| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | Introduceți aici denumirea entității juridice înregistrate | | | | | | | |
| Numărul documentului:<br>P32S | | | | | Titlul documentului:<br>**Politica de continuitate a activității și de recuperare în caz de dezastru** | | | | | | | |
| Versiunea:<br>1.0 | | Data intrării în vigoare:<br>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** |
| | | | |
| | | | |

**Notă juridică (drepturi de autor și restricții de utilizare)**

(C) 2025 Clarysec LLC. All rights reserved.

Acest document este proprietatea intelectuală a Clarysec LLC. Nicio parte a acestui document nu poate fi copiată, reutilizată, distribuită sau modificată în scopuri comerciale sau de implementare fără autorizare prealabilă expresă, în scris.

Utilizarea neautorizată este strict interzisă și poate conduce la acțiuni legale.

Pentru licențiere, contactați: info@clarysec.com

Aliniată la standardele și reglementările aplicabile

| Standard/reglementare | Clauză/articol | Comentariu |
|---|---|---|
| ISO/IEC 27001:2022 | Clauzele 6.1, 6.3, 8 | |
| ISO/IEC 27002:2022 | Controalele 5.29, 5.30 | |
| NIST SP 800-53 Rev.5 | CP-2, CP-4, CP-6, CP-7 | |
| GDPR al UE | Articolele 32, 33 | |
| Directiva NIS2 a UE | Articolul 21(2)(f) | |
| Regulamentul DORA al UE | Articolul 10 | |
| COBIT 2019 | DSS04 | |

**1. Scop**

1.1 Prezenta politică asigură faptul că organizația poate menține activitățile operaționale și poate restaura serviciile IT esențiale în timpul și după evenimente perturbatoare, cum ar fi întreruperile de energie, atacurile cibernetice, infecțiile cu ransomware sau defecțiunile de sistem.

1.2 Aceasta stabilește un cadru clar pentru planificarea continuității activității și a recuperării în caz de dezastru (BC/DR), adaptat IMM-urilor fără echipe IT dedicate.

1.3 Prezenta politică sprijină organizația în îndeplinirea cerințelor obligatorii prevăzute de ISO/IEC 27001:2022, GDPR, NIS2, DORA și COBIT 2019, consolidând totodată reziliența operațională și încrederea clienților.

**2. Domeniu de aplicare**

**2.1 Prezenta politică se aplică următoarelor:**

2.1.1 tuturor sistemelor și serviciilor critice pentru activitatea organizației (de ex., e-mail, stocare în cloud, platforme de facturare, evidențe privind clienții);

2.1.2 tuturor angajaților și furnizorilor externi de servicii IT responsabili de pregătirea și executarea activităților BC/DR;

2.1.3 tuturor tipurilor de perturbări, inclusiv incidentelor cibernetice, defecțiunilor hardware, pierderii alimentării cu energie, inundațiilor și inaccesibilității biroului.

**2.2 Aceasta acoperă:**

2.2.1 managementul backup-urilor;

2.2.2 planificarea continuității activității (BCP);

2.2.3 operațiunile de recuperare în caz de dezastru;

2.2.4 instruirea și testarea personalului;

2.2.5 procedurile de răspuns juridic și de reglementare.

**3. Obiective**

3.1 Protejarea capacității organizației de a furniza servicii esențiale în pofida unor perturbări neplanificate.

3.2 Asigurarea recuperării la timp a sistemelor și datelor, pe baza unor obiective privind timpul de recuperare (RTO) predefinite.

3.3 Asigurarea faptului că întregul personal poate urma procedurile de continuitate în situații de criză, cu un nivel minim de confuzie.

3.4 Menținerea conformității cu cerințele de reglementare privind protecția datelor și reziliența operațională, inclusiv articolul 32 din GDPR și articolul 21 din NIS2.

3.5 Stabilirea unei strategii practice și testabile de continuitate și recuperare, adecvate IMM-urilor.

## 4. Roluri și responsabilități

### 4.1 Director general (GM)

4.1.1 deține procesul BC/DR și prezenta politică;

4.1.2 aprobă planul de continuitate a activității (BCP);

4.1.3 coordonează răspunsul la incidente și comunicarea internă în timpul perturbărilor;

4.1.4 efectuează notificările către autorități, după caz (de ex., notificarea încălcărilor către autoritatea competentă în temeiul GDPR).

### 4.2 Furnizor de suport IT / administrator de sistem

4.2.1 menține și testează backup-urile;

4.2.2 execută procedurile de recuperare în caz de dezastru atunci când acestea sunt declanșate;

4.2.3 documentează toate acțiunile de recuperare și toate evenimentele de restaurare a sistemelor;

4.2.4 raportează imediat Directorului general incidentele IT critice.

[ ... 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 Revizuirea anuală a politicii și a planului

9.1.1 Directorul general (GM) trebuie să se asigure că prezenta politică și planul de continuitate a activității (BCP) aferent sunt revizuite formal cel puțin o dată pe an.

#### 9.1.2 Revizuirea trebuie să includă:

9.1.2.1 evaluarea riscurilor noi sau emergente;

9.1.2.2 revalidarea valorilor RTO/RPO;

9.1.2.3 verificarea informațiilor privind furnizorii și contactele;

9.1.2.4 alinierea cu schimbările din sistemele IT, obligațiile legale sau activitățile organizației.

### 9.2 Actualizări declanșate de evenimente

#### 9.2.1 Prezenta politică trebuie actualizată și ca răspuns la:

9.2.1.1 incidente sau perturbări majore, în special dacă obiectivele nu au fost atinse;

9.2.1.2 noi obligații legale sau de reglementare (de ex., modificări DORA);

9.2.1.3 modificări ale sistemelor critice, platformelor cloud sau personalului;

9.2.1.4 constatările rezultate din testele anuale BCP/DR.

### 9.3 Procesul de control al schimbărilor

9.3.1 Toate schimbările trebuie aprobate de GM.

9.3.2 Trebuie menținut un jurnal al versiunilor, care să includă data, descrierea schimbării și aprobatorul.

9.3.3 Politica actualizată trebuie redistribuită întregului personal relevant, inclusiv furnizorului IT și șefilor de departament.

### 9.4 Documentarea lecțiilor învățate

9.4.1 După teste sau perturbări reale, lecțiile învățate documentate trebuie integrate în revizuirile viitoare.

9.4.2 Aceste revizuiri trebuie să includă și evaluări ale performanței furnizorilor, precum și verificări privind adecvarea răspunsului.

## 10. Politici conexe și interdependențe

### 10.1 Prezenta politică este strâns integrată cu următoarele politici SME:

10.1.1 P1S – Politica de securitate a informației: definește obiectivele de securitate de nivel înalt pe care practicile de continuitate și recuperare trebuie să le susțină.

10.1.2 P4S – Politica de control al accesului: permite revocarea de urgență sau restaurarea accesului utilizatorilor în scenarii de perturbare a activității.

10.1.3 P6S – Politica de management al riscurilor: constituie baza pentru identificarea, evaluarea și prioritizarea riscurilor legate de continuitate.

10.1.4 P8S – Politica privind conștientizarea și instruirea în domeniul securității informației: asigură că angajații sunt pregătiți să acționeze în timpul perturbărilor și înțeleg BCP.

10.1.5 P15S – Politica de backup și restaurare: stabilește proceduri tehnice specifice pentru protejarea disponibilității datelor și pentru recuperare.

10.1.6 P17S – Politica de protecție a datelor și confidențialitate: asigură că planificarea continuității respectă măsurile de protecție a datelor cu caracter personal și cerințele GDPR în timpul și după incidente.

10.1.7 P22S – Politica de jurnalizare și monitorizare: sprijină detectarea evenimentelor care pot declanșa procesele BC/DR și oferă piste de audit criminalistice după perturbări.

10.1.8 P30S – Politica de răspuns la incidente: precedă în mod direct activarea procesului de recuperare în cazul incidentelor cibernetice sau operaționale.

10.1.9 P31S – Politica privind colectarea dovezilor și investigațiile criminalistice: asigură că dovezile digitale sunt colectate în scenarii de continuitate pentru nevoi de conformitate, asigurare sau investigare.

10.2 Aceste politici formează un cadru coerent, pregătit pentru audit, pentru reziliență, responsabilitate și continuitatea controalelor la nivelul tuturor activităților SME.

## 11. Standarde și cadre de referință

### 11.1 ISO/IEC 27001:

11.1.1 Clauza 6.1 – impune planificarea și tratamentul bazate pe risc, inclusiv continuitatea activității și recuperarea.

11.1.2 Clauza 6.3 – subliniază îmbunătățirea continuă după perturbări.

11.1.3 Clauza 8.1 – impune controale operaționale, inclusiv măsuri de continuitate documentate.

### 11.2 ISO/IEC 27002:

11.2.1 Controlul 5.29 – impune stabilirea și menținerea măsurilor de continuitate a activității.

11.2.2 Controlul 5.30 – impune testarea și revizuirea acestor măsuri.

### 11.3 NIST SP 800-53 Rev.5:

11.3.1 CP-2 – definește cerințele pentru planificarea situațiilor de contingență.

11.3.2 CP-4 – impune instruirea personalului organizației privind situațiile de contingență.

11.3.3 CP-6 – acoperă cerințele privind locațiile alternative de stocare.

11.3.4 CP-7 – reglementează cerințele privind locațiile alternative de procesare.

### 11.4 GDPR al UE:

11.4.1 Articolul 32 – impune măsuri pentru a asigura disponibilitatea continuă și reziliența sistemelor și serviciilor de prelucrare.

11.4.2 Articolul 33 – declanșează obligații de notificare a încălcărilor în cazurile în care un eșec de continuitate conduce la compromiterea datelor cu caracter personal.

**11.5 Directiva NIS2 a UE (2022/2555):**

11.5.1 Articolul 21(2)(f) – impune capabilități de planificare a continuității și de management al crizelor ca parte a pregătirii pentru riscuri cibernetice.

**11.6 Regulamentul DORA al UE (2022/2554):**

11.6.1 Articolul 10 – impune implementarea testării rezilienței operaționale digitale și a capabilităților de recuperare, în special pentru IMM-urile din sectorul financiar.

**11.7 COBIT 2019:**

11.7.1 DSS04 – Gestionarea continuității: oferă orientări de guvernanță corporativă pentru menținerea și validarea rezilienței operaționale, inclusiv privind responsabilitatea, testarea, integrarea furnizorilor și revizuirile după evenimente.