					Indsæt navnet på den registrerede juridiske enhed her							
Dokumentnummer: P19S					Dokumenttitel: **Politik for sårbarheds- og patchstyring**							
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	Kapitel 8	
ISO/IEC 27002:2022	Kontrol 8.8, 8.9	
NIST SP 800-53 Rev.5	RA-5, SI-2, CM-2	
EU NIS2	Artikel 21(2)(d), 21(2)(e)	
EU DORA	Artikel 8(1), 10(2)	
COBIT 2019	DSS05.02, APO12	
GDPR	Artikel 32(1)(b)	

1. Formål

1.1 Denne politik fastlægger, hvordan organisationen identificerer, vurderer og afhjælper sårbarheder på tværs af systemer, applikationer og infrastruktur.

1.2 Formålet er at reducere cybersikkerhedsrisici ved at sikre rettidig patching og risikobaserede afhjælpningspraksisser, der er egnede til små og mellemstore virksomheder (SMV'er).

1.3 Denne politik understøtter efterlevelse i forbindelse med certificering efter ISO/IEC 27001:2022 og bidrager til opfyldelse af regulatoriske forpligtelser efter GDPR, NIS2 og DORA ved at stille krav om proaktiv styring af tekniske sårbarheder.

1.4 Organisationen anerkender, at systemer uden opdaterede sikkerhedsrettelser udgør en væsentlig trussel mod informationssikkerheden og skal håndteres systematisk og uden unødig forsinkelse.

2. Omfang

2.1 Denne politik gælder for:

2.1.1 Alle servere, stationære computere, bærbare computere, mobile enheder, netværksudstyr og cloudhostede platforme, som anvendes af organisationen

2.1.2 Alle operativsystemer, tredjepartssoftware, plugins og applikationer, der anvendes i forretningsdriften

2.1.3 Internt it-personale eller eksterne tjenesteudbydere med ansvar for systemvedligeholdelse, opdateringer eller overvågning

2.1.4 Enhver specialudviklet kode eller indlejret software, som vedligeholdes af organisationen eller på dens vegne

2.2 Politikken omfatter både infrastruktur, der forvaltes direkte af organisationen, og systemer, der administreres af kontraherede leverandører eller cloudtjenesteudbydere.

3. Mål

3.1 At identificere og vurdere kendte sårbarheder på tværs af alle it-aktiver rettidigt og ensartet

3.2 At anvende patches og softwareopdateringer på baggrund af alvorlighed og risiko for organisationens drift eller personoplysninger

3.3 At forebygge udnyttelse af tekniske svagheder, der kan medføre driftsafbrydelser, brud på persondatasikkerheden eller manglende overholdelse af lovkrav

3.4 At opretholde nøjagtige registreringer af anvendte patches, udeståender og undtagelser for at sikre revisionsberedskab

3.5 At anvende værktøjer og processer, der er proportionale med organisationens størrelse og operationelle kompleksitet, uden at kompromittere effektiviteten

3.6 At understøtte juridisk og regulatorisk efterlevelse, herunder GDPR artikel 32 og ISO/IEC 27001 bilag A kontrol 8

4. Roller og ansvar

4.1 Direktør (GM)

4.1.1 Har det overordnede ansvar for at sikre, at aktiviteter vedrørende patching og sårbarhedsstyring håndhæves

4.1.2 Godkender risikoundtagelser, hvor patches ikke kan anvendes, og gennemgår tilhørende risikoreducerende foranstaltninger

4.1.3 Gennemgår statusrapporter for patching og sikrer, at der er tilstrækkelige ressourcer til at opfylde kravene til patching

4.2 It-supportleverandør / intern it-administrator

4.2.1 Overvåger systemer for sårbarheder og tilgængelige patches ved hjælp af leverandøradvarsler, trusselsvarslinger og notifikationer på operativsystemniveau

4.2.2 Anvender opdateringer til operativsystemer, firmware og applikationer inden for fastsatte tidsfrister

4.2.3 Vedligeholder en formel patchlog og dokumenterer uløste eller udskudte opdateringer

4.2.4 Gennemfører test og planlægning af kritiske opdateringer for at minimere driftsforstyrrelser

[... 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 mindst én gang årligt af direktøren med input fra it-leverandøren og databeskyttelseskoordinatoren

9.2 Udløsende forhold for gennemgang

9.2.1 Mellemliggende gennemgange skal gennemføres, hvis:

9.2.1.1 En væsentlig sårbarhed eller udnyttelse påvirker systemer inden for politikkens omfang

9.2.1.2 Der sker væsentlige ændringer i systemer eller software

9.2.1.3 En revision identificerer mangler i patchprocesserne

9.2.1.4 En hændelse eller et brud relateret til patching registreres

9.3 Versionsstyring af politikken

9.3.1 Alle opdateringer skal registreres i en versionslog med et resumé af ændringerne

9.3.2 Ændringer skal kommunikeres til berørt personale

9.3.3 Forældede versioner skal arkiveres med begrænset adgang

10. Relaterede politikker og sammenhænge

10.1 Denne politik understøtter og afhænger af flere andre SME-politikker:

10.1.1 P12S – Politik for aktivstyring: Identificerer systemejerskab og klassificering og sikrer, at alle aktiver, der kræver patching, er registreret og indgår i aktivfortegnelsen

10.1.2 P14S – Politik for opbevaring og sikker bortskaffelse af data: Sikrer, at systemer planlagt til udfasning opdateres sikkert eller slettes, hvilket reducerer eksponeringen for sårbarheder

10.1.3 P17S – Databeskyttelses- og privatlivspolitik: Prioriterer afhjælpning af sårbarheder for systemer, der behandler personoplysninger, for at overholde databeskyttelseslovgivningen

10.1.4 P22S – Politik for logning og overvågning: Understøtter identifikation af systemer uden opdaterede sikkerhedsrettelser eller mistænkelig aktivitet, der kan indikere udnyttelse af en sårbarhed

10.1.5 P30S – Politik for hændelseshåndtering: Fastlægger procedurer for håndtering af sårbarheder, der medfører sikkerhedshændelser, herunder eskalations- og rapporteringstrin

11. Referencestandarder og rammeværker

11.1 ISO/IEC 27001

11.1.1 Kapitel 8.1 – Kræver implementering af kontroller til håndtering af operationel risiko, herunder sårbarhedsstyring

11.2 ISO/IEC 27002

11.2.1 Kontrol 8.8 – Specificerer processer for scanning og afhjælpning af kendte svagheder i systemer

11.2.2 Kontrol 8.9 – Fremhæver sikker konfiguration, validering af patches og styring af konfigurationsændringer for at undgå ny eksponering under opdateringer

11.3 NIST SP 800-53 Rev.5

11.3.1 RA-5 – Kræver identifikation af sårbarheder og afhjælpning inden for fastsatte tidsfrister

11.3.2 SI-2 – Kræver hurtig anvendelse af patches og opdateringer på baggrund af alvorlighed

11.3.3 CM-2 – Regulerer systemers baselinekonfigurationer og dokumentation af opdateringer for at sikre ensartet beskyttelse

11.4 GDPR

11.4.1 Artikel 32(1)(b) – Kræver, at organisationer implementerer passende tekniske foranstaltninger, herunder patching, for at opretholde behandlingssikkerhed

11.5 NIS2-direktivet

11.5.1 Artikel 21(2)(d) – Kræver håndtering af sårbarheder gennem systematisk scanning og afhjælpning

11.5.2 Artikel 21(2)(e) – Forpligter til sikker konfiguration og patchstyring for at sikre IKT-robusthed

11.6 DORA

11.6.1 Artikel 8(1) – Kræver identifikation og afbødning af IKT-risici, herunder tekniske sårbarheder

11.6.2 Artikel 10(2) – Pålægger finansielle enheder at afhjælpe svagheder, der påvirker IKT-systemer og drift

11.7 COBIT 2019

11.7.1 DSS05.02 – Kræver håndtering af kendte tekniske sårbarheder for at opretholde sikker drift

11.7.2 APO12.01 – Tilpasser risikostyring med proaktiv overvågning og korrigering af systemsvagheder