					Ange namnet på den registrerade juridiska personen här							
Dokumentnummer: P19S					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**

Anpassning till standarder och regelverk

Standard/regelverk	Klausul/artikel	Kommentar
ISO/IEC 27001:2022	Klausul 8	
ISO/IEC 27002:2022	Kontroller 8.8, 8.9	
NIST SP 800-53 Rev.5	RA-5, SI-2, CM-2	
EU:s NIS2-direktiv	Artikel 21.2 d, 21.2 e	
EU:s DORA-förordning	Artikel 8.1, 10.2	
COBIT 2019	DSS05.02, APO12	
EU:s GDPR	Artikel 32.1 b	

1. Syfte

1.1 Denna policy fastställer hur organisationen identifierar, utvärderar och reducerar risker kopplade till sårbarheter i system, applikationer och infrastruktur.

1.2 Syftet är att minska cybersäkerhetsrisker genom att kräva patchning i rätt tid och riskbaserade åtgärder anpassade för små och medelstora företag (SME).

1.3 Policyn stödjer efterlevnad inför certifiering enligt ISO/IEC 27001:2022 och bidrar till att uppfylla regulatoriska skyldigheter enligt GDPR, NIS2 och DORA genom att kräva proaktiv hantering av tekniska sårbarheter.

1.4 Organisationen erkänner att opatchade system utgör ett betydande hot mot informationssäkerheten och ska hanteras systematiskt och utan dröjsmål.

2. Omfattning

2.1 Denna policy gäller för:

2.1.1 Alla servrar, stationära datorer, bärbara datorer, mobila enheter, nätverksutrustning och molnplattformar som används av organisationen

2.1.2 Alla operativsystem, programvara från tredje part, insticksprogram och applikationer som används i verksamheten

2.1.3 Intern IT-personal eller externa IT-tjänsteleverantörer med ansvar för systemunderhåll, uppdateringar eller övervakning

2.1.4 All egenutvecklad kod eller inbyggd programvara som underhålls av organisationen eller för dess räkning

2.2 Policyn omfattar både infrastruktur som förvaltas direkt av organisationen och system som administreras av upphandlade leverantörer eller driftleverantörer.

3. Mål

3.1 Identifiera och bedöma kända sårbarheter i alla IT-tillgångar på ett snabbt och enhetligt sätt

3.2 Tillämpa patchar och programuppdateringar utifrån allvarlighetsgrad och risk för verksamheten eller personuppgifter

3.3 Förhindra utnyttjande av tekniska säkerhetssvagheter som kan leda till driftavbrott, personuppgiftsincidenter eller bristande efterlevnad av rättsliga krav

3.4 Upprätthålla korrekta uppgifter om tillämpade patchar, kvarstående brister och undantag för att säkerställa revisionsberedskap

3.5 Använda verktyg och processer som är anpassade till organisationens storlek och operativa komplexitet utan att kompromissa med effektiviteten

3.6 Stödja efterlevnad av rättsliga och regulatoriska krav, inklusive artikel 32 i GDPR och bilaga A, kontroll 8 i ISO

4. Roller och ansvar

4.1 Verkställande direktör (VD)

4.1.1 Har det övergripande ansvaret för att aktiviteter för patchhantering och sårbarhetshantering genomförs

4.1.2 Godkänner riskundantag när patchar inte kan tillämpas och granskar tillhörande riskreducerande åtgärder

4.1.3 Granskar statusrapporter för patchning och säkerställer att resurser finns tillgängliga för att uppfylla kraven på patchning

4.2 IT-supportleverantör / intern IT-administratör

4.2.1 Övervakar system avseende sårbarheter och tillgängliga patchar med hjälp av leverantörsaviseringar, hotinformation och notifieringar på operativsystemnivå

4.2.2 Tillämpar uppdateringar av operativsystem, firmware och applikationer inom fastställda tidsramar

4.2.3 Upprätthåller en formell patchlogg och dokumenterar olösta eller uppskjutna uppdateringar

4.2.4 Genomför testning och schemaläggning av kritiska uppdateringar för att minimera påverkan på verksamheten

[... 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 Årlig granskning

9.1.1 Denna policy ska granskas minst en gång per år av den verkställande direktören, med underlag från IT-leverantören och integritetssamordnaren

9.2 Utlösande händelser för granskning

9.2.1 Mellanliggande granskningar ska genomföras om:

9.2.1.1 En allvarlig sårbarhet eller ett angrepp genom utnyttjande påverkar system inom omfattningen

9.2.1.2 Betydande ändringar i system eller programvara genomförs

9.2.1.3 En revision identifierar kontrollbrister i patchhanteringsprocesserna

9.2.1.4 En patchrelaterad incident eller överträdelse registreras

9.3 Policy för versionshantering

9.3.1 Alla uppdateringar ska registreras i en versionslogg med ändringssammanfattning

9.3.2 Ändringar ska kommuniceras till berörd personal

9.3.3 Inaktuella versioner ska arkiveras med begränsad åtkomst

10. Relaterade policyer och kopplingar

10.1 Denna policy stödjer och är beroende av flera andra SME-policyer:

10.1.1 P12S – Policy för tillgångshantering: Identifierar systemägarskap och klassificering samt säkerställer att alla tillgångar som kräver patchning finns redovisade i tillgångsförteckning och inventering

10.1.2 P14S – Policy för datalagring och bortskaffande: Säkerställer att system som är planerade för avveckling uppdateras säkert eller raderas, vilket minskar exponering för sårbarheter

10.1.3 P17S – Policy för dataskydd och integritet: Prioriterar åtgärdande av sårbarheter i system som behandlar personuppgifter för att uppfylla krav i integritetslagstiftningen

10.1.4 P22S – Policy för loggning och övervakning: Stödjer upptäckt av opatchade system eller misstänkt beteende som kan indikera att en sårbarhet utnyttjas

10.1.5 P30S – Policy för incidenthantering: Fastställer rutiner för att hantera sårbarheter som leder till säkerhetsincidenter, inklusive eskalering och rapporteringssteg

11. Referensstandarder och ramverk

11.1 ISO/IEC 27001

11.1.1 Klausul 8.1 – Kräver införande av kontroller för att hantera operativ risk, inklusive sårbarhetshantering

11.2 ISO/IEC 27002

11.2.1 Kontroll 8.8 – Anger processer för att skanna efter och åtgärda kända säkerhetssvagheter i system

11.2.2 Kontroll 8.9 – Betonar säker konfiguration, validering av patchar och ändringsstyrning för att undvika ny exponering vid uppdateringar

11.3 NIST SP 800-53 Rev.5

11.3.1 RA-5 – Kräver identifiering av sårbarheter och åtgärdande inom fastställda tidsramar

11.3.2 SI-2 – Kräver skyndsam tillämpning av patchar och uppdateringar baserat på allvarlighetsgrad

11.3.3 CM-2 – Reglerar systemens baslinjekonfigurationer och dokumentation av uppdateringar för att säkerställa ett enhetligt skydd

11.4 EU:s GDPR

11.4.1 Artikel 32.1 b – Kräver att organisationer inför lämpliga tekniska åtgärder, inklusive patchning, för att upprätthålla säker behandling

11.5 EU:s NIS2-direktiv

11.5.1 Artikel 21.2 d – Kräver hantering av sårbarheter genom systematisk skanning och åtgärdande

11.5.2 Artikel 21.2 e – Kräver säker konfiguration och patchhantering för att säkerställa IKT-resiliens

11.6 EU:s DORA-förordning

11.6.1 Artikel 8.1 – Kräver identifiering och riskreducering av IKT-risker, inklusive tekniska sårbarheter

11.6.2 Artikel 10.2 – Kräver att finansiella entiteter åtgärdar säkerhetssvagheter som påverkar IKT-system och verksamhet

11.7 COBIT 2019

11.7.1 DSS05.02 – Kräver hantering av kända tekniska sårbarheter för att upprätthålla säker drift

11.7.2 APO12.01 – Samordnar riskhantering med proaktiv övervakning och korrigering av säkerhetssvagheter i system