					Indsæt navnet på den registrerede juridiske enhed her							
Dokumentnummer: P40					Dokumenttitel: **Politik for sikkerhedstest og red team-øvelser**							
Version: 1.0		Ikrafttrædelsesdato: 01.01.2025			Dokumentejer:							
X	Politik		Standard		Procedure		Formular		Register		Andet	

Revisionshistorik				
Revisionsnummer	**Revisionsdato**	**Ændringer**	**Gennemgået af**	**Procesejer**

Godkendelser			
Navn	**Stilling**	**Dato**	**Underskrift**

Tilpasset relevante standarder og regler

Standard/forordning	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	
EU GDPR	Art. 32(1)(d)	
EU NIS2	Art. 21(2)(f)	
EU DORA	Art. 25–27	
COBIT 2019	DSS05.07, MEA02.01, MEA02.03	

1. Formål

1 Definere et struktureret program for regelmæssig sikkerhedstest af organisationens netværk, systemer og applikationer, herunder sårbarhedsvurderinger, penetrationstest og red team-øvelser, for at opfylde kravene i NIS2 artikel 21(2)(f) om vurdering af effektiviteten af cybersikkerhedsforanstaltninger.

1.1 Sikre, at svagheder i tekniske og organisatoriske kontroller identificeres og afhjælpes proaktivt gennem kontrolleret testning og dermed løbende forbedrer organisationens sikkerhedsniveau.

2. Omfang

2 Denne politik omfatter alle kritiske informationssystemer, applikationer og understøttende infrastrukturer, som ejes eller drives af organisationen. Den omfatter også test af fysisk sikring af faciliteter, når det er relevant for cybersikkerheden, f.eks. social engineering eller fysiske penetrationstest, hvis dette indgår i red team-omfanget.

2.1 Politikken gælder for interne informationssikkerhedsteams, eventuelle engagerede eksterne sikkerhedstestleverandører og relevante system- og applikationsansvarlige. Alle testaktiviteter skal være autoriserede og gennemføres i overensstemmelse med procedurerne i denne politik for at undgå utilsigtede driftsforstyrrelser.

3. Mål

3 Verificere effektiviteten af implementerede cybersikkerhedskontroller, tekniske, driftsmæssige og organisatoriske, gennem periodisk testning og simuleringer i overensstemmelse med NIS2-kravet om måling af effektivitet.

3.1 Identificere sårbarheder eller mangler, som de almindelige driftsprocesser muligvis ikke opdager, herunder zero-day-forhold eller konfigurationsfejl, under realistiske angrebsscenarier (red teaming), før trusselsaktører udnytter dem.

3.2 Give ledelsen sikkerhed for kontrolniveauet og handlingsorienterede anbefalinger gennem rapportering af testresultater og dermed understøtte velinformerede beslutninger om risikobehandling og løbende forbedring af sikkerhedsprogrammet.

4. Roller og ansvar

4 Sikkerhedstestkoordinator (STC): Udpeges af Chief Information Security Officer (CISO) og er ansvarlig for planlægning og tilsyn med alle sikkerhedstestaktiviteter. Sikrer, at testaktiviteter afgrænses og autoriseres, samt at resultater rapporteres og følges op.

4.1 Internt informationssikkerhedsteam (Blue Team): Deltager i testforløb, f.eks. ved at levere oplysninger til afgrænsning af omfang og overvåge systemer under test. Ved red team-øvelser reagerer Blue Team på simulerede angreb, og teamets detektions- og responskapacitet evalueres.

4.2 Red Team/penetrationstestere: Kan være et internt offensivt sikkerhedsteam eller eksterne konsulenter. Udfører test i henhold til aftalte regler for gennemførelse, dokumenterer alle identificerede sårbarheder og angrebsveje samt opretholder fortrolighed.

[... Afsnit 4.3–8 er ikke inkluderet i denne forhåndsvisning. Køb det fulde dokument for at få adgang til det komplette indhold. ...]

9. Overvågning og revision

9 STC skal føre en kalender og log over alle gennemførte sikkerhedstestaktiviteter. Denne log skal omfatte dato, omfang, hvem der udførte testen, og et resumé af resultaterne. Den skal gennemgås for at sikre overholdelse af den fastlagte plan, f.eks. at intet kritisk system forbliver utestet ud over den årlige cyklus.

9.1 Fremdriften i afhjælpning af testkonstateringer skal overvåges og rapporteres månedligt. Åbne forhold med høj alvorlighed skal gennemgås på ledelsesmøder, indtil de er lukket.

9.2 Intern revision eller en uafhængig revisor skal årligt gennemgå programmet for sikkerhedstest for at verificere, at test er korrekt autoriseret, gennemført og rapporteret, at kritiske konstateringer er håndteret, og at programmet opfylder regulatoriske forventninger, f.eks. at der er udført penetrationstest før lancering af en ny onlinetjeneste, hvis dette kræves. Eventuelle afvigelser skal medføre korrigerende handlinger og behandlingsplaner.

10. Gennemgang og vedligeholdelse

10 Denne politik og den overordnede testplan skal gennemgås mindst én gang årligt. Gennemgangen skal tage højde for ændringer i trusselslandskabet, f.eks. fremkomsten af nye angrebsteknikker, som den nuværende testning ikke dækker, og tilpasse omfang eller hyppighed derefter.

10.1 Efter enhver større sikkerhedshændelse eller ethvert større brud skal denne politik genbesøges for at vurdere, om yderligere eller hyppigere test kunne have forebygget eller detekteret forholdet. Politikken skal derefter opdateres for at indarbejde sådanne justeringer, for eksempel ved at tilføje et nyt scenarie til red team-øvelser baseret på observerede angrebsmønstre.

10.2 Opdateringer til denne politik skal godkendes af CISO og noteres af bestyrelsen. Alt relevant personale skal informeres om ændringer, og eksterne testpartnere skal underrettes, hvis en ændring påvirker vilkårene for deres engagement.

11. Relaterede politikker og sammenhænge

11.1 P06 – Politik for risikostyring. Resultater fra test driver risikovurdering og risikobehandling.

11.2 P22 – Politik for logning og overvågning. Validerer detektionsdækning under øvelser.

11.3 P24 – Politik for sikker udvikling. Integrerer konstateringer fra test i kontroller i softwareudviklingslivscyklussen (SDLC).

11.4 P25 – Politik for krav til applikationssikkerhed. Sikrer, at krav afspejler læring fra test.

11.5 P30 – Politik for hændelseshåndtering. Red team-scenarier forfiner playbooks og respons.

11.6 P31 – Politik for indsamling af bevismateriale og digital efterforskning. Indsamler artefakter under test på sikker vis.

11.7 P32 – Politik for forretningskontinuitet og genopretning efter alvorlige hændelser. Øvelser verificerer robusthed under angreb.

11.8 P33 – Politik for revisions- og overvågningsprogram for efterlevelse. Uafhængigt tilsyn med effektiviteten af programmet for sikkerhedstest.

12. Referencer

12.1 NIS2-direktivet (EU 2022/2555), artikel 21(2), litra (f) (politikker og procedurer til vurdering af effektiviteten af foranstaltninger til styring af cybersikkerhedsrisici)

12.2 Kommissionens gennemførelsesforordning (EU) 2024/2690, bilag afsnit 7 (krav til overvågning, testning og evaluering af effektiviteten af cybersikkerhedsforanstaltninger)

12.3 ENISA Technical Guidance (2025) – bilag om sikkerhedstest og revision (retningslinjer for gennemførelse af cybersikkerhedsøvelser og tekniske test)

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

12.5 Branchens best practice: OWASP Testing Guide, NIST SP 800-115 (Technical Guide to Security Testing), CBEST/GREEN Team (rammeværker for red teaming i den finansielle sektor til reference)