					Introduceți aici denumirea entității juridice înregistrate							
Numărul documentului: P40					Titlul documentului: **Politica privind testarea de securitate și exercițiile de tip red team**							
Versiunea: 1.0		Data intrării în vigoare: 01.01.2025			Proprietarul documentului:							
X	Politică		Standard		Procedură		Formular		Registru		Altul	

Istoricul reviziilor				
Numărul reviziei	**Data reviziei**	**Modificări**	**Revizuit de**	**Proprietarul procesului**

Aprobări			
Nume	**Funcție**	**Data**	**Semnătură**

Aliniată la standardele și reglementările aplicabile

Standard/reglementare	Clauză/articol	Comentariu
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	
GDPR al UE	Art. 32(1)(d)	
Directiva NIS2 a UE	Art. 21(2)(f)	
Regulamentul DORA al UE	Art. 25–27	
COBIT 2019	DSS05.07, MEA02.01, MEA02.03	

1. Scop

1 Se definește un program structurat pentru testarea periodică a securității rețelelor, sistemelor și aplicațiilor organizației, incluzând evaluări ale vulnerabilităților, teste de penetrare și exerciții de tip red team, pentru a îndeplini cerințele articolului 21 alineatul (2) litera (f) din Directiva NIS2 a UE privind evaluarea eficacității măsurilor de securitate cibernetică.

1.1 Punctele slabe din măsurile tehnice și organizatorice trebuie identificate și remediate proactiv prin testare controlată, contribuind astfel la îmbunătățirea continuă a profilului de risc al organizației în materie de securitate.

2. Domeniu de aplicare

2 Prezenta politică se aplică tuturor sistemelor informatice critice, aplicațiilor și infrastructurii-suport deținute sau operate de organizație. Politica include și testarea securității fizice a facilităților, în măsura în care aceasta este relevantă pentru securitatea cibernetică, de exemplu inginerie socială sau teste de penetrare fizică, dacă acestea intră în domeniul de aplicare al exercițiilor de tip red team.

2.1 Politica se aplică echipei interne de securitate, oricăror furnizori externi contractați pentru testare de securitate și proprietarilor relevanți de sisteme/aplicații. Toate activitățile de testare trebuie să fie autorizate și să urmeze procedurile prevăzute în prezenta politică, pentru a evita perturbările neintenționate.

3. Obiective

3 Se verifică eficacitatea controalelor de securitate cibernetică implementate, tehnice, operaționale și organizatorice, prin testare periodică și simulări, în conformitate cu cerința NIS2 privind măsurarea eficacității.

3.1 Se identifică vulnerabilități sau lacune pe care procesele operaționale curente le-ar putea omite, inclusiv probleme de configurare sau vulnerabilități zero-day, în scenarii de atac realiste, prin exerciții de tip red team, înainte ca acestea să fie exploatate de actori de amenințare.

3.2 Se furnizează conducerii asigurare privind eficacitatea controalelor și recomandări acționabile prin raportarea constatărilor rezultate din testare, pentru a permite decizii informate privind tratamentul riscului și îmbunătățirea continuă a programului de securitate.

4. Roluri și responsabilități

4 Coordonatorul testării de securitate (STC): desemnat de Directorul de securitate a informațiilor, este responsabil pentru planificarea și supravegherea tuturor activităților de testare de securitate. Acesta se asigură că testele au un domeniu de aplicare definit, sunt autorizate, iar rezultatele sunt raportate și tratate corespunzător.

4.1 Echipa internă de securitate a informațiilor (Blue Team): colaborează în cadrul testelor, de exemplu prin furnizarea de informații pentru definirea domeniului de aplicare și prin monitorizarea sistemelor pe durata testelor. În cadrul exercițiilor de tip red team, Blue Team răspunde la atacurile simulate, iar capacitatea sa de detectare și răspuns este evaluată.

4.2 Red Team / testeri de penetrare: pot fi o echipă internă de securitate ofensivă sau consultanți externi. Aceștia execută testele în baza regulilor de angajament convenite, documentează toate vulnerabilitățile identificate și căile de exploatare și mențin confidențialitatea.

[... Secțiunile 4.3–8 nu sunt incluse în această previzualizare. Achiziționați documentul complet pentru a accesa conținutul integral. ...]

9. Monitorizare și audit

9 STC trebuie să mențină un calendar și un registru al tuturor activităților de testare de securitate desfășurate. Acest registru trebuie să includă data, domeniul de aplicare, persoana sau entitatea care a efectuat testul și un rezumat al rezultatelor. Registrul va fi revizuit pentru a asigura respectarea calendarului impus, de exemplu astfel încât niciun sistem critic să nu rămână netestat peste ciclul anual.

9.1 Progresul remedierii constatărilor rezultate din testare va fi monitorizat și raportat lunar. Problemele restante cu severitate ridicată vor fi revizuite în ședințele de management până la închidere.

9.2 Auditul Intern sau un auditor independent va revizui anual programul de testare de securitate pentru a verifica faptul că testele sunt autorizate, desfășurate și raportate corespunzător, că constatările critice au fost tratate și că programul îndeplinește așteptările de reglementare. De exemplu, auditorii pot verifica dacă un test de penetrare a fost efectuat înainte de lansarea unui nou serviciu online, atunci când acest lucru este impus. Orice abatere de la politică va conduce la planuri de acțiuni corective.

10. Revizuire și mentenanță

10 Prezenta politică și planul general de testare vor fi revizuite cel puțin o dată pe an. Revizuirea va lua în considerare modificările din peisajul amenințărilor, de exemplu apariția unor noi tehnici de atac pe care testarea actuală nu le acoperă, și va adapta în consecință domeniul de aplicare sau frecvența.

10.1 După orice incident major de securitate cibernetică sau încălcare a securității, această politică trebuie reanalizată pentru a stabili dacă testări suplimentare sau mai frecvente ar fi putut preveni sau detecta problema. Politica va fi apoi actualizată pentru a integra astfel de ajustări, de exemplu prin adăugarea unui nou scenariu în exercițiile de tip red team pe baza tiparelor de atac observate.

10.2 Actualizările aduse acestei politici trebuie aprobate de Directorul de securitate a informațiilor și aduse la cunoștința consiliului de administrație. Tot personalul relevant va fi informat cu privire la modificări, iar partenerii externi de testare vor fi notificați dacă vreo modificare le afectează condițiile colaborării.

11. Politici conexe și interdependențe

11.1 P06 – Politica de management al riscurilor. Rezultatele testării susțin evaluarea și tratamentul riscurilor.

11.2 P22 – Politica de jurnalizare și monitorizare. Validează acoperirea detecției în timpul exercițiilor.

11.3 P24 – Politica de dezvoltare securizată. Integrează constatările testării în controalele SDLC.

11.4 P25 – Politica privind cerințele de securitate a aplicațiilor. Asigură reflectarea lecțiilor rezultate din testare în cerințe.

11.5 P30 – Politica de răspuns la incidente. Scenariile de tip red team rafinează playbook-urile și răspunsul.

11.6 P31 – Politica privind colectarea dovezilor și activitățile criminalistice. Colectează artefacte în timpul testării în condiții de siguranță.

11.7 P32 – Politica privind continuitatea activității și recuperarea în caz de dezastru. Exercițiile verifică reziliența în condiții de atac.

11.8 P33 – Politica de audit și monitorizare a conformității. Asigură supravegherea independentă a eficacității programului de testare.

12. Referințe

12.1 Directiva NIS2 (UE 2022/2555), articolul 21 alineatul (2), litera (f) (politici și proceduri pentru evaluarea eficacității măsurilor de management al riscurilor de securitate cibernetică)

12.2 Regulamentul de punere în aplicare al Comisiei (UE) 2024/2690, anexa, secțiunea 7 (cerințe privind monitorizarea, testarea și evaluarea eficacității măsurilor de securitate cibernetică)

12.3 Ghidul tehnic ENISA (2025) – anexa privind testarea de securitate și auditul (linii directoare pentru desfășurarea exercițiilor de securitate cibernetică și a testelor tehnice)

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

12.5 Cele mai bune practici din industrie: OWASP Testing Guide, NIST SP 800-115 (ghid tehnic pentru testarea de securitate), CBEST/GREEN Team (cadre de referință pentru exerciții de tip red team în sectorul financiar)