

**S.R.L “CloudSentinel”**

**POLITICA PRIVIND UTILIZAREA CONTROALELOR CRIPTOGRAFICE**

|  |  |
| --- | --- |
| Cod: | PRUCC-01 |
| Versiune: | 0.3.1a |
| Data versiunii: | Jun 5, 2024 |
| Creat de: | Vozian Vladimir |
| Aprobat de: | Boboc Sandu |
| Nivelul de confidențialitate: | Strict Secret |

**Istoricul modificărilor**

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Version** | **Created by** | **Description of change** |
| 2024-07-05 | 0.1.1 | Chirita Stanislav | Actualizarea secțiunii privind procedurile de gestionare a cheilor.  Introducerea unei secțiuni despre revizuirea și auditarea politicii |
| 2024-07-15 | 0.2.1 | Chihai Adrian | Adăugarea unor exemple de scenarii de utilizare a controalelor criptografice |
| 2024-07-25 | 0.3.1a | Boboc Sandu | Finalizarea și aprobarea politicii de către conducerea companiei |

**Cupris**

[1. Purpose, scope and users 3](#_Toc270023386)

[2. Reference documents 3](#_Toc270023387)

[3. Use of cryptography 3](#_Toc270023388)

[3.1. Cryptographic controls 3](#_Toc270023389)

[3.2. Cryptographic keys 3](#_Toc270023390)

[4. Managing records kept on the basis of this document 4](#_Toc270023391)

[5. Validity and document management 4](#_Toc270023392)

# Scop, domeniu de aplicare și utilizatori

Scopul acestui document este de a defini regulile pentru utilizarea controalelor criptografice, precum și regulile pentru utilizarea cheilor criptografice, în scopul protejării confidențialității, integrității, autenticității și non-repudierii informațiilor.

Acest document se aplică întregului domeniu de aplicare al Sistemului de Management al Securității Informațiilor (ISMS), adică tuturor sistemelor și informațiilor utilizate în cadrul domeniului de aplicare al ISMS.

Utilizatorii acestui document sunt angajații cu funcția de "Specialist în Securitatea Informațiilor".

# Documente de referință

* Standardul ISO/IEC 27001, clauzele A.10.1.1, A.10.1.2, A.18.1.5
* Politica de Securitate a Informațiilor
* Politica de Clasificare a Informațiilor
* **NIST Special Publication 800-53**: Acest document oferă o listă exhaustivă de controale de securitate, inclusiv cele referitoare la criptografie, care pot fi aplicate în mediile cloud.
* **ISO/IEC 27017**: Această standardă oferă ghiduri și recomandări specifice pentru securitatea informațiilor în cadrul serviciilor cloud, inclusiv pentru utilizarea criptografiei.
* **AWS Cryptography** (pentru Amazon Web Services): AWS oferă documentație extensivă despre modalitățile în care clienții săi pot utiliza și gestiona criptografia în serviciile lor cloud.

# Utilizarea criptografiei

## Controale criptografice

În conformitate cu Politica de Clasificare a Informațiilor, precum și cu obligațiile legale și contractuale, organizația trebuie să protejeze sistemele sau informațiile individuale prin intermediul următoarelor controale criptografice:

|  |  |  |  |
| --- | --- | --- | --- |
| ***Numele sistemului / tipul informației*** | ***Instrument criptografic*** | ***Algoritm de criptare*** | ***Dimensiunea cheii*** |
| Bază de date financiară | OpenSSL | AES | 256 biți |
| Comunicări email între clienți și server | GnuPG | RSA | 4096 biți |
| Stocare fișiere sensibile | Azure Key Vault | RSA | 2048 biți |

Specialist în Securitatea Cibernetică este responsabil pentru elaborarea instrucțiunilor detaliate privind utilizarea uneltelor criptografice menționate. Proprietarii activelor individuale cărora li se aplică controalele criptografice sunt responsabili pentru aplicarea corespunzătoare a controalelor criptografice individuale.

## Cheile criptografice

Specialistul în Securitatea Cibernetică este responsabil pentru prescrierea următoarelor reguli referitoare la managementul cheilor:

* generarea cheilor criptografice private și publice
* activarea și distribuția cheilor criptografice
* definirea limitei de timp pentru utilizarea cheilor și actualizarea lor regulată (în conformitate cu evaluarea riscurilor)
* arhivarea cheilor inactive necesare pentru arhivele electronice criptate
* distrugerea cheilor.

Cheile sunt gestionate de proprietarii lor conform regulilor menționate mai sus.

Cheile criptografice vor fi protejate prin (Cheile criptografice vor fi protejate prin implementarea unui set riguros de controale de securitate. Accesul la chei va fi restricționat doar la personalul autorizat, care va utiliza autentificare cu factori multipli pentru a accesa cheile sensibile. Cheile vor fi stocate într-un mediu sigur și criptat, astfel încât să fie protejate împotriva accesului neautorizat și a pierderii de date. Vor fi implementate măsuri de monitorizare și auditare pentru a detecta orice activitate suspectă sau tentativă de acces neautorizat.) În caz de pierdere, corupție sau distrugere, cheile vor fi recuperate prin (Backup și restaurare, **Recuperare de la un furnizor de servicii de gestionare a cheilor (KMS)**).

# Gestionarea înregistrărilor păstrate pe baza acestui document

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Numele înregistrării | Locația de stocare | Persoana responsabilă pentru stocare | Controale pentru protecția înregistrării | Perioada de reținere |
| Înregistrări de gestionare a cheilor | Calculatorul Administratorului de Securitate Cibernetică | Administratorul de Securitate Cibernetică | Acces restricționat la Administratorul de Securitate Cibernetică | 10 ani |
| Instrucțiuni detaliate privind utilizarea uneltelor criptografice | Intranetul companiei | Specialistul în Securitatea Cibernetică | Acces exclusiv pentru Specialistul în Securitatea Cibernetică | 3 ani |
| Reguli pentru gestionarea cheilor | Intranetul companiei | Specialistul în Securitatea Cibernetică | Acces exclusiv pentru Specialistul în Securitatea Cibernetică | 3 ani |

Doar Administratorul de Securitate Cibernetică poate acorda altor angajați acces la oricare dintre înregistrările menționate mai sus.

# Valabilitatea și managementul documentelor

Acest document este valabil începând cu 01.01.2025.

Proprietarul acestui document este Administratorul de Securitate Cibernetică, care trebuie să verifice și, dacă este necesar, să actualizeze documentul cel puțin o dată la fiecare șase luni.

La evaluarea eficacității și adecvării acestui document, trebuie luate în considerare următoarele criterii:

* numărul de incidente legate de pierdere, compromitere sau distrugere a cheilor criptografice
* numărul de sisteme la care controalele criptografice sunt aplicate în contradicție cu această politică

Responsabilul de Securitate a Informațiilor

Boboc Sandu

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

Semnătura