efterlevelse.

11.2.3 Bilag A, kontrol 6.2 – Awareness, uddannelse og træning i informationssikkerhed: Integrerede trænings- og anerkendelsesprocesser er en del af håndhævelsen af AUP.

11.2.4 Bilag A, kontrol 8.1 – Brugerendepunkter og 8.12 – Forebyggelse af datatab: Omhandler acceptabel adfærd på brugerenheder og regulerer aktiviteter, der kan føre til dataeksponering eller datalækage.

11.3 NIST SP 800-53 Rev.5:

11.3.1 AC-19 (adgangskontrol for mobile enheder) og AC-20 (brug af eksterne informationssystemer): Denne politik fastlægger brugerforpligtelser og begrænsninger for BYOD og tredjepartsadgang til systemer.

11.3.2 PL-4 (adfærdsregler): Indeholder detaljerede krav til acceptabel brug, som er i overensstemmelse med denne politik.

11.3.3 AT-2 (awareness-træning i sikkerhed): Understøttes gennem brugertræning og dokumenteret anerkendelse af politikken.

11.3.4 AU-2 (revisionshændelser) og AU-12 (generering af revisionsspor): Håndhævelsen bygger på overvågning af brugerhandlinger og alarmering ved overtrædelser.

11.4 EU GDPR (2016/679):

11.4.1 Artikel 5, stk. 1, litra f: Kræver sikkerhed og integritet for personoplysninger; denne politik reducerer risici, der opstår gennem menneskelig adfærd og uautoriseret brug.

11.4.2 Artikel 32: Kræver tekniske og organisatoriske foranstaltninger, såsom adfærdskontroller og brugsbegrænsninger, til beskyttelse af personoplysninger.

11.4.3 Betragtning 39: Fremhæver behovet for alene at sikre nødvendig adgang til og lovlig brug af data for autoriserede personer.

11.5 EU NIS2-direktivet (2022/2555):

11.5.1 Artikel 21, stk. 2, litra a-d: Kræver operationelle politikker og oplæring i sikker brug af systemer, hvilket denne AUP leverer ved at definere adfærd, overvågning og håndhævelsesprocesser.

11.6 EU DORA (2022/2554):

11.6.1 Artikel 5: Denne politik understøtter rammerne for styring af IKT-risici ved at definere regler for samspillet mellem menneske og system og minimere eksponering for cyberrisici baseret på adfærd.

11.7 COBIT 2019:

11.7.1 APO07 – Managed Human Resources: Håndhæver brugeransvar og awareness på tværs af hele medarbejderlivscyklussen.

11.7.2 BAI05 – Managed Organizational Change: Indlejrer styring af acceptabel brug i ændringsprocesser, der påvirker brugeradfærd.

11.7.3 DSS05 – Managed Security Services: Understøtter overvågning af brugeraktiviteter, adfærdsbaserede alarmer og automatiserede responsmekanismer.

11.7.4 MEA01 – Monitor, Evaluate, and Assess Performance and Conformance: Politikken fastlægger målepunkter og mekanismer til validering af brugernes efterlevelse af de adfærdsmæssige forventninger.