					Introduceți aici denumirea entității juridice înregistrate							
Numărul documentului: P30S					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**

Aliniere la standarde și reglementări

Standard/reglementare	Clauză/articol	Comentariu
ISO/IEC 27001:2022	Clauzele 6.1, 6.3, 8	Gestionarea incidentelor, îmbunătățire continuă, control operațional
ISO/IEC 27002:2022	Controalele 5.24, 5.25	Detectarea incidentelor, pregătire, lecții învățate
NIST SP 800-53 Rev.5	IR-4, IR-5, IR-6	Gestionarea și monitorizarea incidentelor, raportare
GDPR	Articolul 33	Cerințe de notificare a încălcărilor securității datelor
Directiva UE NIS2	Articolul 23	Raportarea obligatorie a incidentelor cibernetice
Regulamentul UE DORA	Articolul 17	Gestionarea incidentelor TIC
COBIT 2019	DSS02, DSS04	Gestionarea serviciilor și incidentelor, precum și continuitatea

1. Scop

1.1. Prezenta politică stabilește modul în care organizația detectează, raportează și răspunde la incidente de securitate a informațiilor care afectează sistemele, datele sau serviciile digitale ale acesteia.

1.2. Aceasta permite organizației să minimizeze impactul, să protejeze datele clienților și să își îndeplinească obligațiile de reglementare, cum ar fi cerința GDPR de notificare a încălcărilor în termen de 72 de ore.

1.3. Politica asigură responsabilități clare, etape de comunicare și activități ulterioare incidentului, inclusiv pentru organizațiile mici care nu dispun de o echipă dedicată de securitate.

2. Domeniu de aplicare

2.1. Prezenta politică se aplică următoarelor:

2.1.1. Tuturor angajaților, contractorilor și furnizorilor externi de servicii IT

2.1.2. Tuturor sistemelor și serviciilor administrate de companie, inclusiv site-urilor web, platformelor cloud, dispozitivelor mobile, laptopurilor și conturilor de e-mail

2.1.3. Tuturor tipurilor de incidente, inclusiv:

2.1.3.1. Acces neautorizat la date sau sisteme

2.1.3.2. Infectări cu programe malware sau atacuri de tip ransomware

2.1.3.3. Tentative de phishing sau de inginerie socială

2.1.3.4. Indisponibilitatea sistemelor ca urmare a unui atac cibernetic sau a unei utilizări necorespunzătoare

2.1.3.5. Divulgarea accidentală sau ștergerea informațiilor sensibile

2.1.3.6. Pierderea sau furtul dispozitivelor de serviciu ori al mediilor de stocare

3. Obiective

3.1. Stabilirea unui proces clar pentru identificarea și escaladarea incidentelor de securitate.

3.2. Asigurarea faptului că incidentele sunt raportate, înregistrate și tratate în termenele stabilite.

3.3. Asigurarea limitării rapide a impactului, a recuperării datelor și a restabilirii serviciilor.

3.4. Asigurarea notificării părților afectate (de exemplu, clienți, autorități de reglementare), atunci când legea impune acest lucru.

3.5. Prevenirea reapariției prin analiza cauzei-rădăcină, acțiuni corective și îmbunătățirea politicii.

3.6. Sprijinirea IMM-urilor în îndeplinirea cerințelor de certificare ISO/IEC 27001 și în demonstrarea responsabilității în cadrul auditurilor.

4. Roluri și responsabilități

4.1. Directorul general (GM)

4.1.1. Deține responsabilitatea pentru această politică și asigură implementarea acesteia.

4.1.2. Supraveghează activitățile de răspuns la incidente și aprobă notificările către autoritățile de reglementare sau către clienți.

4.1.3. Revizuiește rapoartele ulterioare incidentului și se asigură că politica este actualizată atunci când este necesar.

4.1.4. Poate delega atribuțiile de coordonare, dar păstrează responsabilitatea finală.

4.2. Furnizorul de servicii IT / administratorul de sistem (intern sau extern)

4.2.1. Detectează și investighează potențiale incidente de securitate.

4.2.2. Implementează măsuri de limitare a impactului și de recuperare (de exemplu, dezactivarea accesului, restaurarea copiilor de siguranță).

4.2.3. Notifică GM-ul cu privire la toate incidentele confirmate sau suspectate în termen de 1 oră de la identificare.

4.2.4. Menține un jurnal al incidentelor care include marcaje temporale, evaluarea impactului și acțiunile de răspuns.

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

9. Cerințe de revizuire și actualizare

9.1. Revizuire programată

9.1.1. Prezenta politică trebuie revizuită cel puțin o dată la 12 luni de către Directorul general (GM), pentru a asigura:

9.1.1.1. Alinierea la controalele ISO/IEC 27001:2022

9.1.1.2. Capacitatea de răspuns la noi amenințări, riscuri și incidente

9.1.1.3. Menținerea conformității cu obligațiile legale și contractuale (de exemplu, GDPR, DORA)

9.2. Evenimente declanșatoare

9.2.1. Politica trebuie, de asemenea, revizuită și actualizată după:

9.2.1.1. Orice incident de severitate ridicată sau notificare către autoritățile de reglementare

9.2.1.2. Introducerea unei noi infrastructuri IT sau a unor modificări de sistem

9.2.1.3. Modificări ale cerințelor legale referitoare la încălcările de securitate

9.3. Documentarea revizuirii și distribuire

9.3.1. Toate revizuirile și modificările trebuie documentate în jurnalul de modificări al politicii

9.3.2. Versiunile actualizate trebuie distribuite tuturor angajaților, furnizorilor și prestatorilor de servicii IT implicați în securitate sau în operarea sistemelor

9.3.3. Dovezile privind conștientizarea personalului (de exemplu, note de ședință sau confirmări prin e-mail) trebuie păstrate pentru pregătirea auditului

10. Politici conexe și corelări

10.1. Prezenta politică trebuie aplicată în corelare cu următoarele politici SME:

10.1.1. P1S – Politica de securitate a informațiilor: stabilește așteptările generale privind menținerea confidențialității, integrității și disponibilității în cadrul activităților organizației, inclusiv gestionarea incidentelor.

10.1.2. P2S – Politica privind rolurile și responsabilitățile de guvernanță: stabilește structurile de autoritate și responsabilitate pentru detectarea, raportarea și escaladarea incidentelor.

10.1.3. P4S – Politica de control al accesului: permite revocarea imediată a drepturilor de acces în timpul măsurilor de răspuns la incidente.

10.1.4. P8S – Politica de conștientizare și instruire în domeniul securității informațiilor: asigură faptul că toți angajații pot identifica și raporta eficace incidentele de securitate.

10.1.5. P17S – Politica de protecție a datelor și confidențialitate: orientează procedurile legale de notificare a încălcărilor în temeiul GDPR și susține conformitatea de reglementare pe durata incidentelor.

10.1.6. P22S – Politica de jurnalizare și monitorizare: oferă instrumentele și vizibilitatea necesare pentru detectarea, analizarea și auditarea evenimentelor de securitate.

10.1.7. P31S – Politica de colectare a dovezilor și investigații criminalistice digitale: sprijină investigarea și susținerea juridică a acțiunilor legate de incidente prin orientări privind gestionarea corectă a probelor.

10.2. Aceste politici stabilesc împreună cadrul operațional al IMM-ului pentru detectarea, răspunsul și recuperarea în urma incidentelor de securitate a informațiilor.

11. Standarde și cadre de referință

11.1. ISO/IEC 27001

11.1.1. Clauza 6.1 – Impune planificarea tratării riscurilor, inclusiv pregătirea pentru incidente.

11.1.2. Clauza 6.3 – Susține îmbunătățirea continuă prin lecțiile învățate din evenimentele de securitate.

11.1.3. Clauza 8.1 – Evidențiază controlul operațional pentru gestionarea incidentelor și a întreruperilor.

11.2. ISO/IEC 27002

11.2.1. Controlul 5.24 – Impune o abordare structurată pentru raportarea, evaluarea și răspunsul la incidente de securitate a informațiilor.

11.2.2. Controlul 5.25 – Se concentrează pe învățarea din incidente pentru îmbunătățirea pregătirii viitoare și a rezilienței sistemelor.

11.3. NIST SP 800-53 Rev.5

11.3.1. IR-4 – Definește procedurile de gestionare a incidentelor, inclusiv limitarea impactului și recuperarea.

11.3.2. IR-5 – Stabilește cerințele pentru monitorizarea și analiza incidentelor.

11.3.3. IR-6 – Impune protocoale de raportare a incidentelor, atât interne, cât și externe.

11.4. GDPR

11.4.1. Articolul 33 – Impune raportarea încălcărilor securității datelor cu caracter personal către autoritățile de reglementare în termen de 72 de ore, incluzând detalii privind amploarea și măsurile de reducere a impactului.

11.5. Directiva UE NIS2 (2022/2555)

11.5.1. Articolul 23 – Impune entităților esențiale și importante să notifice autoritățile competente cu privire la incidentele semnificative, utilizând formate standardizate de raportare.

11.6. Regulamentul UE DORA (2022/2554)

11.6.1. Articolul 17 – Impune entităților financiare să clasifice, să raporteze și să urmărească incidentele și întreruperile legate de TIC.

11.7. COBIT 2019

11.7.1. DSS02 – Gestionarea cererilor de servicii și a incidentelor: oferă îndrumări pentru tratarea eficace a incidentelor operaționale și de securitate, în concordanță cu obiectivele de guvernanță.

11.7.2. DSS04 – Gestionarea continuității: corelează răspunsul la incidente cu strategiile mai ample de continuitate și recuperare.