					Introduceți aici denumirea entității juridice înregistrate							
Numărul documentului: P30					Titlul documentului: **Politica de răspuns la incidente**							
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	Clauza 8.1, Clauza 9	Procese structurate pentru gestionarea riscurilor și răspunsul la incidente
ISO/IEC 27002:2022	Controalele 5.25–5.27	Roluri, raportare, răspuns și îmbunătățire privind incidentele
NIST SP 800-53 Rev.5	IR-1 până la IR-9	Ciclu de viață complet al răspunsului la incidente
GDPR al UE	Articolul 33 alineatul (1), 33 alineatul (3) literele (a)–(d), 34 alineatul (1), 34 alineatul (2) literele (a)–(c)	Termene pentru notificarea încălcărilor, raportare și comunicarea către persoanele vizate
Directiva NIS2 a UE	Articolul 23 alineatele (1)–(4)	Notificarea autorității naționale și raportare structurată
Regulamentul DORA al UE	Articolul 17 alineatele (1)–(3)	Raportarea incidentelor majore legate de TIC pentru entitățile financiare
COBIT 2019	DSS02, DSS04, MEA	Definirea, monitorizarea și evaluarea gestionării incidentelor, continuității și controalelor de evaluare

1. Scop

1.1 Prezenta politică stabilește cadrul formal pentru identificarea, raportarea, analiza, limitarea, răspunsul, recuperarea și evaluarea ulterioară a incidentelor de securitate a informațiilor care afectează organizația.

1.2 Aceasta asigură un răspuns prompt, coordonat și eficace pentru a reduce la minimum perturbarea activităților operaționale ale organizației, pierderile financiare, prejudiciul reputațional și neconformitatea cu cerințele de reglementare.

1.3 Politica sprijină, de asemenea, îmbunătățirea continuă a nivelului de reziliență cibernetică al organizației prin valorificarea lecțiilor învățate și integrarea constatărilor post-incident în guvernanță, instrumente și programe de instruire.

2. Domeniu de aplicare

2.1 Prezenta politică se aplică următoarelor:

2.1.1 Întregului personal, inclusiv angajaților, contractorilor, consultanților și furnizorilor terți de servicii

2.1.2 Tuturor sistemelor informatice, aplicațiilor, infrastructurii, rețelelor și datelor, indiferent dacă sunt locale, în cloud sau hibride

2.1.3 Tuturor tipurilor de incidente de securitate, inclusiv, fără a se limita la:

2.1.3.1 Acces neautorizat sau escaladarea privilegiilor

2.1.3.2 Atacuri cu programe malware și ransomware

2.1.3.3 Atacuri de tip refuz de serviciu (DoS/DDoS)

2.1.3.4 Pierdere de date, scurgeri de date sau exfiltrare de date

2.1.3.5 Utilizare abuzivă internă sau încălcări ale politicii

2.1.3.6 Breșe de securitate fizică ce afectează activele digitale

2.2 Politica acoperă detectarea, triajul, investigarea, escaladarea, limitarea, gestionarea dovezilor, notificarea, recuperarea și analiza cauzei principale.

3. Obiective

3.1 Stabilirea unei capabilități de răspuns la incidente repetabile și scalabile, care să permită detectarea, clasificarea și reducerea rapidă a impactului incidentelor de securitate.

3.2 Reducerea la minimum a impactului evenimentelor de securitate asupra activităților organizației prin proceduri structurate de limitare, eradicare și recuperare a sistemelor.

3.3 Asigurarea faptului că raportarea incidentelor și răspunsul la acestea sunt aliniate cu cerințele legale, de reglementare și contractuale, în special cele privind termenele de notificare a încălcărilor și gestionarea dovezilor.

3.4 Sprijinirea transparenței și responsabilității prin jurnalizare, documentare și monitorizarea indicatorilor pentru toate incidentele de securitate.

3.5 Promovarea îmbunătățirii continue prin analize post-incident, acțiuni corective și instruirea părților interesate.

4. Roluri și responsabilități

4.1 Directorul pentru securitatea informațiilor (CISO)

4.1.1 Deține cadrul de răspuns la incidente, asigură aplicarea politicii și supraveghează coordonarea incidentelor la nivelul întregii organizații.

4.1.2 Acționează ca principal punct de contact cu autoritățile de reglementare, conducerea executivă și consilierii juridici externi pe durata incidentelor majore.

4.2 Coordonatorul răspunsului la incidente

4.2.1 Coordonează echipele de răspuns multifuncționale, gestionează fluxurile de lucru și urmărește stadiul activităților de limitare și recuperare.

4.2.2 Inițiază și conduce analizele post-incident (PIR) și se asigură că acțiunile corective sunt înregistrate și implementate.

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

9. Cerințe privind revizuirea și actualizarea

9.1 Prezenta politică trebuie revizuită cel puțin anual și actualizată, după caz, pentru a include:

9.1.1 Modificări ale peisajului amenințărilor, tipurilor de incidente sau vectorilor de atac

9.1.2 Lecții învățate din incidente majore, incidente evitate la limită sau constatări ale autorităților de reglementare

9.1.3 Actualizări ale legilor și reglementărilor aplicabile (de exemplu, GDPR, DORA, NIS2)

9.1.4 Feedback din exercițiile de răspuns la incidente și din analizele post-incident

9.2 CISO este responsabil pentru inițierea și coordonarea procesului de revizuire, în consultare cu:

9.2.1.1 Consilierul juridic și DPO

9.2.1.2 SOC și operațiunile IT

9.2.1.3 Echipele de continuitate a activității și de management al riscului

9.2.1.4 Conducerea executivă

9.3 Modificările politicii trebuie să fie:

9.3.1 Documentate într-un depozit cu control al versiunilor

9.3.2 Comunicate tuturor echipelor afectate și incluse în instruirea de conștientizare actualizată

9.3.3 Validate prin exerciții de răspuns la incidente, tabletop sau practice, în termen de trei luni de la aprobare

9.4 Actualizările urgente determinate de amenințări emergente, constatări de audit sau obligații legale nou emise trebuie puse în aplicare imediat și consemnate în istoricul de revizuire al politicii.

10. Politici conexe și corelări

10.1 Prezenta politică este susținută de și depinde de următoarele politici ale organizației:

10.1.1 P1 – Politica de securitate a informațiilor: stabilește cerința generală pentru operațiuni bazate pe risc și pregătite pentru incidente.

10.1.2 P5 – Politica de management al schimbărilor: asigură că activitățile de limitare și recuperare care implică infrastructura sau serviciile urmează proceduri formale.

10.1.3 P13 – Politica de clasificare și etichetare a datelor: sprijină clasificarea severității incidentelor pe baza sensibilității datelor.

10.1.4 P15 – Politica de backup și restaurare: permite recuperarea după ransomware sau atacuri distructive, cu asigurarea integrității.

10.1.5 P18 – Politica privind controalele criptografice: definește măsuri de criptare care reduc impactul incidentelor și riscurile de expunere a datelor.

10.1.6 P22 – Politica de jurnalizare și monitorizare: oferă vizibilitatea de bază asupra evenimentelor, alertarea și păstrarea jurnalelor necesare pentru detectare eficace și analize criminalistice.

10.1.7 P29 – Politica privind datele de test și mediile de testare: asigură că incidentele care afectează sistemele non-producție sunt gestionate, de asemenea, într-un mod structurat și sigur.

10.1.8 P33 – Politica de audit și monitorizare a conformității: validează pregătirea pentru incidente și eficacitatea răspunsului prin audituri structurate și evaluări de conformitate.

11. Standarde și cadre de referință

11.1 ISO/IEC 27001: Clauza 8.1 – Planificare și control operațional: procese structurate pentru gestionarea riscurilor și planificarea răspunsului la incidente.

11.2 ISO/IEC 27002:2022 – Controalele 5.25–5.27: responsabilități privind gestionarea incidentelor, raportarea, răspunsul, comunicarea și îmbunătățirea.

11.3 NIST SP 800-53 Rev.5: IR-1 până la IR-9, AU-6, PL-2: cerințe complete pentru ciclul de viață al răspunsului la incidente, audit și planificarea securității.

11.4 GDPR al UE: Articolele 33 și 34: obligații de raportare către autoritățile de supraveghere și cerințe de notificare a persoanelor vizate (cu excepțiile definite).

11.5 Directiva NIS2 a UE (2022/2555): Articolul 23: raportare națională obligatorie, inclusiv obligații de raportare intermediară și finală.

11.6 DORA a UE (2022/2554): Articolul 17: cerințe de raportare către autorități a incidentelor TIC pentru instituțiile financiare.

11.7 COBIT 2019: DSS02, DSS04, MEA01: gestionarea incidentelor de serviciu și a continuității, precum și monitorizarea performanței și conformității.