					Voer hier de naam van de geregistreerde rechtspersoon in						
Documentnummer: P19S					Documenttitel: **Beleid inzake beheer van kwetsbaarheden en patches**						
Versie: 1.0		Ingangsdatum: 01.01.2025			Documenteigenaar:						
X	Beleid		Standaard		Procedure		Formulier		Register		Overig

Revisiegeschiedenis				
Revisienummer	**Revisiedatum**	**Wijzigingen**	**Beoordeeld door**	**Proceseigenaar**

Goedkeuringen			
Naam	**Functie**	**Datum**	**Handtekening**

Afgestemd op normen en regelgeving

Norm/regelgeving	Clausule/artikel	Opmerking
ISO/IEC 27001:2022	Clausule 8	
ISO/IEC 27002:2022	Beheersmaatregelen 8.8, 8.9	
NIST SP 800-53 Rev.5	RA-5, SI-2, CM-2	
EU NIS2	Artikelen 21(2)(d), 21(2)(e)	
EU DORA	Artikelen 8(1), 10(2)	
COBIT 2019	DSS05.02, APO12	
AVG	Artikel 32(1)(b)	

1. Doel

1.1 Dit beleid bepaalt hoe de organisatie kwetsbaarheden in systemen, toepassingen en infrastructuur identificeert, beoordeelt en mitigeert.

1.2 Het doel is het cyberbeveiligingsrisico te verlagen door tijdige patching en risicogebaseerde herstelmaatregelen af te dwingen die passend zijn voor het midden- en kleinbedrijf (mkb).

1.3 Dit beleid ondersteunt naleving in het kader van ISO/IEC 27001:2022-certificering en draagt bij aan het voldoen aan wettelijke verplichtingen op grond van de AVG, NIS2 en DORA door proactief beheer van technische kwetsbaarheden te vereisen.

1.4 De organisatie erkent dat niet-gepatchte systemen een aanzienlijk risico vormen voor de informatiebeveiliging en systematisch en zonder onnodige vertraging moeten worden aangepakt.

2. Reikwijdte

2.1 Dit beleid is van toepassing op:

2.1.1 Alle servers, desktops, laptops, mobiele apparaten, netwerkapparatuur en cloudgehoste platforms die door de organisatie worden gebruikt

2.1.2 Alle besturingssystemen, software van derden, plug-ins en toepassingen die in de bedrijfsvoering worden gebruikt

2.1.3 Interne IT-medewerkers of externe dienstverleners die verantwoordelijk zijn voor systeemonderhoud, updates of monitoring

2.1.4 Alle maatwerkcode of embedded software die door of namens de organisatie wordt onderhouden

2.2 Dit beleid omvat zowel infrastructuur die rechtstreeks door de organisatie wordt beheerd als systemen die worden beheerd door gecontracteerde leveranciers of hostingproviders.

3. Doelstellingen

3.1 Bekende kwetsbaarheden in alle IT-middelen tijdig en consistent identificeren en beoordelen

3.2 Patches en software-updates toepassen op basis van ernst en risico voor de bedrijfsvoering of persoonsgegevens

3.3 Exploitatie van technische kwetsbaarheden voorkomen die kunnen leiden tot dienstuitval, een datalek of niet-naleving van wet- en regelgeving

3.4 Nauwkeurige registraties bijhouden van toegepaste patches, openstaande bevindingen en uitzonderingen om auditgereed te zijn

3.5 Hulpmiddelen en processen gebruiken die passen bij de omvang en operationele complexiteit van de organisatie, zonder afbreuk te doen aan de doeltreffendheid

3.6 Juridische en regelgevende naleving ondersteunen, waaronder AVG artikel 32 en ISO Annex A beheersmaatregel 8

4. Rollen en verantwoordelijkheden

4.1 Algemeen directeur (GM)

4.1.1 Draagt de eindverantwoordelijkheid om ervoor te zorgen dat activiteiten voor patch- en kwetsbaarhedenbeheer worden afgedwongen

4.1.2 Keurt risicouitzonderingen goed wanneer patches niet kunnen worden toegepast en beoordeelt de bijbehorende mitigerende maatregelen

4.1.3 Beoordeelt statusrapportages over patches en ziet erop toe dat voldoende middelen beschikbaar zijn om aan patchverplichtingen te voldoen

4.2 IT-supportdienstverlener / interne IT-beheerder

4.2.1 Bewaakt systemen op kwetsbaarheden en beschikbare patches met behulp van leveranciersmeldingen, dreigingsadviezen en meldingen op besturingssysteemniveau

4.2.2 Past updates voor besturingssystemen, firmware en toepassingen toe binnen de vastgestelde termijnen

4.2.3 Houdt een formeel patchlogboek bij en documenteert niet-opgeloste of uitgestelde updates

4.2.4 Voert tests uit en plant kritieke updates zodanig dat operationele verstoring tot een minimum wordt beperkt

[... Secties 4.3–8 zijn niet opgenomen in dit voorbeeld. Koop het volledige document voor toegang tot de volledige inhoud. ...]

9. Eisen voor beoordeling en actualisering

9.1 Jaarlijkse beoordeling

9.1.1 Dit beleid moet ten minste jaarlijks worden beoordeeld door de algemeen directeur, met inbreng van de IT-dienstverlener en de privacycoördinator

9.2 Triggers voor beoordeling

9.2.1 Tussentijdse beoordelingen moeten plaatsvinden indien:

9.2.1.1 Een ernstige kwetsbaarheid of exploit gevolgen heeft voor systemen binnen de reikwijdte

9.2.1.2 Significante wijzigingen in systemen of software plaatsvinden

9.2.1.3 Een audit tekortkomingen in patchprocessen identificeert

9.2.1.4 Een patchgerelateerd incident of datalek wordt geregistreerd

9.3 Versiebeheer van beleid

9.3.1 Alle updates moeten worden vastgelegd in een versielogboek met een samenvatting van wijzigingen

9.3.2 Wijzigingen moeten worden gecommuniceerd aan betrokken medewerkers

9.3.3 Verouderde versies moeten met beperkte toegang worden gearchiveerd

10. Gerelateerde beleidslijnen en samenhang

10.1 Dit beleid ondersteunt en is afhankelijk van verschillende andere mkb-beleidslijnen:

10.1.1 P12S – Beleid inzake beheer van bedrijfsmiddelen: identificeert systeemeigenaarschap en classificatie, zodat alle activa die patching vereisen zijn verantwoord en opgenomen in de inventaris

10.1.2 P14S – Beleid inzake gegevensbewaring en afvoer: zorgt ervoor dat systemen die voor buitengebruikstelling zijn gepland veilig worden bijgewerkt of gewist, waardoor de blootstelling aan kwetsbaarheden afneemt

10.1.3 P17S – Beleid inzake gegevensbescherming en privacy: geeft prioriteit aan herstelmaatregelen voor kwetsbaarheden in systemen die persoonsgegevens verwerken om te voldoen aan privacywetgeving

10.1.4 P22S – Beleid inzake logging en monitoring: ondersteunt de detectie van niet-gepatchte systemen of verdachte gedragingen die erop kunnen wijzen dat een kwetsbaarheid wordt uitgebuit

10.1.5 P30S – Incidentresponsbeleid: definieert procedures voor het reageren op kwetsbaarheden die leiden tot beveiligingsincidenten, inclusief escalatie- en meldingsstappen

11. Referentienormen en -raamwerken

11.1 ISO/IEC 27001

11.1.1 Clausule 8.1 – Vereist de implementatie van beheersmaatregelen om operationele risico's aan te pakken, waaronder kwetsbaarhedenbeheer

11.2 ISO/IEC 27002

11.2.1 Beheersmaatregel 8.8 – Specificeert processen voor het scannen op en verhelpen van bekende kwetsbaarheden in systemen

11.2.2 Beheersmaatregel 8.9 – Benadrukt veilige configuratie, validatie van patches en wijzigingsbeheer om nieuwe blootstellingen tijdens updates te voorkomen

11.3 NIST SP 800-53 Rev.5

11.3.1 RA-5 – Vereist identificatie van kwetsbaarheden en remediatie binnen vastgestelde termijnen

11.3.2 SI-2 – Verplicht de tijdige toepassing van patches en updates op basis van ernst

11.3.3 CM-2 – Regelt baselineconfiguraties van systemen en documentatie van updates om consistente bescherming te waarborgen

11.4 AVG

11.4.1 Artikel 32(1)(b) – Vereist dat organisaties passende technische maatregelen implementeren, waaronder patching, om de beveiliging van de verwerking te waarborgen

11.5 EU NIS2-richtlijn

11.5.1 Artikel 21(2)(d) – Vereist de afhandeling van kwetsbaarheden door systematische scans en remediatie

11.5.2 Artikel 21(2)(e) – Verplicht veilige configuratie en patchbeheer om ICT-veerkracht te waarborgen

11.6 EU DORA

11.6.1 Artikel 8(1) – Vereist detectie en mitigatie van ICT-risico's, waaronder technische kwetsbaarheden

11.6.2 Artikel 10(2) – Verplicht financiële entiteiten om kwetsbaarheden die ICT-systemen en -operaties raken te verhelpen

11.7 COBIT 2019

11.7.1 DSS05.02 – Vereist behandeling van bekende technische kwetsbaarheden om veilige bedrijfsvoering te handhaven

11.7.2 APO12.01 – Stemt risicobeheer af op proactieve monitoring en correctie van systeemkwetsbaarheden