					[Insert Registered Legal Entity Name Here]								
Document number: P40					Document Title: Security Testing and Red-Teaming Policy								
Version: 1.0		Effective Date: 01.01.2025			Document Owner:								
X	Policy		Standard		Procedure		Form		Register		Other		

Revision history				
Revision number	**Revision Date**	**Changes**	**Reviewed by**	**Process owner**

Approvals			
Name	**Title**	**Date**	**Signature**

Aligned with standards and regulations where applicable		
Standard/Regulation	**Clause/Article**	**Comment**
ISO/IEC 27001:2022	**9.1, 9.2, 9.3**	
ISO/IEC 27002:2022	**5.7, 5.36, 8.8, 8.29, 8.30, 8.31**	
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	

NOTE:
This policy bolsters Article 21(2)(f) compliance by formalizing how the organization assesses the effectiveness of its cybersecurity measures through continuous testing. NIS2 Article 21(2)(f) requires policies to assess cybersecurity risk-management measures' effectiveness. The Implementing Regulation and ENISA guidance reinforce this by detailing requirements for regular testing, monitoring, and evaluation of security controls. P40 introduces a structured program for vulnerability scanning, annual pen-testing of critical systems, and periodic red-team simulations. It ensures an all-hazards, proactive approach as envisioned by NIS2, where defenses are continuously validated against evolving threats. It also provides documentation and reporting mechanisms that will make it easier to demonstrate to regulators or auditors that the entity is testing and improving its cyber measures per NIS2's intent.

1. **Purpose**
   1.1 Define a structured program for regular security testing of the organization's networks, systems, and applications – including vulnerability assessments, penetration testing, and red team exercises – to satisfy NIS2 Article 21(2)(f) requirements on assessing the effectiveness of cybersecurity measures.
   1.2 Ensure that weaknesses in technical and organizational measures are proactively identified and remedied through controlled testing, thereby continually improving the organization's security posture.
2. **Scope**
   2.1 This policy covers all critical information systems, applications, and supporting infrastructure owned or operated by the organization. It also includes physical security testing of facilities as relevant to cybersecurity (e.g., social engineering or physical penetration tests, if in scope of red team).
   2.2 The policy applies to internal security teams, any contracted external security testing firms, and relevant system/application owners. All testing activities must be authorized and follow the procedures herein to avoid unintended disruptions.
3. **Objectives**
   3.1 Verify the effectiveness of implemented cybersecurity controls (technical, operational, and organizational) through periodic testing and simulations, in line with NIS2's mandate for measuring effectiveness
   3.2 Uncover vulnerabilities or gaps that regular operational processes might miss, including zero-day or configuration issues, under realistic attack scenarios (red teaming) before adversaries exploit them.
   3.3 Provide management with assurance and actionable recommendations by reporting on test findings, thereby enabling informed risk treatment decisions and continuous improvement of the security program.
4. **Roles and Responsibilities**
   4.1 **Security Testing Coordinator (STC)**: Appointed by the CISO, responsible for planning and overseeing all security testing activities. Ensures tests are scoped, authorized, and that results are reported and acted upon.
   4.2 **Internal Security Team (Blue Team):** Collaborates in tests (e.g., provides information for scoping, monitors systems during tests). For red team exercises, the Blue Team responds to simulated attacks, and their detection/response is evaluated.
   4.3 **Red Team / Penetration Testers**: Could be an internal offensive security team or external consultants. Execute tests under agreed rules of engagement, document all discovered vulnerabilities and exploitation paths, and maintain confidentiality.
   4.4 **System/Application Owners**: Provide necessary access or information to testers under STC's coordination, assist in remediation of identified issues, and ensure systems stability during and after tests.

[……

……

……

……

…….]

10. **Review and Maintenance**
   10.1 This policy and the overall testing plan will be reviewed at least once a year. The review will consider changes in the threat landscape (e.g., emergence of new attack techniques that our current testing might not cover) and adapt scopes or frequencies accordingly.

10.2 After any major cybersecurity incident or breach, this policy must be revisited to determine if additional or more frequent testing could have prevented or detected the issue. The policy will then be updated to incorporate such adjustments (for instance, adding a new scenario to red team exercises based on attack patterns observed).

10.3 Updates to this policy must be approved by the CISO and noted by the Management Board. All relevant personnel will be informed of changes, and external testing partners will be notified if any change affects their engagement terms.

11. Related Policies and Linkages

11.1 P06 – Risk Management Policy. Testing outputs drive risk evaluation and treatment.

11.2 P22 – Logging and Monitoring Policy. Validates detection coverage during exercises.

11.3 P24 – Secure Development Policy. Integrates test findings into SDLC controls.

11.4 P25 – Application Security Requirements Policy. Ensures requirements reflect test learnings.

11.5 P30 – Incident Response Policy. Red-team scenarios refine playbooks and response.

11.6 P31 – Evidence Collection and Forensics Policy. Collects artifacts during testing safely.

11.7 P32 – Business Continuity and Disaster Recovery Policy. Exercises verify resilience under attack.

11.8 P33 – Audit and Compliance Monitoring Policy. Independent oversight of testing program effectiveness.

12. References

12.1 NIS2 Directive (EU 2022/2555), Article 21(2), point (f) (policies and procedures to assess the effectiveness of cybersecurity risk-management measures)

12.2 Commission Implementing Regulation (EU) 2024/2690, Annex Section 7 (Requirements for monitoring, testing, and evaluating the effectiveness of cybersecurity measures)

12.3 ENISA Technical Guidance (2025) – Annex on security testing and audit (guidelines on conducting cybersecurity exercises and technical tests)

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

12.5 Industry Best Practices: OWASP Testing Guide, NIST SP 800-115 (Technical Guide to Security Testing), CBEST/GREEN Team (financial sector red teaming frameworks for reference)