1. Scop

Scopul PRECDI este să asigure protejarea adecvată a informaţiilor prin setarea unor nivele de secretizare.
Acest document se aplică tuturor tipurilor de informaţii, indiferent de format - documente tipărite sau electronice, aplicaţii şi baze de date, cunoştinţele oamenilor etc. Pentru identificarea ameninţărilor, vulnerabilităţilor şi riscurilor sunt identificate toate activele informationale ale organizatiei, care se materializează printr-o listă.
Utilizatorii acestui document sunt toţi angajaţii organizatiei.

2. Responsabilitati

2.1 Fiecare angajat care este detinatorul activului informational este responsabil de clasificarea si etichetarea informatiilor.

2.2 este responsabil cu asigurarea si administrarea mijloacelor technologice specifice tehnologiei informatiei sau a masurilor tehnice de securitate informationala, care sa ajute detinatorul activului informational sau persoanele autorizate de catre acestia, sa

clasifice si sa eticheteze informatiile,
acceseze si sa proceseze suportul informational sau de catre persoanele autorizate de catre acestia.

2.3 Managerul de securitate a informaţiilor este responsabil sa verifice ca masurile tehnice specifice pentru protectia informatiilor sunt luate, sa efectueze reevaluari ale nivelului de risc asupra riscului activului informational.

3. Clasificarea informaţiilor

3.1 Criterii de clasificare

Nivelul de confidenţialitate este stabilit în baza următoarelor criterii:

- valoarea informaţiilor - pe baza impactului evaluat în cadrul evaluării riscurilor
- sensibilitatea şi gravitatea informaţiilor - pe baza celui mai ridicat nivel de risc calculat pentru fiecare informaţie în cadrul evaluării riscurilor
- obligaţii legale şi contractuale

3.2 Niveluri de confidenţialitate

Toate informaţiile trebuie clasificate pe niveluri de confidenţialitate.

Nivel de confidenţialitate	Etichete	Criterii de clasificare	Restricţii de acces
Informaţii publice	(neetichetate)	Publicarea informaţiilor nu poate dăuna organizaţiei în niciun fel	Informaţii disponibile publicului
De uz intern	DE UZ INTERN	Accesul neautorizat la aceste informaţii poate cauza daune minore şi/sau deranj organizaţiei	Informaţiile sunt disponibile tuturor angajaţilor şi unor anumiţi terţi
Restricţionate	RESTRICŢIONATE	Accesul neautorizat la informaţii poate dăuna în mod considerabil afacerii şi/sau reputaţiei organizaţiei	Informaţiile sunt disponibile doar unui anumit grup de angajaţi şi terţi autorizaţi
Confidenţiale	CONFIDENŢIALE	Accesul neautorizat la informaţii poate cauza daune catastrofale (ireparabile) afacerii şi/sau reputaţiei organizaţiei	Informaţiile sunt disponibile doar persoanelor din cadrul organizaţiei

Regula de bază este utilizarea celui mai scăzut nivel de confidenţialitate care asigură un nivel adecvat de protecţie, pentru a evita costurile inutile.

3.3 Listă de persoane autorizate

Informaţiile clasificate ca fiind „restricţionate" şi „confidenţiale" trebuie însoţite de o Listă a persoanelor autorizate, în care responsabilul specifică numele sau funcţiile persoanelor cu drept de ale accesa.

Aceeaşi regulă se aplică nivelului de confidenţialitate „uz intern", dacă persoane din afara organizaţiei vor avea acces la acest document.

3.4 Reclasificare

Responsabilii trebuie să revizuiască nivelul de confidenţialitate al activelor lor informaţionale annual şi să evalueze posibilitatea schimbării acestuia. Dacă este posibil, nivelul de confidenţialitate trebuie redus.

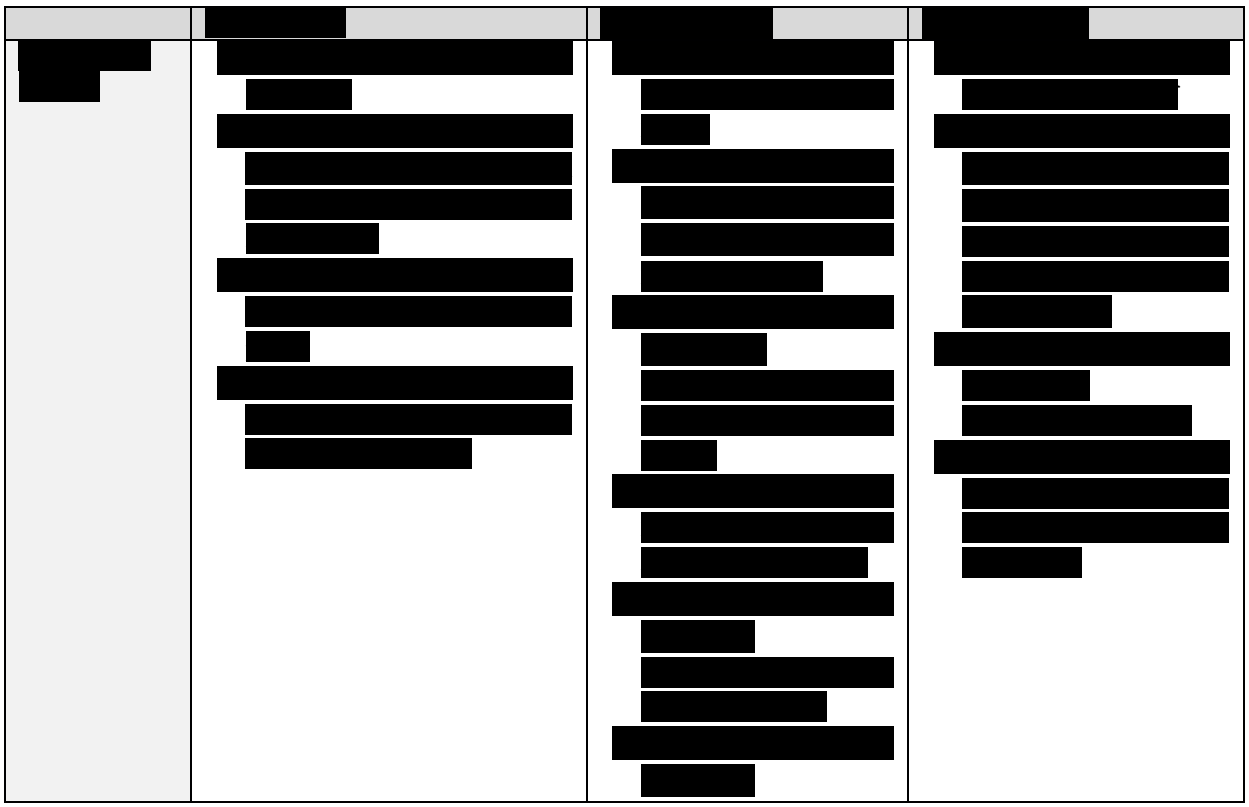
4. Etichetarea informaţiilor

Nivelurile de confidenţialitate sunt etichetate astfel:

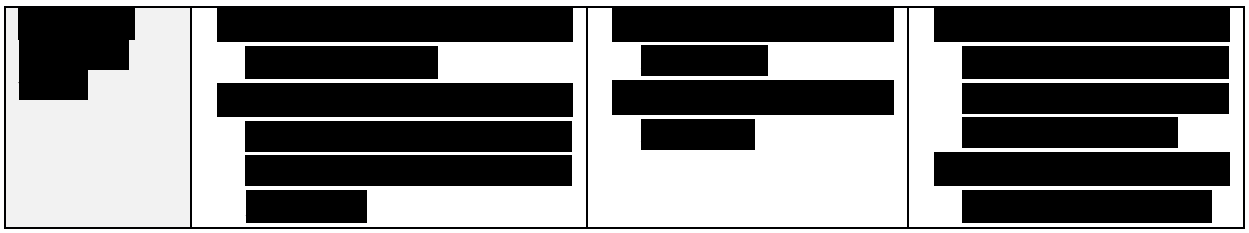
- **documente tipărite –** nivelul de confidenţialitate este indicat în colţul dreapta-sus al fiecărei pagini; este indicat şi pe copertă sau pe plicul în care se află documentul, cât şi pe dosarul în care este arhivat documentul.
- **documente electronice –** nivelul de confidenţialitate este indicat în colţul dreapta-sus al fiecărei pagini.
- **sisteme de informaţii –** nivelul de confidenţialitate în aplicaţii şi baze de date trebuie indicat pe monitorul de acces sistem, cât şi în colţul dreapta-sus al fiecărui ecran consecutiv care afişează informaţiile confidenţiale
- **e-mail –** nivelul de confidenţialitate este indicat în primul rând al conţinutului sau in proprietile emailului
- **medii de stocare electronică** (CD/DVD, carduri de memorie etc.) - nivelul de confidenţialitate trebuie indicat pe suprafaţa acestui mediu
- **informaţii transmise verbal –** nivelul de confidenţialitate al informaţiilor confidenţiale ce vor fi transmise faţă în faţă, la telefon sau prin alte mijloace de comunicare trebuie comunicat înainte de informaţie.

5. Administrarea informaţiilor confidenţiale

Toate persoanele care accesează informaţii clasificate trebuie să urmeze regulile din tabelul următor.
Departamentul de resurse umane trebuie să ia măsuri disciplinare ori de câte ori se încalcă regulile sau dacă informaţiile sunt comunicate unor persoane neautorizate.
Activele informaţionale pot fi îndepărtate din sediu doar după obţinerea unei autorizaţii în acest sens.
Metoda de ştergere sigură şi distrugere a suporturilor media este prevăzută în **Politica de retenţia datelor.**



[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]



Tabel cu Clasificarea informatiei in organizatie.

Nr	Descriere	Emitent / responsabil	Grad de confidenţialitate	Grad de acces	Drepturi	Grup de acces
1.						
2.						
3.						
4.						
5.						
6.						
7.						
8.						
9.						
10.						
11.						
12.						
13.						
14.						
15.						
16.						
17.						
18.						
19.						
20.						
21.						
22.						
23.						
24.						
25.						
26.						
27.						
28.						
29.						

Versiune	Data	Creat	Revizuit	Aprobat	Descriere
1.0	02.2022	Consultant		Management	Versiunea iniţială a NIS PRECDI