					Indsæt navnet på den registrerede juridiske enhed her							
Dokumentnummer: P03S					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**

I overensstemmelse med standarder og regler

Standard/regulering	Klausul/artikel	Kommentar
ISO/IEC 27001:2022	Klausul 5	Relevant for politikkens overordnede omfang og implementering
ISO/IEC 27002:2022	5.10, 5.11, 5	Vejledning om krav og kontroller for acceptabel brug
NIST SP 800-53 Rev.5	AC-19, AC-20, AT-2	Omfatter brug af systemer og enheder, overvågning og brugeruddannelse
EU GDPR	Artikel 5(1)(f), 32	Integritet og fortrolighed af data samt sikkerhedsforanstaltninger
EU NIS2	Artikel 21(2)(b)	Kræver passende sikkerhedspolitikker og regler for acceptabel brug
EU DORA	Artikel 9	Politik for styring af IKT-risici, kontroller og håndhævelse
COBIT 2019	DSS05, BAI08	Sikkerhedstjenester og vidensstyring

1. Formål

1.1. Denne politik fastlægger kravene til acceptabel, ansvarlig og sikker brug af virksomhedens systemer, enheder, internetadgang, e-mail, cloudtjenester og eventuelle personligt ejede enheder, der anvendes til forretningsformål.

1.2. Politikken skal sikre, at alle forstår deres forpligtelser ved brug af organisationens it-ressourcer, herunder beskyttelse af dataintegritet, privatliv og driftskontinuitet.

1.3. Denne politik understøtter efterlevelse af ISO/IEC 27001:2022 ved at fastsætte klare krav til brugeradfærd i overensstemmelse med juridiske, kontraktuelle og regulatoriske krav.

2. Omfang

2.1. Denne politik gælder for alle personer, der tilgår, administrerer eller på anden måde interagerer med virksomhedens systemer eller data, herunder:

2.1.1. Medarbejdere og konsulenter

2.1.2. Midlertidigt ansatte og praktikanter

2.1.3. Eksterne it-tjenesteudbydere

2.2. Politikken omfatter:

2.2.1. Virksomhedsejede computere, telefoner og tablets

2.2.2. Personligt ejede enheder, der er godkendt til erhvervsmæssig brug (BYOD)

2.2.3. Virksomhedens netværk, cloudplatforme og softwaretjenester

2.2.4. Internetadgang, e-mailsystemer, delt lagring og forretningsapplikationer

2.3. Denne politik gælder i alle arbejdsmiljøer – på virksomhedens lokationer, ved fjernarbejde og i hybride arbejdssituationer – samt i hele arbejdstiden.

3. Mål

3.1. Fastlægge, hvad der udgør acceptabel og uacceptabel brug af it-systemer.

3.1.1. Reducere sikkerhedsrisici som følge af misbrug, uautoriseret adgang eller introduktion af malware.

3.1.2. Beskytte forretningsdata, kundeoplysninger og virksomhedens omdømme.

3.1.3. Fastlægge ensartede regler og sikre ansvarlighed for alle brugere.

3.1.4. Understøtte overvågning og efterlevelse med henblik på tidlig identifikation af overtrædelser og iværksættelse af korrigerende handlinger.

4. Roller og ansvar

4.1. Direktør

4.1.1. Godkender denne politik og er ansvarlig for at sikre, at de nødvendige ressourcer og beføjelser er til rådighed for håndhævelse.

4.1.2. Gennemgår og godkender eventuelle undtagelser fra denne politik.

4.2. It-ansvarlig eller ekstern it-leverandør

4.2.1. Vedligeholder fortegnelser over godkendt software og hardware.

4.2.2. Konfigurerer enheder, så reglerne for acceptabel brug håndhæves, eksempelvis gennem indholdsfiltrering og logning af adgang.

4.2.3. Overvåger brugen med henblik på mulige overtrædelser og undersøger hændelser.

4.2.4. Sikrer, at personlige enheder (BYOD), der anvendes erhvervsmæssigt, er godkendt og tilstrækkeligt sikret.

[... 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. Årlig gennemgang

9.1.1. Denne politik skal gennemgås årligt af den it-ansvarlige med endelig godkendelse fra direktøren for at sikre, at den fortsat er tilpasset teknologiske brugsmønstre, nye risici og compliancekrav.

9.2. Udløsende forhold for mellemliggende gennemgang

9.2.1. Gennemgange skal også gennemføres som reaktion på:

9.2.2. Nye systemer eller teknologier, f.eks. en ny cloudtjeneste eller endpoint-platform

9.2.3. Væsentlige overtrædelser af politikken

9.2.4. Opdateret lovgivning eller kontraktvilkår, der påvirker brugen af it

9.3. Dokumentation af ændringer

9.3.1. Alle opdateringer skal registreres i en versionslog, som indeholder:

9.3.1.1. Versionsnummer

9.3.1.2. Dato for gennemgang

9.3.1.3. Resumé af ændringer

9.3.1.4. Godkendende instans

9.4. Kommunikation af politikken

9.4.1. Reviderede versioner af denne politik skal distribueres til alle berørte brugere. Medarbejdere skal bekræfte modtagelse og forståelse som led i deres forpligtelser vedrørende sikkerhedsbevidsthed.

10. Relaterede politikker og sammenhænge

10.1. Denne politik skal ses i sammenhæng med en række andre SME-politikker for at sikre en dækkende regulering af sikkerhedsansvar:

10.1.1. P4S – Politik for adgangsstyring: Fastlægger teknisk og proceduremæssig håndhævelse af tilladt brug og begrænsninger i kontoadgang.

10.1.2. P8S – Politik for awareness og træning i informationssikkerhed: Omfatter brugeruddannelse om grænser for acceptabel brug og rapporteringsforpligtelser.

10.1.3. P9S – Politik for fjernarbejde: Regulerer brugen af virksomhedens systemer uden for virksomhedens lokationer eller på hjemmearbejdspladser.

10.1.4. P17S – Politik for databeskyttelse og privatliv: Håndhæver regler for behandling af personoplysninger, som overlapper med overvågning af acceptabel brug og BYOD.

10.1.5. P30S – Politik for hændelseshåndtering: Fastlægger procedurer for undersøgelse af og reaktion på misbrug eller overtrædelser af reglerne for acceptabel brug.

11. Referencestandarder og rammeværker

11.1. ISO/IEC 27001

11.1.1. Kontrol 5.10 – Kræver, at organisationer definerer og håndhæver acceptabel brug af informationsaktiver.

11.2. ISO/IEC 27002

11.2.1. Kontrol 5.10 – Indeholder retningslinjer for acceptabel brug af systemer, herunder tilladt og forbudt adfærd.

11.3. NIST SP 800-53 Rev.5

11.3.1. AC-19 – Omhandler styring af systembrug, herunder personligt ejede enheder.

11.3.2. AC-20 – Kræver autorisation og overvågning af eksterne systemer.

11.3.3. AT-2 – Fremhæver oplæring af brugere i praksis for acceptabel brug.

11.4. EU GDPR

11.4.1. Artikel 5(1)(f) – Kræver integritet og fortrolighed for personoplysninger, som kan kompromitteres ved brugermisbrug.

11.4.2. Artikel 32 – Kræver implementering af tekniske og organisatoriske foranstaltninger til sikring af systemer og data.

11.5. EU NIS2

11.5.1. Artikel 21(2)(b) – Kræver passende sikkerhedspolitikker, herunder regler for acceptabel brug, for at begrænse cybertrusler.

11.6. EU DORA

11.6.1. Artikel 9 – Kræver politikker for styring af IKT-risici, som omfatter brugskontroller og håndhævelsesmekanismer.

11.7. COBIT 2019

11.7.1. DSS05 – Styring af sikkerhedstjenester: Fremhæver kontrol med brugeradfærd baseret på politikker.

11.7.2. BAI08 – Styring af viden: Omhandler kendskab til politiske forpligtelser og oplæring i acceptabel brug.