					Voer hier de naam van de geregistreerde rechtspersoon in						
Documentnummer: P19					Documenttitel: **Beleid inzake kwetsbaarheden- en patchmanagement**						
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	Systematische behandeling van technische kwetsbaarheden; blijvende doeltreffendheid van beveiligingsmaatregelen.
ISO/IEC 27002:2022	Beheersmaatregelen 8.8, 8.9, 5	Implementatierichtlijnen voor patchmanagement, kwetsbaarheidsscans, software-integriteit, veilige configuratie en bedrijfsmiddelenregisters.
NIST SP 800-53 Rev.5	RA-5, SI-2, CM-2, CM-6	Frequente scans, herstel van bevindingen en configuratiebeheer worden afgedwongen.
EU AVG	Artikel 32, overweging 49	Technische maatregelen voor tijdige patching, behandeling van kwetsbaarheden en continue beveiliging.
EU NIS2	Artikel 21(2)(d)	Detectie, respons en mitigatie van kwetsbaarheden ter ondersteuning van een hoog niveau van cyberbeveiligingshygiëne.
EU DORA	Artikelen 8, 10(2)(f)	Tijdig herstel van ICT-kwetsbaarheden; continue dreigingsgestuurde beoordelingen.
COBIT 2019	DSS05.02, DSS01.03, MEA	Technische kwetsbaarheden scannen/volgen/mitigeren; toezicht houden op misbruik; doeltreffendheid beoordelen, inclusief patchstatus.

1. Doel

1.1 Dit beleid definieert de verplichte eisen van de organisatie voor het identificeren, classificeren, verhelpen en monitoren van technische kwetsbaarheden en softwarefouten in alle informatiesystemen en bedrijfsmiddelen binnen de reikwijdte van het managementsysteem voor informatiebeveiliging (ISMS).

1.2 Het waarborgt dat alle bekende kwetsbaarheden op een risicogebaseerde en tijdige wijze worden beoordeeld en aangepakt door middel van gecoördineerde patching, configuratieaanpassingen of compenserende beheersmaatregelen, in overeenstemming met bedrijfsbehoeften en complianceverplichtingen.

1.3 Dit beleid ondersteunt naleving van ISO/IEC 27001 Annex A, beheersmaatregel 8.8, en de richtlijnen van ISO/IEC 27002, en geeft invulling aan wettelijke en toezichthoudende vereisten op grond van artikel 8 van DORA, artikel 21 van NIS2, artikel 32 van de AVG en de DSS- en APO-domeinen van COBIT 2019.

2. Reikwijdte

2.1 Dit beleid is van toepassing op alle informatiesystemen, bedrijfsmiddelen en omgevingen die gegevens opslaan, verwerken of verzenden en die onder de governance van het ISMS vallen, waaronder:

2.1.1 besturingssystemen, toepassingen, netwerkapparatuur, firmware, cloudplatformen, API's en software van derden.

2.1.2 systemen in ontwikkel-, test-, acceptatie-, productie-, back-up- en disasterrecoveryomgevingen.

2.1.3 endpoints, servers, IoT-apparaten, virtualisatie-infrastructuur en containers.

2.2 Dit beleid is bindend voor:

2.2.1 interne medewerkers: IT-beheerders, systeemengineers, applicatieontwikkelaars, beveiligingsanalisten en infrastructuurteams.

2.2.2 externe partijen: contractanten en externe dienstverleners, managed service providers (MSP's), softwareleveranciers en systeemintegratoren met technische verantwoordelijkheden voor bedrijfsmiddelen binnen de reikwijdte.

2.3 Het beleid omvat de volledige levenscyclus van kwetsbaarheden- en patchmanagement, waaronder:

2.3.1 scannen en detectie

2.3.2 risicoclassificatie en prioritering

2.3.3 verwerving, testen, uitrol en rollback van patches

2.3.4 afhandeling van uitzonderingen en planning van compenserende beheersmaatregelen

2.3.5 logging, rapportage en audittrail

3. Doelstellingen

3.1 Waarborgen dat alle bekende kwetsbaarheden worden geïdentificeerd, beoordeeld en verholpen op een wijze die de risicoblootstelling minimaliseert en aansluit bij operationele prioriteiten.

3.2 Consistente, organisatiebrede processen vaststellen voor kwetsbaarheidsscans, ernstclassificatie (bijvoorbeeld CVSS) en patchmanagement, inclusief noodafhandeling en rollbackplanning.

3.3 Veilig configuratiebeheer mogelijk maken door afstemming op hardening-baselines, wijzigingsbeheerpraktijken en actuele dreigingsinformatie.

3.4 Meetbare naleving realiseren van wettelijke en normatieve beheersmaatregelen met betrekking tot systeemintegriteit, patchhygiëne en tijdig herstel van fouten.

3.5 Verantwoordelijkheden en accountability over rollen heen vastleggen voor de volledige levenscyclus van kwetsbaarhedenbeheer, zodat alle stakeholders handelen binnen vastgestelde SLA's en rapporteerbare beheersingsindicatoren.

3.6 Auditgereedheid ondersteunen en de weerbaarheid tegen opkomende dreigingen vergroten, waaronder zero-day-kwetsbaarheden, actieve exploitketens en openbaarmakingen met hoge impact door leveranciers.

4. Rollen en verantwoordelijkheden

4.1 Chief Information Security Officer (CISO)

4.1.1 Is eigenaar van dit beleid en borgt de integratie ervan binnen het ISMS.

4.1.2 Stelt de risicobereidheid van de organisatie vast en borgt afstemming op wettelijke, toezichthoudende en controlverwachtingen.

4.2 Verantwoordelijke kwetsbaarhedenbeheer / manager Security Operations

4.2.1 Houdt toezicht op de end-to-end-uitvoering van kwetsbaarheden- en patchmanagement.

4.2.2 Coördineert scanschema's, prioriteringsmodellen en termijnen voor herstelmaatregelen.

4.2.3 Beheert het kwetsbaarhedenregister en werkt samen aan de beoordeling van compenserende beheersmaatregelen.

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

9. Eisen voor herziening en actualisatie

9.1 Dit beleid moet ten minste jaarlijks worden herzien, of wanneer zich een van de volgende situaties voordoet:

9.1.1 significante wijzigingen in wet- en regelgeving (bijvoorbeeld wijzigingen in DORA of NIS2)

9.1.2 wijzigingen in kaders voor prioritering van kwetsbaarheden (bijvoorbeeld updates van CVSS)

9.1.3 majeure wijzigingen in de IT-omgeving (bijvoorbeeld cloudmigratie of een ingrijpende wijziging van EDR)

9.1.4 beveiligingsincidenten met hoge impact of externe adviezen die aanscherping van het beleid vereisen

9.2 Herzieningen moeten worden uitgevoerd door de CISO in samenwerking met Security Operations, risicomanagement en de leiding van de infrastructuurfunctie.

9.3 Actualisaties van beleid moeten:

9.3.1 worden gedocumenteerd in het ISMS-documentenregister

9.3.2 worden beoordeeld en goedgekeurd door het topmanagement

9.3.3 worden gecommuniceerd aan alle relevante stakeholders, waaronder externe verwerkers

9.4 Historische versies moeten veilig worden bewaard ten behoeve van audits en accountability.

10. Gerelateerd beleid en samenhang

10.1 P1 - Informatiebeveiligingsbeleid. Legt de overkoepelende verplichting vast om systemen en gegevens te beschermen, waaronder proactief beheer van kwetsbaarheden en het waarborgen van software-integriteit.

10.2 P5 - Wijzigingsbeheerbeleid. Stuurt alle patchuitrol en configuratieaanpassingen aan en vereist documentatie, testen, goedkeuring en rollbackprocedures die de processen voor het verhelpen van kwetsbaarheden ondersteunen.

10.3 P6 - Beleid inzake risicobeheer. Ondersteunt de classificatie en behandeling van niet-verholpen kwetsbaarheden via gestructureerde risicobeoordelingen, impactanalyses en procedures voor acceptatie van restrisico.

10.4 P12 - Beleid inzake beheer van bedrijfsmiddelen. Borgt dat systemen nauwkeurig worden geïnventariseerd en geclassificeerd, zodat consistente kwetsbaarheidsscans, toewijzing van eigenaarschap en patchdekking gedurende de gehele levenscyclus mogelijk zijn.

10.5 P22 - Logging- en monitoringbeleid. Definieert vereisten voor gebeurtenisdetectie en het vastleggen van een audittrail. Dit beleid ondersteunt zichtbaarheid op patchactiviteiten, ongeautoriseerde wijzigingen en exploitpogingen gericht op bekende kwetsbaarheden.

10.6 P30 - Incidentresponsbeleid (P30). Specificeert escalatieprotocollen en indammingsstrategieën voor uitgebuite kwetsbaarheden, onderzoeken naar incidenten en corrigerende maatregelen die in lijn zijn met de beheersmaatregelen van dit beleid.

11. Referentienormen en -raamwerken

11.1 ISO/IEC 27001: Clausule 8.1 - operationele planning en beheersing: vereist systematische behandeling van technische kwetsbaarheden om de blijvende doeltreffendheid van beveiligingsmaatregelen te waarborgen.

11.2 ISO/IEC 27002:2022 - Beheersmaatregelen 8.8, 8.9, 5: biedt implementatierichtlijnen voor patchmanagement, kwetsbaarheidsscans, software-integriteit en integratie met veilige configuratie en bedrijfsmiddelenregisters.

11.3 NIST SP 800-53 Rev.5: RA-5 - monitoring en scanning van kwetsbaarheden: vereist frequente scans en het volgen van herstelmaatregelen. SI-2 - herstel van fouten: vereist snelle beoordeling en mitigatie van fouten met beschikbare patches of andere maatregelen. CM-2 / CM-6 - baselineconfiguraties en beheersmaatregelen voor configuratiebeheer: vormt de basis voor veilige systeemconfiguraties gekoppeld aan de afdwinging van patches.

11.4 EU AVG (2016/679): Artikel 32 - beveiliging van de verwerking: vereist de implementatie van passende technische maatregelen, zoals tijdige patching en behandeling van kwetsbaarheden, om de vertrouwelijkheid en veerkracht van systemen te waarborgen. Overweging 49: moedigt organisaties aan preventieve beheersmaatregelen tegen bekende dreigingen te implementeren ter ondersteuning van beveiliging en continuïteit.

11.5 EU NIS2-richtlijn (2022/2555): Artikel 21(2)(d): verplicht essentiële en belangrijke entiteiten om systeemkwetsbaarheden te detecteren, erop te reageren en deze te mitigeren, en een hoog niveau van cyberbeveiligingshygiëne te handhaven.

11.6 EU DORA (2022/2554): Artikel 8 - ICT-risicobeheer: vereist identificatie en tijdig herstel van kwetsbaarheden in informatie- en communicatietechnologie die in financiële systemen worden gebruikt. Artikel 10(2)(f): benadrukt continue dreigingsgestuurde kwetsbaarheidsbeoordelingen en patching als onderdeel van operationele weerbaarheid.

11.7 COBIT 2019: DSS05.02 - beveiligingskwetsbaarheden beheren: stuurt organisaties aan om bekende technische kwetsbaarheden te scannen, volgen en mitigeren. DSS01.03 - infrastructuur monitoren: borgt dat systemen worden bewaakt op signalen van misbruik of zwakte. MEA03 - naleving monitoren, evalueren en beoordelen: vereist regelmatige audits van de doeltreffendheid van beheersmaatregelen, inclusief patchstatus en afhandeling van uitzonderingen.