					Ange namnet på den registrerade juridiska personen här							
Dokumentnummer: P40					Dokumenttitel: **Policy för säkerhetstestning och red team-övningar**							
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/förordning	Klausul/artikel	Kommentar
ISO/IEC 27001:2022	9.1, 9.2, 9.3	
ISO/IEC 27002:2022	5.7, 5.36, 8.8, 8.29, 8.30, 8.1	
NIST SP 800-53 Rev.5	CA-2, CA-7, CA-8, RA-5	
Dataskyddsförordningen (GDPR)	Art. 32(1)(d)	
NIS2-direktivet	Art. 21(2)(f)	
DORA-förordningen	Art. 25–27	
COBIT 2019	DSS05.07, MEA02.01, MEA02.03	

1. Syfte

1 Fastställa ett strukturerat program för regelbunden säkerhetstestning av organisationens nätverk, system och applikationer, inklusive sårbarhetsbedömningar, penetrationstester och red team-övningar, för att uppfylla kraven i artikel 21.2 f i NIS2 avseende bedömning av cybersäkerhetsåtgärdernas effektivitet.

1.1 Säkerställa att svagheter i tekniska och organisatoriska åtgärder identifieras proaktivt och åtgärdas genom kontrollerad testning, så att organisationens säkerhetsläge fortlöpande förbättras.

2. Omfattning

2 Denna policy omfattar alla kritiska informationssystem, applikationer och stödjande infrastrukturer som ägs eller drivs av organisationen. Den omfattar även fysisk säkerhetstestning av lokaler där detta är relevant för cybersäkerheten, till exempel social manipulation eller fysiska penetrationstester, om detta ingår i red team-övningens omfattning.

2.1 Policyn gäller för interna säkerhetsteam, eventuellt kontrakterade externa leverantörer av säkerhetstestning samt relevanta systemägare och applikationsägare. Alla testaktiviteter ska vara godkända och följa rutinerna i detta dokument för att undvika oavsiktliga störningar.

3. Mål

3 Verifiera effektiviteten i införda cybersäkerhetskontroller, tekniska, operativa och organisatoriska, genom periodisk testning och simuleringar i linje med NIS2:s krav på effektivitetsmätning.

3.1 Identifiera sårbarheter eller brister som ordinarie operativa processer kan missa, inklusive zero-days eller felkonfigurationer, under realistiska angreppsscenarier (red teaming) innan hotaktörer utnyttjar dem.

3.2 Ge ledningen beslutsunderlag och genomförbara rekommendationer genom rapportering av testresultat, så att välgrundade beslut om riskbehandling och kontinuerlig förbättring av informationssäkerhetsprogrammet kan fattas.

4. Roller och ansvar

4 Samordnare för säkerhetstestning (STC): Utses av informationssäkerhetschefen (CISO) och ansvarar för att planera och övervaka all säkerhetstestning. Säkerställer att tester avgränsas, godkänns samt att resultat rapporteras och följs upp.

4.1 Internt säkerhetsteam (Blue Team): Medverkar i tester, exempelvis genom att tillhandahålla information för avgränsning och övervaka system under tester. Vid red team-övningar ska Blue Team respondera på simulerade angrepp, och deras detekterings- och responsförmåga ska utvärderas.

4.2 Red Team/penetrationstestare: Kan utgöras av ett internt offensivt säkerhetsteam eller externa konsulter. Genomför tester enligt överenskomna spelregler, dokumenterar alla identifierade sårbarheter och angreppsvägar samt upprätthåller sekretess.

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

9. Övervakning och revision

9 STC ska upprätthålla en kalender och logg över alla genomförda aktiviteter för säkerhetstestning. Denna logg ska omfatta datum, omfattning, vem som utförde testet samt en sammanfattning av resultaten. Den ska granskas för att säkerställa efterlevnad av det fastställda schemat, till exempel att inget kritiskt system lämnas otestat längre än den årliga cykeln.

9.1 Framdriften i åtgärdandet av testresultat ska övervakas och rapporteras månadsvis. Utestående iakttagelser med hög allvarlighetsgrad ska granskas i ledningsmöten till dess att de har stängts.

9.2 Internrevision eller en oberoende revisor ska årligen granska programmet för säkerhetstestning för att verifiera att tester godkänns, genomförs och rapporteras korrekt, att kritiska iakttagelser har hanterats och att programmet uppfyller regulatoriska förväntningar. Exempelvis kan revisorer kontrollera att ett penetrationstest genomfördes innan en ny onlinetjänst togs i produktion, om detta krävs. Eventuella avvikelser ska leda till riskbehandlingsplaner för korrigerande åtgärder.

10. Granskning och underhåll

10 Denna policy och den övergripande testplanen ska granskas minst en gång per år. Granskningen ska beakta förändringar i hotlandskapet, till exempel framväxten av nya angreppstekniker som vår nuvarande testning kanske inte täcker, och anpassa omfattning eller frekvens därefter.

10.1 Efter varje större cybersäkerhetsincident eller överträdelse ska denna policy ses över för att avgöra om ytterligare eller tätare testning hade kunnat förhindra eller upptäcka problemet. Policyn ska därefter uppdateras för att införliva sådana justeringar, exempelvis genom att lägga till ett nytt scenario i red team-övningar baserat på observerade angreppsmönster.

10.2 Uppdateringar av denna policy ska godkännas av informationssäkerhetschefen (CISO) och noteras av styrelsen. All relevant personal ska informeras om ändringar, och externa testpartner ska underrättas om någon ändring påverkar villkoren för deras uppdrag.

11. Relaterade policyer och kopplingar

11.1 P06 – Riskhanteringspolicy. Resultat från testning ligger till grund för riskbedömning och riskbehandling.

11.2 P22 – Loggnings- och övervakningspolicy. Validerar detekteringstäckning under övningar.

11.3 P24 – Policy för säker utveckling. Integrerar testresultat i SDLC-kontroller.

11.4 P25 – Policy för applikationssäkerhetskrav. Säkerställer att krav återspeglar lärdomar från testning.

11.5 P30 – Policy för incidenthantering. Red team-scenarier förfinar åtgärdsplaner och respons.

11.6 P31 – Policy för bevisinsamling och forensik. Säkerställer att artefakter samlas in på ett säkert sätt under testning.

11.7 P32 – Policy för verksamhetskontinuitet och katastrofåterställning. Övningar verifierar resiliens under angrepp.

11.8 P33 – Policy för revision och regelefterlevnadsövervakning. Säkerställer oberoende tillsyn av testprogrammets effektivitet.

12. Referenser

12.1 NIS2-direktivet (EU 2022/2555), artikel 21.2 f (policyer och rutiner för att bedöma effektiviteten i åtgärder för hantering av cybersäkerhetsrisker)

12.2 Kommissionens genomförandeförordning (EU) 2024/2690, bilaga avsnitt 7 (krav för övervakning, testning och utvärdering av cybersäkerhetsåtgärdernas effektivitet)

12.3 ENISA Technical Guidance (2025) – bilaga om säkerhetstestning och revision (vägledning för genomförande av cybersäkerhetsövningar och tekniska tester)

12.4 ISO/IEC 27001:2022 / ISO/IEC 27002:2022

12.5 Bästa branschpraxis: OWASP Testing Guide, NIST SP 800-115 (Technical Guide to Security Testing), CBEST/GREEN Team (ramverk för red team-övningar inom finanssektorn som referens)