

Politica privind accesul la date

1. Politica privind accesul la date

1.1. Scopul

Scopul acestei politici este de a menține un nivel de adecvat de securitate pentru a proteja datele cu caracter personal ale instituției și sistemele de informații de acces neautorizat. Această politică definește regulile necesare pentru a asigura această protecție și pentru a asigura o funcționare sigură și fiabilă a sistemelor informatice a instituției.

1.2. Politica

Numai utilizatorii autorizați au acces la sistemele informatice, iar utilizatorii sunt limitați la aplicații specifice, documentate și aprobate, cu diferite niveluri de acces. Accesul la sistemul informatic se realizează pe baza unui ID unic pentru fiecare utilizator.

1.2.1 Cui se aplică politica?

Această politică se aplică tuturor angajaților instituției, precum și tuturor contractanților, consultanților și angajaților temporari.

Angajații care încalcă în mod deliberat această politică vor fi supuși acțiunilor disciplinare prevăzute de Codul Muncii.

1.2.2 Sistemele afectate

Această politică se aplică tuturor calculatoarelor, dispozitivelor și sistemelor informatice deținute sau operate de instituție.

În mod similar, această politică se aplică tuturor platformelor (sistemelor de operare) și tuturor sistemelor de aplicații.

1.2.3 Autentificarea:

Orice utilizator (de la distanță sau intern), care trebuie să acceseze rețelele și sistemele Informatice ale instituției, **trebuie să treacă prin procesul de autentificare.**

Nivelul de autentificare trebuie să fie ridicat.

Autentificarea va include, dar nu se va limita la:

- Deconectarea automată;
- Un identificator unic pentru fiecare utilizator

Cel puțin una dintre următoarele: (1) Verificare în doi factori (pași); (2) Token;

Parolele utilizate sunt șiruri de caractere, adecvate din punct de vedere al securității ca lungime și compoziție, conținând majuscule și caractere speciale. Parolele nu sunt afișate pe monitor. Acestea sunt schimbate periodic, cel puțin o dată la două luni. Schimbarea periodică a parolilor se face numai de către utilizatori autorizați.

1.2.4 Notificare

O notificare preliminară care atrage atenția că sistemul este o rețea privată și că acei utilizatori neautorizați trebuie să se deconecteze imediat va fi afișată imediat înainte de logarea la sistem.

1.2.5 Aprobarea accesului

Accesul la sistem nu va fi acordat niciunui utilizator fără aprobarea corespunzătoare. Accesul utilizatorilor trebuie imediat revocat în cazul în care relația de muncă sau de colaborare cu persoana a încetat. Dacă persoana este transferată către alt sector, privilegiile trebuie modificate în mod corespunzător.

1.2.6 Accesul la informații

- Mijloacele de autentificare în sistem (username, parolă etc) sunt proprietatea fiecărui angajat și el este singurul responsabil de a nu divulga aceste informații.
- Este strict interzisă utilizarea credențialelor altui angajat.
- Fiecare angajat va fi responsabil să mențină securitatea oricărei informații, și în special informațiilor personale (datelor cu caracter personal) și să le protejeze de acces neautorizat (vizualizare, alterare, furt sau distrugere).
- Trebuie obținută aprobarea din partea proprietarului informației înainte de crearea, modificarea sau ștergerea unei autorizații de acces.
- Este strict interzisă copierea de fișiere electronice, iar angajatul care încalcă această regulă va fi supus sancțiunilor disciplinare, inclusiv desfacerea contractului de muncă.
- Pentru copierea fișierelor electronice, Instituția își rezervă dreptul de a depune plângere penală împotriva angajatului și de a-l acționa pe acesta la instanțele civile pentru acoperirea oricărui prejudiciu adus instituției.
- Este interzisă navigarea prin fișierele personale sau conturile altor angajați, cu excepția cazului în care acest lucru a fost aprobat în prealabil.
- Programatorii care vor dezvolta sisteme IT nu vor avea acces la date cu caracter personal, decât dacă acestea au fost anonimizate complet.
- Personalul care asigură suportul tehnic nu va avea acces la date cu caracter personal, decât în situații excepționale și, în toate cazurile, cu respectarea tuturor obligațiilor impuse de Regulamentul (EU) 679/2016 persoanelor împuternicite și, în special, existența unor clauze contractuale exprese privind protecția datelor.

1.2.7 Accesul la sistem

- Notarea sau stocarea parolelor pe orice suport fizic este strict interzisă.
- Sistemul trebuie blocat ori de câte ori angajatul părăsește biroul sau nu utilizează calculatorul.
- După terminarea programului, calculatorul va fi închis. De asemenea, se va verifica faptul că închiderea s-a finalizat cu succes și fără erori.
- Este strict interzisă utilizarea „*Print screen-ului*” (prin folosirea tastei print screen sau a altor procedee) sau prin fotografierea monitorului cu telefonul pentru a salva/imprima datele cu caracter personal existente pe monitor.
- Listarea documentelor ce conțin date cu caracter personal se va realiza doar de către utilizatorii autorizați sau cu aprobarea scrisă și prealabilă a conducerii.

2. Consecințe

Nerespectarea prezentei Politici de către angajații instituției sau alți colaboratori externi poate conduce către sancțiuni disciplinare (inclusiv încetarea contractului de muncă), rezilierea contractelor și, în funcție de circumstanțe, acționarea în instanță pentru recuperarea integrală a prejudiciilor aduse Instituției ca urmare a nerespectării prezentei Politici. Când există suspiciunea unor activități ilegale (cum ar fi, exemplificativ, sustragerea documentelor, copierea, distribuirea, transferul bazelor de date), Instituția va denunța activitatea infracțională organelor legii pentru tragerea la răspundere penală a făptuitorului.

Prezenta Politică va fi adusă de către conducerea Instituției la cunoștința tuturor angajaților, colaboratorilor sau a altor terți.