

**S.R.L “CloudSentinel”**

**PROCEDURA DE ACȚIUNE CORECTIVĂ**

|  |  |
| --- | --- |
| Cod: | PAC-01 |
| Versiune: | 0.4.1a |
| Data versiunii: | Jun 5, 2024 |
| Creat de: | Chirita Stanislav |
| Aprobat de: | Boboc Sandu |
| Nivelul de confidențialitate: | Strict Secret |

**Istoricul modificărilor**

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Version** | **Created by** | **Description of change** |
| 2024-01-01 | 0.1 | Chirita Stanislav | Crearea procedurii de acțiune corectivă |
| 2024-03-15 | 0.2 | Chihai Andiran | Adăugarea detaliilor privind identificarea neconformităților |
| 2024-05-10 | 0.3 | Chihai Andiran | Actualizarea criteriilor de evaluare a necesității de acțiuni corective |
| 2024-07-20 | 0.4 | Boboc Sandu | Clarificarea procesului de implementare a acțiunilor corective |
| 2024-09-05 | 0.4.1a | Chirita Stanislav | Revizuire generală a întregului document |

**Cuprins:**

[1. Scop, domeniu de aplicare și utilizatori 3](#__RefHeading___Toc491_1450245376)

[2. Documente de referință 3](#__RefHeading___Toc493_1450245376)

[3. Corecții și acțiuni corective 4](#__RefHeading___Toc495_1450245376)

[3.1. Neconformități și corecții 4](#__RefHeading___Toc497_1450245376)

[3.2. Acțiuni corective 4](#__RefHeading___Toc499_1450245376)

[3.3. Implementarea acţiunilor corective 4](#__RefHeading___Toc501_1450245376)

[4. Gestionarea înregistrărilor păstrate pe baza acestui document 6](#__RefHeading___Toc503_1450245376)

[5. Valabilitatea și managementul documentelor 6](#__RefHeading___Toc505_1450245376)

[6. Anexe 6](#__RefHeading___Toc507_1450245376)

# Scop, domeniu de aplicare și utilizatori

Scopul acestei proceduri este de a descrie toate activitățile legate de inițierea, implementarea și păstrarea înregistrărilor corecțiilor, precum și a acțiunilor corective.

Această procedură se aplică tuturor activităților implementate în Sistemul de Management al Securității Informației (ISMS) Sistemul de Management al Continuității Serviciilor Cloud (CMCC).

Utilizatorii acestui document sunt toți angajații CloudSentinel.

# Documente de referință

* ISO/IEC 27001 standard, clauza 10.1
* ISO 22301 standard, clauza 10.1
* BS 25999-2 standard, clauza 6.1
* Politica de Securitate a Informațiilor
* Politica de Continuitate a Afacerilor
* Procedura de audit intern
* Procedura de management al incidentelor
* Politica de management al schimbărilor
* Politica de gestionare a riscurilor de securitate a informațiilor
* Procedura de gestionare a vulnerabilităților
* **ISO/IEC 27002:** Codul de practică pentru managementul securității informațiilor, care oferă orientări și recomandări pentru implementarea și menținerea unui sistem eficient de management al securității informațiilor.
* **ISO/IEC 27005:** Standardul pentru managementul riscurilor de securitate a informațiilor, care furnizează un cadru și o metodologie pentru identificarea, evaluarea și gestionarea riscurilor de securitate a informațiilor într-un mediu de cloud computing.
* **ISO/IEC 27034:** Standardul pentru securitatea aplicațiilor, care oferă orientări și bune practici pentru dezvoltarea și implementarea aplicațiilor securizate într-un mediu de cloud computing.
* **NIST SP 800-171:** Standardele de securitate cibernetică pentru informațiile nereprezentând informații controlate, care sunt esențiale pentru asigurarea securității datelor în cloud, în special în cazul organizațiilor care lucrează cu informații guvernamentale sau militare.

# Corecții și acțiuni corective

## Neconformități și corecții

O nonconformitate este orice eșec în îndeplinirea cerințelor standardelor, documentației interne, reglementărilor, obligațiilor contractuale și altor obligații în cadrul serviciului de cloud. Nonconformitățile pot fi identificate în timpul unei auditări interne sau externe, pe baza rezultatelor revizuirii de management, după incidente, în timpul operațiunilor normale de afaceri sau în orice altă ocazie.

Un angajat care observă o nonconformitate trebuie să ia măsuri imediate pentru a o controla, a o limita și a o corecta, și să gestioneze consecințele acesteia; dacă un angajat nu este responsabil pentru o astfel de nonconformitate, el/ea trebuie să transmită informații despre acea nonconformitate unei persoane responsabile, care trebuie să facă corectarea necesară.

## Acțiuni corective

Această persoană responsabilă trebuie să evalueze necesitatea eliminării cauzei nonconformității și prevenirea recurenței acesteia prin luarea de măsuri corective. Principala diferență constă în faptul că acțiunile corective elimină cauza unei nonconformități, în timp ce corecția se concentrează doar pe controlul nonconformității și gestionarea consecințelor directe. Acțiunea corectivă poate fi inițiată de orice angajat sau (în cazul potrivit) client, furnizor sau partener de externalizare al organizației. Acțiunea corectivă poate necesita modificări la orice document, proces sau aranjament din cadrul Sistemului de Management al Securității Informațiilor (ISMS).

## Implementarea acţiunilor corective

Acțiunea corectivă este implementată în felul următor:

|  |  |
| --- | --- |
| ***Pasul*** | ***Persoana responsabilă pentru implementare*** |
| 1. Revizuirea neconformității | Oricine are un rol în ISMS |
| 1. Determining the cause of nonconformity | Determinarea cauzei neconformității |
| 1. Identificați dacă există deja o neconformitate similară | Persoana responsabilă de zona în care a fost identificată neconformitatea |
| 1. Evaluarea necesității de a lua măsuri pentru eliminarea neconformității | Persoana responsabilă de zona în care a fost identificată neconformitatea |
| 1. Determinarea acţiunilor necesare pentru a elimina cauzele neconformităţii şi pentru a se asigura că neconformităţile nu reapar | Persoana responsabilă de zona în care a fost identificată neconformitatea |
| 1. Implementarea acțiunilor planificate | Persoana responsabilă cu punerea în aplicare, numită de persoana responsabilă |
| 1. Revizuirea măsurii în care măsura luată a dus la eliminarea cauzelor neconformității | Coordonatorul ISMS |
| 1. Informarea tuturor persoanelor în cauză că au fost puse în aplicare măsuri corective | Persoana responsabilă cu punerea în aplicare, numită de persoana responsabilă |
| 1. Efectuarea de modificări ale ISMS, dacă este necesar | Persoană responsabilă cu coordonarea ISMS |

Fiecare dintre etapele de mai sus trebuie să fie înregistrate în formularul de acțiune corectivă.

# Gestionarea înregistrărilor păstrate pe baza acestui document

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Numele înregistrării | Locația de stocare | Persoana responsabilă pentru stocare | Control pentru protecția înregistrării | Perioada de păstrare |
| Formular de acțiune corectivă | CorectiveActions\_Folder | Administratorul de Sistem Cloud | După ce toate datele au fost înregistrate, orice adăugiri noi sau editări trebuie dezactivate | 3 ani |

# Valabilitatea și managementul documentelor

Acest document este valabil începând cu 01.01.2025.

Proprietarul acestui document este Managerul de Securitate Cibernetică, care trebuie să verifice și, dacă este necesar, să actualizeze documentul cel puțin o dată pe an. La evaluarea eficacității și adecvării acestui document, trebuie luate în considerare următoarele criterii:

* numărul acțiunilor corective inițiate
* numărul acțiunilor corective incomplete
* numărul acțiunilor corective întreprinse fără a fi înregistrate într-o formă desemnată

# Anexe

* Anexa – Formular de Acțiune Corectivă

Responsabilul de Securitate a Informațiilor

Boboc Sandu

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Semnătura