					Voer hier de naam van de geregistreerde rechtspersoon in							
Documentnummer: P40					Documenttitel: **Beleid inzake beveiligingstesten en red teaming**							
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	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	
AVG	Art. 32(1)(d)	
EU NIS2	Art. 21(2)(f)	
EU DORA	Art. 25–27	
COBIT 2019	DSS05.07, MEA02.01, MEA02.03	

1. Doel

1. Een gestructureerd programma vaststellen voor periodieke beveiligingstesten van de netwerken, systemen en applicaties van de organisatie, waaronder kwetsbaarheidsbeoordelingen, penetratietesten en red-teamoefeningen, om te voldoen aan de vereisten van NIS2, artikel 21(2)(f), inzake het beoordelen van de doeltreffendheid van cyberbeveiligingsmaatregelen.

1.1 Waarborgen dat zwakke punten in technische en organisatorische maatregelen proactief worden geïdentificeerd en verholpen door middel van gecontroleerde tests, teneinde de risicohouding op het gebied van informatiebeveiliging van de organisatie voortdurend te verbeteren.

2. Reikwijdte

2. Dit beleid is van toepassing op alle kritieke informatiesystemen, applicaties en ondersteunende infrastructuur die eigendom zijn van of worden beheerd door de organisatie. Het omvat tevens fysieke beveiligingstesten van faciliteiten voor zover deze relevant zijn voor cyberbeveiliging, zoals social-engineeringtests of fysieke penetratietesten indien deze binnen de reikwijdte van het red team vallen.

2.1 Dit beleid is van toepassing op interne beveiligingsteams, gecontracteerde externe partijen voor beveiligingstesten en relevante systeem- en applicatie-eigenaren. Alle testactiviteiten moeten zijn geautoriseerd en worden uitgevoerd in overeenstemming met de in dit beleid vastgestelde procedures om onbedoelde verstoringen te voorkomen.

3. Doelstellingen

3. De doeltreffendheid verifiëren van geïmplementeerde cyberbeveiligingsmaatregelen, waaronder technische, operationele en organisatorische maatregelen, door middel van periodieke tests en simulaties, in lijn met de NIS2-verplichting om de doeltreffendheid te meten.

3.1 Kwetsbaarheden of hiaten identificeren die in reguliere operationele processen mogelijk onopgemerkt blijven, waaronder zero-days of configuratieproblemen, onder realistische aanvalsscenario's (red teaming), voordat dreigingsactoren deze misbruiken.

3.2 Het management voorzien van assurance en uitvoerbare aanbevelingen door te rapporteren over testbevindingen, zodat onderbouwde besluiten over risicobehandeling en continue verbetering van het beveiligingsprogramma mogelijk worden gemaakt.

4. Rollen en verantwoordelijkheden

4. Coördinator beveiligingstesten (STC): door de CISO aangewezen en verantwoordelijk voor het plannen van en het toezicht op alle beveiligingstestactiviteiten. Waarborgt dat tests zijn afgebakend en geautoriseerd en dat resultaten worden gerapporteerd en opgevolgd.

4.1 Intern beveiligingsteam (Blue Team): werkt mee aan tests, bijvoorbeeld door informatie te verstrekken voor de afbakening en systemen tijdens tests te monitoren. Bij red-teamoefeningen reageert het Blue Team op gesimuleerde aanvallen en worden de detectie- en responsvermogens beoordeeld.

4.2 Red team / penetratietesters: kunnen bestaan uit een intern offensief beveiligingsteam of externe consultants. Voeren tests uit volgens overeengekomen spelregels voor uitvoering, documenteren alle ontdekte kwetsbaarheden en aanvalspaden en waarborgen vertrouwelijkheid.

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

9. Monitoring en audit

9. De STC houdt een kalender en logboek bij van alle uitgevoerde beveiligingstestactiviteiten. Dit logboek moet ten minste de datum, reikwijdte, uitvoerende partij en een samenvatting van de resultaten bevatten. Het logboek wordt beoordeeld om te waarborgen dat het vereiste schema wordt nageleefd, bijvoorbeeld dat geen enkel kritisch systeem langer dan de jaarlijkse cyclus ongetest blijft.

9.1 De voortgang van remediatie van testbevindingen wordt maandelijks gemonitord en gerapporteerd. Openstaande kwesties met een hoge ernst worden in managementvergaderingen beoordeeld totdat zij zijn afgesloten.

9.2 De interne audit- en compliancefunctie of een onafhankelijke auditor beoordeelt het programma voor beveiligingstesten jaarlijks om te verifiëren dat tests naar behoren zijn geautoriseerd, uitgevoerd en gerapporteerd, dat kritieke bevindingen zijn opgepakt en dat het programma voldoet aan de verwachtingen van toezichthouders. Auditors kunnen bijvoorbeeld controleren of vóór de lancering van een nieuwe onlinedienst een penetratietest is uitgevoerd, indien dit vereist is. Afwijkingen leiden tot corrigerende maatregelen.

10. Herziening en onderhoud

10. Dit beleid en het overkoepelende testplan worden ten minste eenmaal per jaar beoordeeld. Bij deze beoordeling wordt rekening gehouden met veranderingen in het dreigingslandschap, zoals het ontstaan van nieuwe aanvalstechnieken die door de huidige tests nog niet worden afgedekt, waarna de reikwijdte of frequentie dienovereenkomstig wordt aangepast.

10.1 Na ieder groot cyberbeveiligingsincident of iedere inbreuk moet dit beleid opnieuw worden beoordeeld om vast te stellen of aanvullende of frequentere tests het probleem hadden kunnen voorkomen of detecteren. Het beleid wordt vervolgens bijgewerkt om dergelijke aanpassingen op te nemen, bijvoorbeeld door een nieuw scenario toe te voegen aan red-teamoefeningen op basis van waargenomen aanvalspatronen.

10.2 Wijzigingen in dit beleid moeten worden goedgekeurd door de CISO en ter kennis worden gebracht van de raad van bestuur. Alle relevante medewerkers worden geïnformeerd over wijzigingen, en externe testpartners worden op de hoogte gebracht indien een wijziging gevolgen heeft voor de voorwaarden van hun opdracht.

11. Gerelateerde beleidslijnen en samenhang

11.1 P06 – Beleid inzake risicobeheer. Uitkomsten van tests sturen risicobeoordeling en risicobehandeling.

11.2 P22 – Beleid voor logging en monitoring. Valideert de detectiedekking tijdens oefeningen.

11.3 P24 – Beleid inzake veilige ontwikkeling. Verwerkt testbevindingen in beheersmaatregelen binnen de Software Development Life Cycle (SDLC).

11.4 P25 – Beleid inzake vereisten voor applicatiebeveiliging. Waarborgt dat vereisten de leerpunten uit tests weerspiegelen.

11.5 P30 – Incidentresponsbeleid. Red-teamscenario's verfijnen draaiboeken en respons.

11.6 P31 – Beleid inzake bewijsverzameling en forensisch onderzoek. Verzamelt artefacten tijdens tests op veilige wijze.

11.7 P32 – Beleid voor bedrijfscontinuïteit en herstel na verstoringen. Oefeningen verifiëren weerbaarheid onder aanvalsomstandigheden.

11.8 P33 – Beleid voor audit en toezicht op naleving. Biedt onafhankelijk toezicht op de doeltreffendheid van het programma voor beveiligingstesten.

12. Referenties

12.1 NIS2-richtlijn (EU 2022/2555), artikel 21(2), punt (f) (beleidslijnen en procedures om de doeltreffendheid van maatregelen voor cyberbeveiligingsrisicobeheer te beoordelen)

12.2 Uitvoeringsverordening (EU) 2024/2690 van de Commissie, bijlage, sectie 7 (vereisten voor het monitoren, testen en evalueren van de doeltreffendheid van cyberbeveiligingsmaatregelen)

12.3 ENISA Technical Guidance (2025) – bijlage over beveiligingstesten en audit (richtsnoeren voor het uitvoeren van cyberbeveiligingsoefeningen en technische tests)

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

12.5 Best practices in de sector: OWASP Testing Guide, NIST SP 800-115 (Technical Guide to Security Testing), CBEST/GREEN Team (red-teamingraamwerken voor de financiële sector ter referentie)