Politica de securitate a reţelelor şi sistemelor informatice care asigură furnizarea serviciilor esenţiale	Document Control Referinta: NIS PONIS Versiune: 1.0 Data: Page: 1 of 5

Politica de securitate a reţelelor şi sistemelor informatice care asigură furnizarea serviciilor esenţiale este aprobata in data de (introduceti data) si este disponibilă publicului din data de (introduceti data)in interactiunile esentiale si canalele de comunicare.

OSE, este permanent preocupată de asigurarea nivelului optim de securitate informaţională prin implementarea unui sistem de management al securităţii informaţiei în conformitate cu standardul ISO27001:2018 dar si in conformitate cu prevederile Legii nr. 362/2018 privind asigurarea unui nivel comun ridicat de securitate a reţelelor şi sistemelor informatice.
Informaţia este printre cele mai importante valori ale OSE, de aceea securitatea informaţiei şi a tehnologiei care facilitează utilizarea acesteia este o responsabilitate împărtăşită de tot personalul organizaţiei.
Serviciile esentiale furnizate de catre OSE sunt importante pentru viata umana si OSE depune eforturi sustinute pentru mentinerea unui nivel adecvat de securitate al informatiei cat si a sistemelor informationale care sustin aceste servicii esentiale.
Conducerea OSE este responsabilă pentru implementarea regulilor şi tehnicilor adecvate cu privire la asigurarea securităţii informaţiei pentru a menţine obiectivele generale de securitate:

- Asigurare a confidenţialităţii, integrităţii şi disponibilităţii informaţiilor.
- Implementare, menţinere şi îmbunătăţire a unui sistemului de management al securităţii informaţiei conform prevederilor legii Legii nr. 362/2018.
- Asigurarea securităţii proceselor de afaceri din cadrul organizaţiei.
- Obiectivele generale de securitate informaţională vor sta la baza obiectivelor specifice, care se vor realiza în conformitate cu programul de obiective al companiei.

Prin implementarea Sistemului de management al securităţii informaţiei, conducerea OSE se angajează pentru:

- Satisfacerea cerinţelor clienţilor, cerinţelor legale şi de reglementare;
- Menţinerea unui cadru organizatoric adecvat, capabil să asigure realizarea politicii şi obiectivelor în domeniul securităţii informaţiei;
- Asigurarea resurselor necesare implementării si menţinerii sistemului de management al securităţii informaţiei;
- Analiza anuală a eficientei i îmbunătăţirea continuă a eficacităţii Sistemului de management al securităţii informaţiei;
- Protejarea sistemelor informaţionale administrate de întreprindere de orice ameninţare la adresa securităţii informaţionale atât din interiorul, cât şi din exteriorul organizaţiei;
- Menţinerea riscurilor informaţionale la nivelul acceptat de conducerea organizaţiei;
- Menţinerea unui sistem eficient de instruire permanentă şi continuă a angajaţilor şi clienţilor organizaţiei în domeniul securităţii informaţiei;
- Stabilirea unor măsuri adecvate pentru tratarea şi investigarea incidentelor actuale sau potenţiale de securitate, astfel încât sa se asigure un procedeu de răspuns în timp util şi să se prevină reapariţia acestora;
- Stabilirea unor planuri pentru minimalizarea impactului asupra clienţilor şi pentru reluarea activităţi în cel mai scurt timp în eventualitatea unei întreruperi majore ale activităţii organizaţiei;
- Aplicarea de măsuri disciplinare asupra oricărui angajat care încalcă sau nu respectă politica de securitate;
- Raportarea organelor competente privind acţiunile, care contravin legislaţiei în vigoare. Sistemul de management al securităţii informaţiei va fi monitorizat prin audituri interne şi analizat periodic de managementul de vârf al OSE pentru a se asigura că prezenta politică de securitate se implementează în cadrul organizaţiei.

Conducerea OSE se asigură că cerinţele Sistemului de management al securităţii informaţiei sunt cunoscute, însuşite şi aplicate de întreg personalul organizaţiei.
Politica şi angajamentul managementului în domeniul securităţii informaţiei sunt comunicate în cadrul organizaţiei şi sunt disponibile pentru toţi angajaţii şi public.
Prezenta politică a fost aprobată de către conducerea şi va fi revizuită anual.

Director General
OSE

Data: 07.09.2020

1. **Alte Considerente ale Politicii de Securitate.**
2. **Introducere**

În acord cu prevederile din prezentul document, Resursele Informatice şi de Comunicaţii (RIC) puse la dispozitie şi administrate de OSE sunt bunuri strategice care trebuie administrate ca resurse ale organizatiei.
Compromiterea securităţii acestor resurse poate afecta capacitatea OSE de a oferi servicii esentiale societatii, conform obiectului de activitate si poate conduce la fraude sau distrugerea datelor, la violarea clauzelor contractuale, divulgarea secretelor, la afectarea credibilităţii organizatiei în faţa partenerilor si a clientilor săi.

Această politică este stabilită astfel încât:

- Să fie în conformitate cu statutul, regulamentele, legile şi alte documente oficiale în vigoare privind administrarea resurselor informatice;
- Să stabilească practici prudente şi acceptabile privind utilizarea Resurselor Informatice şi de Comunicaţii ale OSE ;
- Să instruiască utilizatorii care au dreptul de folosire a Resurselor Informatice şi de Comunicaţii privind responsabilităţile asociate unei astfel de utilizări.

3. **Scop**

Politica de securitate a Resurselor Informatice şi de Comunicaţii are ca scop asigurarea integrităţii, confidenţialităţii şi disponibilităţii informatiei (CID) cat si a sistemelor informationale si informatice care suporta crearea, utilizarea, schimbul si decomisionarea acesteia, in ciclul de viata specific.

- Confidenţialitatea se referă la protecţia datelor împotriva accesului neautorizat. Angajatii societatii răspund personal de confidenţialitatea datelor încredinţate prin procedurile de acces la Resursele Informatice şi de Comunicaţii.
- Integritatea se referă la măsurile şi procedurile utilizate pentru protecţia datelor împotriva modificărilor sau distrugerii neautorizate.
- Disponibilitatea se asigură prin funcţionarea continuă a tuturor componentelor Resurselor Informatice şi de Comunicaţii. Diverse aplicaţii au nevoie de nivele diferite de disponibilitate în funcţie de impactul sau daunele produse ca urmare a nefuncţionării corespunzătoare a Resurselor Informatice şi de Comunicaţii.

Politica de securitate are ca scop, de asemenea, stabilirea cadrului necesar pentru elaborarea regulamentelor şi procedurilor de securitate. Acestea sunt obligatorii pentru toţi utilizatorii Resurselor Informatice şi de Comunicaţii.

4. **Domeniu de aplicare**

Politica de securitate a Resurselor Informatice şi de Comunicaţii ale OSE se aplică nediscriminatoriu tuturor persoanelor cărora li s-a permis accesul la orice resursă informatică şi de comunicaţii a organizatiei.
Următoarele entităţi şi utilizatori sunt vizaţi în mod distinct de prevederile Politicii:

- Angajaţii cu contract de muncă pe perioadă determinată sau nedeterminată care au acces la sistemul informaţional şi de comunicaţii;
- Colaboratorii OSE care au acces la Resursele Informatice şi de Comunicaţii;
- Furnizorii OSE care au acces la Resursele Informatice şi de Comunicaţii;
- Clientii OSE care au acces la Resursele Informatice si de Comunicatii;
- Alte persoane, entităţi sau organizaţii care au acces la Resursele Informatice şi de Comunicaţii.

[redacted]

[redacted]

[redacted]

[redacted]

Sfarsitul documentului.