					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

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, 8.1	
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. Purpose

1 Define a structured programme for regular security testing of the organisation's networks, systems, and applications, including vulnerability assessments, penetration testing, and red-teaming exercises, to meet the requirements of NIS2 Article 21(2)(f) for assessing the effectiveness of cybersecurity measures.

1.1 Ensure that weaknesses in technical and organisational measures are proactively identified and remediated through controlled testing, thereby continuously improving the organisation's security posture.

2. Scope

2 This policy applies to all critical information systems, applications, and supporting IT infrastructure owned or operated by the organisation. It also includes physical security testing of facilities where relevant to cybersecurity, such as social engineering or physical penetration testing where these fall within the scope of red teaming.

2.1 This policy applies to internal security teams, contracted external security testing providers, and relevant system and application owners. All testing activities must be authorised and carried out in accordance with the procedures defined herein to avoid unintended disruption.

3. Objectives

3 Verify the effectiveness of implemented cybersecurity controls, including technical, operational, and organisational controls, through periodic testing and simulations, in line with NIS2 requirements for measuring effectiveness.

3.1 Identify vulnerabilities or control gaps that routine operational processes may not detect, including zero-day vulnerabilities or configuration weaknesses, under realistic attack scenarios through red teaming before they can be exploited by adversaries.

3.2 Provide Top Management with assurance and actionable recommendations through reporting on test results, thereby enabling informed risk treatment decisions and continuous improvement of the security programme.

4. Roles and Responsibilities

4 Security Testing Coordinator (STC): Appointed by the CISO and responsible for planning and overseeing all security testing activities. Ensures testing is appropriately scoped, authorised, and that results are reported and acted upon.

4.1 Information Security Team (Blue Team): Participates in testing activities, for example by providing information for scoping and monitoring systems during tests. For red-teaming exercises, the Blue Team responds to simulated attacks, and its detection and response capabilities are evaluated.

4.2 Red Team / Penetration Testers: May consist of an internal offensive security team or external consultants. Execute tests in accordance with agreed rules of engagement, document all identified vulnerabilities and exploitation paths, and maintain confidentiality.

[... Sections 4.3–8 are not included in this preview. Purchase the full document to access the complete policy content. ...]

9. Monitoring and Audit

9 The STC shall maintain a calendar and log of all security testing activities performed. This log shall include the date, scope, the party performing the test, and a summary of the results. It shall be reviewed to confirm adherence to the required testing schedule, including ensuring that no critical system remains untested beyond the annual cycle.

9.1 Progress on remediation of test findings shall be monitored and reported monthly. Outstanding high-severity issues shall be reviewed in management meetings until closure.

9.2 The Internal Audit and Compliance Function, or an independent auditor, shall review the security testing programme annually to verify that tests are properly authorised, conducted, and reported; that critical findings have been addressed; and that the programme meets regulatory expectations. Any deviations shall result in corrective actions.

10. Review and Maintenance

10 This policy and the overall testing plan shall be reviewed at least annually. The review shall consider changes in the threat landscape, including the emergence of new attack techniques that may not be covered by current testing, and shall adjust scope or testing frequency accordingly.

10.1 Following any major cybersecurity incident or data breach, this policy must be reviewed to determine whether additional or more frequent testing could have prevented or detected the issue. The policy shall then be updated to incorporate any necessary adjustments, for example by adding a new scenario to red-teaming exercises based on observed attack patterns.

10.2 Changes to this policy must be approved by the CISO and noted by the Management Board. All relevant personnel shall be informed of the changes, and external testing partners shall be notified where any change affects their engagement terms.

11. Related Policies and Linkages

11.1 P06 – Risk Management Policy. Testing outputs support security risk assessment 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 lessons learned from testing.

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

11.6 P31 – Evidence Collection and Forensics Policy. Ensures artefacts are collected safely during testing.

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

11.8 P33 – Audit and Compliance Monitoring Policy. Provides independent oversight of the effectiveness of the testing programme.

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 (guidance on conducting cybersecurity exercises and technical testing)

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

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)