					Ange namnet på den registrerade juridiska personen här							
Dokumentnummer: P19					Dokumenttitel: **Policy för sårbarhets- och patchhantering**							
Version: 1.0		Ikraftträdandedatum: 01.01.2025			Dokumentägare:							
X	Policy		Standard		Rutin		Formulär		Register		Övrigt	

Revisionshistorik				
Revisionsnummer	**Revisionsdatum**	**Ändringar**	**Granskad av**	**Processägare**

Godkännanden			
Namn	**Titel**	**Datum**	**Underskrift**

Ansluten till standarder och regelverk

Standard/regelverk	Klausul/artikel	Kommentar
ISO/IEC 27001:2022	Klausul 8	Systematisk hantering av tekniska sårbarheter samt fortlöpande effektivitet i säkerhetskontroller.
ISO/IEC 27002:2022	Kontroller 8.8, 8.9, 5	Vägledning för patchhantering, sårbarhetsskanning, programvaruintegritet, säker konfiguration och tillgångsförteckningar.
NIST SP 800-53 Rev.5	RA-5, SI-2, CM-2, CM-6	Frekvent skanning, åtgärdande av brister och konfigurationshantering ska tillämpas.
EU:s GDPR	Artikel 32, skäl 49	Tekniska åtgärder för skyndsam patchning, hantering av sårbarheter och upprätthållande av säkerhet.
EU:s NIS2-direktiv	Artikel 21(2)(d)	Detektering, respons och riskreducering av sårbarheter för god cyberhygien.
EU:s DORA-förordning	Artiklarna 8, 10(2)(f)	Skyndsamt åtgärdande av IKT-sårbarheter samt kontinuerliga hotstyrda bedömningar.
COBIT 2019	DSS05.02, DSS01.03, MEA	Skanna, följa upp och riskreducera tekniska svagheter, övervaka tecken på exploatering samt granska effektivitet inklusive patchstatus.

1. Syfte

1.1 Denna policy fastställer organisationens obligatoriska krav för att identifiera, klassificera, åtgärda och övervaka tekniska sårbarheter och programvarubrist i alla informationssystem och tillgångar inom ISMS omfattning.

1.2 Policyn säkerställer att alla kända sårbarheter bedöms och hanteras riskbaserat och inom rätt tid genom samordnad patchning, konfigurationsändringar eller kompenserande kontroller, i linje med verksamhetens behov och krav på regelefterlevnad.

1.3 Denna policy stödjer efterlevnad av ISO/IEC 27001 bilaga A, kontroll 8.8, och vägledningen i ISO/IEC 27002 samt adresserar regulatoriska krav enligt artikel 8 i DORA, artikel 21 i NIS2, artikel 32 i GDPR samt DSS- och APO-domänerna i COBIT 2019.

2. Omfattning

2.1 Denna policy gäller för alla informationssystem, tillgångar och miljöer som lagrar, behandlar eller överför data som omfattas av ISMS-styrning, inklusive:

2.1.1 Operativsystem, applikationer, nätverksenheter, firmware, molnplattformar, API:er och programvara från tredje part.

2.1.2 System i utvecklings-, test-, produktions-, säkerhetskopierings- och katastrofåterställningsmiljöer.

2.1.3 Slutpunkter, servrar, IoT-enheter, virtualiseringsinfrastruktur och containrar.

2.2 Policyn är bindande för:

2.2.1 Intern personal: IT-administratörer, systemingenjörer, applikationsutvecklare, säkerhetsanalytiker och infrastrukturteam.

2.2.2 Externa parter: entreprenörer och tredjepartstjänsteleverantörer, leverantörer av hanterade tjänster (MSP:er), programvaruleverantörer och integratörer med tekniskt ansvar för tillgångar inom omfattningen.

2.3 Policyn omfattar hela livscykeln för sårbarhets- och patchhantering, inklusive:

2.3.1 Skanning och identifiering

2.3.2 Riskklassificering och prioritering

2.3.3 Inhämtning, testning, driftsättning och återställning av patchar

2.3.4 Undantagshantering och planering av kompenserande kontroller

2.3.5 Loggning, rapportering och spårbarhet för revision

3. Mål

3.1 Säkerställa att alla kända sårbarheter identifieras, bedöms och åtgärdas på ett sätt som minimerar riskexponeringen och är anpassat till verksamhetens operativa prioriteringar.

3.2 Etablera konsekventa och organisationsövergripande processer för sårbarhetsskanning, klassificering av allvarlighetsgrad (t.ex. CVSS) och patchhantering, inklusive akut hantering och planering för återställning.

3.3 Möjliggöra säker konfigurationshantering genom anpassning till härdningsbaslinjer, ändringshanteringsprocesser och hotinformation i realtid.

3.4 Säkerställa mätbar efterlevnad av regulatoriska krav och standardbaserade kontroller kopplade till systemintegritet, patchhygien och skyndsamt åtgärdande av brister.

3.5 Fastställa ansvar och ansvarsskyldighet mellan roller för hela livscykeln för sårbarhetshantering, så att alla intressenter agerar inom definierade SLA:er och rapporterbara kontrollmätetal.

3.6 Stärka revisionsberedskapen och förbättra motståndskraften mot framväxande hot, inklusive nolldagssårbarheter, aktiva exploitkedjor och offentliga säkerhetsmeddelanden från större leverantörer.

4. Roller och ansvar

4.1 Informationssäkerhetschef (CISO)

4.1.1 Är policyägare och säkerställer att policyn integreras i ISMS.

4.1.2 Fastställer organisationens risktolerans och säkerställer anpassning till regulatoriska krav och förväntade kontroller.

4.2 Ansvarig för sårbarhetshantering / chef för säkerhetsdrift

4.2.1 Ansvarar för den samlade hanteringen av sårbarhets- och patchhantering från början till slut.

4.2.2 Samordnar skanningsscheman, prioriteringsmodeller och tidsplaner för åtgärder.

4.2.3 Upprätthåller sårbarhetsregistret och medverkar i utvärderingen av kompenserande kontroller.

[... Avsnitt 4.3–8 ingår inte i denna förhandsvisning. Köp det fullständiga dokumentet för att få tillgång till hela innehållet. ...]

9. Krav för granskning och uppdatering

9.1 Denna policy ska granskas minst årligen eller vid:

9.1.1 Betydande regulatoriska uppdateringar (t.ex. ändringar i DORA eller NIS2)

9.1.2 Förändringar i ramverk för prioritering av sårbarheter (t.ex. uppdateringar av CVSS)

9.1.3 Större förändringar i IT-miljön (t.ex. migrering till molnmiljö eller större förändring av EDR)

9.1.4 Allvarliga incidenter eller externa säkerhetsmeddelanden som kräver förstärkning av policyn

9.2 Granskningar ska genomföras av CISO i samverkan med säkerhetsdrift, riskhantering och infrastrukturledning.

9.3 Uppdateringar av policyn ska:

9.3.1 Dokumenteras i ISMS dokumentregister för dokumentstyrning

9.3.2 Granskas och godkännas av verkställande ledning

9.3.3 Kommuniceras till alla berörda intressenter, inklusive tredjepartsbiträden

9.4 Historiska versioner ska bevaras på ett säkert sätt för revision och ansvarsskyldighet.

10. Relaterade policyer och kopplingar

10.1 P1 - Informationssäkerhetspolicy. Fastställer det övergripande åtagandet att skydda system och data, vilket omfattar proaktiv hantering av sårbarheter och säkerställande av programvaruintegritet.

10.2 P5 - Ändringshanteringspolicy. Styr all driftsättning av patchar och konfigurationsändringar och kräver dokumentation, testning, godkännande och återställningsrutiner som kompletterar processerna för åtgärdande av sårbarheter.

10.3 P6 - Riskhanteringspolicy. Stödjer klassificering och behandling av sårbarheter som inte har åtgärdats genom strukturerade riskbedömningar, konsekvensanalyser och processer för acceptans av kvarstående risk.

10.4 P12 - Policy för tillgångshantering. Säkerställer att system förtecknas och klassificeras korrekt, vilket möjliggör konsekvent sårbarhetsskanning, tilldelning av ägarskap och patchtäckning över hela livscykeln.

10.5 P22 - Loggnings- och övervakningspolicy. Definierar krav för händelseidentifiering och skapande av revisionsspår. Policyn stödjer spårbarhet i patchaktiviteter, otillåtna ändringar och exploateringsförsök riktade mot kända sårbarheter.

10.6 P30 - Policy för incidenthantering. Anger eskaleringsprotokoll och strategier för begränsning av exploaterade sårbarheter, utredningar av överträdelser och korrigerande åtgärder i linje med denna policys kontroller.

11. Referensstandarder och ramverk

11.1 ISO/IEC 27001: Klausul 8.1 - Operativ planering och styrning: Kräver systematisk hantering av tekniska sårbarheter för att säkerställa fortlöpande effektivitet i säkerhetskontroller.

11.2 ISO/IEC 27002:2022 - Kontroller 8.8, 8.9, 5: Ger vägledning för patchhantering, sårbarhetsskanning, programvaruintegritet och integration med säker konfiguration och tillgångsförteckningar.

11.3 NIST SP 800-53 Rev.5: RA-5 - Övervakning och skanning av sårbarheter: Kräver frekvent skanning och uppföljning av åtgärder. SI-2 - Åtgärdande av brister: Kräver skyndsam bedömning och riskreducering av brister med tillgängliga patchar eller andra åtgärder. CM-2 / CM-6 - Baskonfigurationer och kontroller för konfigurationshantering: Etablerar grunden för säkra systemkonfigurationer kopplade till tillämpning av patchning.

11.4 EU:s GDPR (2016/679): Artikel 32 - Säkerhet i behandlingen: Kräver genomförande av lämpliga tekniska åtgärder, såsom skyndsam patchning och hantering av sårbarheter, för att säkerställa konfidentialitet och systemens motståndskraft. Skäl 49: Uppmuntrar organisationer att införa förebyggande kontroller mot kända hot för att stödja säkerhet och kontinuitet.

11.5 EU:s NIS2-direktiv (2022/2555): Artikel 21(2)(d): Förpliktar väsentliga och viktiga aktörer att identifiera, hantera och riskreducera systemens sårbarheter samt upprätthålla en hög nivå av cyberhygien.

11.6 EU:s DORA-förordning (2022/2554): Artikel 8 - IKT-riskhantering: Kräver identifiering och skyndsamt åtgärdande av sårbarheter i informations- och kommunikationsteknik som används i finansiella system. Artikel 10(2)(f): Betonar kontinuerliga hotstyrda bedömningar av sårbarheter och patchning som en del av operativ motståndskraft.

11.7 COBIT 2019: DSS05.02 - Hantera säkerhetssårbarheter: Anger att organisationer ska skanna, följa upp och riskreducera kända tekniska svagheter. DSS01.03 - Övervaka infrastruktur: Säkerställer att system övervakas avseende tecken på exploatering eller svagheter. MEA03 - Övervaka, utvärdera och bedöma regelefterlevnad: Kräver regelbunden revision av kontrolleffektivitet, inklusive patchstatus och undantagshantering.