

**S.R.L “CloudSentinel”**

**DOCUMENTUL ISMS SCOPE**

|  |  |
| --- | --- |
| Cod: | SCP-3301 |
| Versiune: | 0.4.1a |
| Data versiunii: | 01.04.2024 |
| Creat de: | Chihai Adrian |
| Aprobat de: | Chirita Stanislav |
| Nivelul de confidențialitate: | Confidențial |

**Istoricul modificărilor**

|  |  |  |  |
| --- | --- | --- | --- |
| **Data** | **Versiune** | **Create de** | **Descriere a schimbării** |
| 2024-04-01 | 0.1 | Chihai Adrian | Inițială: Schiță de bază a documentului ISMS Scope |
| 2024-04-02 | 0.2 | Vozian Vladimir | Adăugată secțiunea Introducere în documentul ISMS Scope |
| 2024-04-03 | 0.3 | Vozian Vladimir | Adăugată secțiunea Concluzie în documentul ISMS Scope |
| 2024-04-04 | 0.4.1a | Chirita Stanislav | Inserată bibliografia și formatare îmbunătățită în documentul ISMS Scope |

**Cuprins**

[1. Scop, domeniu de aplicare și utilizatori 3](#__RefHeading___Toc2026_998641587)

[2. Documente de referință 3](#__RefHeading___Toc2028_998641587)

[3. Definirea domeniului de aplicare al SMSI 3](#__RefHeading___Toc2030_998641587)

[3.1. Procese și servicii 4](#__RefHeading___Toc2032_998641587)

[3.2. Unități organizaționale 4](#__RefHeading___Toc2034_998641587)

[3.3. Locații 4](#__RefHeading___Toc2036_998641587)

[3.4. Rețele și infrastructură IT 4](#__RefHeading___Toc2038_998641587)

[3.5. Excluderi din domeniul de aplicare 4](#__RefHeading___Toc2040_998641587)

[4. Valabilitatea și managementul documentelor 5](#__RefHeading___Toc2042_998641587)

[5. Obiectivele 5](#__RefHeading___Toc2044_998641587)

# Scop, domeniu de aplicare și utilizatori

Scopul acestui document este de a defini clar limitele Sistemului de Management al Securității Informațiilor (ISMS) în CloudSentinel.

Acest document se aplică tuturor documentelor și activităților din cadrul ISMS.

Utilizatorii acestui document sunt membrii managementului CloudSentinel, membrii echipei de proiect care implementează ISMS-ul, precum și Chirita Stanislav și Boboc Sandu, Chihai Adrian, Vozian Vladimir.

# Documente de referință

* Standardul ISO/IEC 27001, clauza 4.3
* Planul de Proiect pentru Implementarea ISO 27001
* Procedura pentru Identificarea Cerințelor
* Legea nr. 133 din 8 iulie 2011 privind protecția datelor cu caracter personal - Această lege reglementează modul în care datele cu caracter personal trebuie gestionate și protejate. Este crucială pentru orice serviciu de cloud care procesează date cu caracter personal ale rezidenților din Moldova.
* Legea nr. 71 din 22 martie 2007 privind registrul de stat al actelor juridice - Această lege poate conține informații relevante despre gestionarea documentelor și a înregistrărilor electronice, aspecte importante pentru furnizorii de servicii cloud.
* Legea nr. 284 din 22 iulie 2004 privind comerțul electronic - Reglementează aspecte legate de comerțul electronic, inclusiv tranzacțiile online și securitatea acestora, fiind relevantă pentru serviciile cloud care susțin activitățile economice online.

# Definirea domeniului de aplicare al SMSI

Organizația trebuie să definească limitele ISMS-ului său pentru a decide ce informații dorește să protejeze. Aceste informații vor trebui protejate indiferent dacă sunt stocate, procesate sau transferate în sau în afara domeniului de aplicare al ISMS-ului. Faptul că unele informații sunt disponibile în afara domeniului de aplicare nu înseamnă că măsurile de securitate nu se aplică acestora - acest lucru înseamnă doar că responsabilitatea pentru aplicarea măsurilor de securitate va fi transferată unei terțe părți care gestionează acele informații.

Ținând cont de cerințele legale, de reglementare, contractuale și de altă natură, domeniul de aplicare al ISMS este definit astfel cum se specifică în următoarele elemente:

## Procese și servicii

* **Provisionarea și gestionarea resurselor**
* Securitatea și conformitatea
* Monitorizarea și gestionarea performanței
* Suport și asistență tehnică
* Backup și recuperare de date
* Scalabilitate și elasticitate
* Servicii de rețea
* Servicii de gestionare a identității și accesului

## Unități organizaționale

**Organizational units pentru cloud trebuie să fie clar definite și structurate pentru a asigura o gestionare eficientă a resurselor și a proceselor din cadrul infrastructurii cloud. Aceste unități organizaționale pot fi responsabile de diferite aspecte, cum ar fi gestionarea resurselor, securitatea informațiilor, suportul tehnic, conformitatea și administrarea relațiilor cu clienții. Prin organizarea corespunzătoare a acestor unități, se asigură că fiecare aspect al infrastructurii cloud este gestionat și monitorizat în mod eficient și că cerințele clienților sunt îndeplinite în mod corespunzător.**

## Locații

**Sediu, Centre de Date, Spatii de Lucru la Distanta, Locatii Utilizatori.**

## Rețele și infrastructură IT

**Rețea Internă, Rețea de Producție, Rețea de Dezvoltare și Testare, Suport Clienți Networ**

## Excluderi din domeniul de aplicare

Următoarele nu sunt incluse în domeniul de aplicare: Servicii terțe, Dispozitive deținute de Utilizator, Măsuri de Securitate Fizică.

# Valabilitatea și managementul documentelor

Acest document este valabil începând cu 2025-04-05.

Proprietarul acestui document este Boboc Sandu, care trebuie să verifice și, dacă este necesar, să actualizeze documentul cel puțin o dată pe an.

Excepții de la actualizare: În cazul unor evenimente semnificative, cum ar fi atacurile malware sau dezastrele naturale, cum ar fi cutremurele, este necesar să se revizuiască și să se actualizeze imediat documentul pentru a aborda orice modificare a profilului de risc și pentru a integra noi măsuri de securitate.

# Obiectivele

1. Asigurarea confidențialității datelor: Protejarea datelor împotriva accesului neautorizat prin implementarea controlului accesului, criptarea datelor în repaus și în tranzit și alte măsuri de securitate.
2. Integritatea datelor: Asigurarea faptului că datele nu sunt modificate. Punerea în aplicare a sumelor de control, a asemănărilor digitale și a auditurilor periodice sunt esențiale pentru menținerea integrității datelor.
3. Disponibilitatea serviciilor: Asigurarea faptului că serviciile și datele cloud sunt disponibile utilizatorilor atunci când sunt necesare. Aceasta include implementarea de soluții de rezervă, redundanța sistemului și planuri robuste de continuitate a afacerii și de recuperare în caz de dezastru.
4. Gestionarea riscurilor: Identificarea, evaluarea și atenuarea riscurilor de securitate a informațiilor într-un mediu cloud. Aceasta poate include evaluări periodice ale riscurilor și aplicarea unor măsuri de control adecvate pentru a limita riscurile la un nivel acceptabil.
5. Respectarea reglementărilor: Asigurarea faptului că serviciul cloud respectă legile și reglementările relevante privind protecția datelor, cum ar fi GDPR în Europa. Aceasta include politici și proceduri de punere în aplicare care susțin conformitatea.

Co-founders

Boboc Sandu

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

Semnătura