					Introduceți aici denumirea entității juridice înregistrate							
Numărul documentului: P32					Titlul documentului: **Politica privind continuitatea activității și recuperarea în caz de dezastru**							
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	
ISO/IEC 27002:2022	Controalele 5.29, 5.30	
NIST SP 800-53 Rev. 5	CP-1 până la CP-11	
NIST SP 800-34 Rev. 1	Planificarea măsurilor de continuitate	Cadru
ISO 22301:2019		Cerințe pentru sistemul de management al continuității activității
GDPR al UE	Articolul 32	
Directiva NIS2 a UE	Articolul 21(2)(f)	
Regulamentul DORA al UE	Articolul 10	
COBIT 2019	DSS04	

1. Scop

1.1. Prezenta politică definește controalele și responsabilitățile obligatorii pentru asigurarea capacității organizației de a menține sau de a restabili activitățile operaționale critice și serviciile TIC de suport în timpul și după producerea unui incident perturbator.

1.2. Aceasta are ca scop protejarea vieții, a stabilității operaționale, a obligațiilor legale, a angajamentelor față de clienți și a reputației organizației, prin integrarea rezilienței în planificarea proactivă și în capabilitățile de recuperare validate.

1.3. Prezenta politică constituie baza cadrului organizațional pentru managementul continuității activității (BCM) și recuperarea în caz de dezastru (DR), asigurând conformitatea cu cerințele de reglementare, contractuale și de industrie aplicabile.

2. Domeniu de aplicare

2.1. Prezenta politică se aplică tuturor unităților organizaționale, sistemelor informatice, proceselor de business, personalului și serviciilor prestate de terți care sunt clasificate drept critice sau esențiale pe baza rezultatelor analizei impactului asupra activității (BIA).

2.2. Politica acoperă:

2.2.1. Perturbări naturale și provocate de om, inclusiv atacuri cibernetice, defecțiuni de infrastructură, indisponibilitatea centrelor de date, pandemii și întreruperi ale serviciilor furnizorilor

2.2.2. Planificarea, testarea și îmbunătățirea continuă a planurilor de continuitate a activității (BCP) și a planurilor de recuperare în caz de dezastru (DRP)

2.2.3. Rolurile și responsabilitățile pentru răspunsul în situații de urgență, coordonarea recuperării și escaladarea incidentelor

2.3. Intră sub incidența prevederilor prezentei politici tot personalul care are responsabilități privind continuitatea sau recuperarea, inclusiv IT, proprietarii de procese de business, managerii de criză și furnizorii.

3. Obiective

3.1. Asigurarea continuității activităților și serviciilor organizației prin proceduri predefinite și testate, cu minimizarea impactului operațional, reputațional și juridic.

3.2. Recuperarea serviciilor TIC în limitele Obiectivului privind timpul de recuperare (RTO) și ale Obiectivului privind punctul de recuperare (RPO) stabilite, aliniate cu nivelurile de toleranță la risc ale organizației.

3.3. Atribuirea clară a responsabilității pentru planificarea, execuția și guvernanța continuității activității și a recuperării în caz de dezastru la nivelul întregii organizații.

3.4. Asigurarea faptului că capabilitățile de continuitate sunt testate, menținute și îmbunătățite periodic pe baza unor scenarii realiste și a constatărilor de audit.

3.5. Îndeplinirea obligațiilor de conformitate în raport cu ISO, NIST, GDPR, DORA și NIS2, în sprijinul diligenței necesare privind reziliența operațională și disponibilitatea.

4. Roluri și responsabilități

4.1. Conducerea executivă

4.1.1. Aprobă politica privind continuitatea activității și recuperarea în caz de dezastru și asigură alinierea strategică.

4.1.2. Alocă bugetul și resursele necesare pentru susținerea continuității activității, a răspunsului în situații de urgență și a exercițiilor de recuperare.

4.2. Managerul de continuitate a activității (responsabil BCM)

4.2.1. Are responsabilitatea pentru elaborarea și menținerea BCP-urilor la nivelul întregii organizații și pentru coordonarea testării continuității.

4.2.2. Menține calendarul BIA, facilitează instruirea și se asigură că documentația respectă cerințele de conformitate.

[... 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. Prezenta politică trebuie revizuită anual de Managerul de continuitate a activității și de Directorul de securitate a informațiilor pentru a asigura alinierea cu:

9.1.1. schimbările din activitățile organizației, sistemele critice sau infrastructură

9.1.2. lecțiile învățate din incidente, audituri, exerciții de tip tabletop sau teste DR

9.1.3. obligațiile actualizate de reglementare sau contractuale (de exemplu, DORA, GDPR, cerințe RTO/RPO ale clienților)

9.1.4. modificările apetitului la risc al organizației sau ale strategiei de continuitate

9.2. Revizuirile trebuie să includă:

9.2.1. validarea relevanței planurilor și a datelor de contact

9.2.2. reevaluarea RTO, RPO și a încadrării pe niveluri de recuperare

9.2.3. evaluarea capacității serviciilor de backup și DR

9.2.4. feedbackul părților interesate care au executat recent planuri sau teste de recuperare

9.3. Toate modificările politicii trebuie:

9.3.1. să fie supuse controlului versiunilor, cu justificare documentată și aprobarea părților interesate

9.3.2. să fie comunicate personalului-cheie și echipelor cu responsabilități actualizate

9.3.3. să fie reflectate în instruirea actualizată, materialele de conștientizare și procedurile operaționale

9.4. Actualizările interimare de urgență trebuie emise dacă apare o schimbare organizațională majoră, o obligație legală sau o constatare critică ce face ca planurile sau politica actuală să nu mai fie viabile.

10. Politici corelate și interdependențe

10.1. Prezenta politică funcționează în coordonare cu următoarele documente-cheie:

10.1.1. P1 – Politica de securitate a informației: stabilește cerința privind operațiuni reziliente, bazate pe risc, în orice condiții.

10.1.2. P5 – Politica de management al schimbărilor: asigură că orice schimbări de configurație sau de infrastructură legate de recuperare urmează fluxuri documentate și aprobate.

10.1.3. P14 – Politica de păstrare și eliminare a datelor: reglementează ciclul de viață al mediilor de backup și al datelor recuperate utilizate în activitățile de continuitate.

10.1.4. P15 – Politica de backup și restaurare: impune controale privind frecvența backup-urilor, securitatea și verificarea restaurării.

10.1.5. P18 – Politica privind controalele criptografice: asigură că procesele de recuperare respectă standardele de criptare și confidențialitate.

10.1.6. P22 – Politica de jurnalizare și monitorizare: sprijină detectarea și escaladarea evenimentelor care afectează continuitatea.

10.1.7. P30 – Politica de răspuns la incidente: definește procesele de izolare, escaladare și analiză a cauzei principale, aliniate cu declanșatorii de continuitate.

10.1.8. P33 – Politica de audit și monitorizare a conformității: validează integritatea și eficacitatea practicilor de continuitate și recuperare la nivelul sistemelor și proceselor.

11. Standarde și cadre de referință

11.1. Prezenta politică este aliniată la standarde recunoscute la nivel internațional privind continuitatea activității și recuperarea în caz de dezastru, susținând caracterul verificabil, reziliența și conformitatea legală.

11.2. ISO/IEC 27002

11.2.1. Anexa A, Controlul 5.29 – securitatea informației în timpul perturbărilor: impune continuitatea măsurilor de securitate în condiții adverse.

11.2.2. Anexa A, Controlul 5.30 – pregătirea TIC pentru continuitatea activității: impune pregătirea, testarea și validarea capabilităților de recuperare TIC.

11.3. ISO 22301:2019 – sisteme de management al continuității activității

11.3.1. Oferă cadrul pentru stabilirea, implementarea și menținerea practicilor BCM aliniate cu obiectivele organizației și pragurile de risc.

11.4. NIST SP 800-34 Rev. 1 – ghid pentru planificarea măsurilor de continuitate

11.4.1. Prezintă bune practici pentru planurile de continuitate ale sistemelor IT, inclusiv elaborarea strategiei de continuitate, analiza impactului și testarea planurilor.

11.5. GDPR al UE (2016/679)

11.5.1. Articolul 32 – Securitatea prelucrării: impune reziliența sistemelor și serviciilor de prelucrare, precum și restaurarea în timp util a disponibilității și a accesului la datele cu caracter personal după un incident.

11.6. Directiva NIS2 a UE (2022/2555)

11.6.1. Articolul 21(2)(f): impune măsuri privind continuitatea activității și managementul crizelor pentru susținerea securității rețelelor și sistemelor informatice.

11.7. Regulamentul DORA al UE (2022/2554)

11.7.1. Articolul 10 – continuitatea activității TIC: impune entităților financiare să elaboreze și să testeze planuri de continuitate TIC, inclusiv RTO/RPO bazate pe risc și capabilități de comutare în caz de avarie.

11.8. COBIT 2019

11.8.1. DSS04 – managementul continuității: acoperă toate aspectele planificării continuității, inclusiv identificarea amenințărilor, analiza impactului, strategia de recuperare și testarea periodică.