4. Procedura cu privire la managementul incidentelor de securitate a informaţiei

4.1. PREVEDERI GENERALE

4.1.1. Obiectul Instrucţiunii

4.1.2. Domeniul de aplicare

4.1.3. Scopul Instrucțiunii

4.2. GLOSAR

4.3. PRINCIPIILE DE BAZĂ

4.3.1. Obiectivul

4.3.2. Prevederile

4.3.3. Accesului privilegiat

4.3.4. Revizuiri periodice

4.3.5. Utilizatorii

4.4 IDENTIFICAREA

4.4.1. Principii generale

4.4.2. Formatul identificatorului

4.4.3. Gestionarea identificatorilor

4.4.4. Identificatori generici

4.4.5. Controlul identificatorilor

4.5. AUTENTIFICAREA

4.5.1. Principii generale

4.5.2. Parola – Principii generale

4.5.3. Cerințele de bază față de parole

4.5.4. Robustețea parolei

4.5.5. Parola inițială

4.5.6. Introducerea parolei

4.5.7. Schimbarea parolei

4.5.8. Înregistrarea/Stocarea parolelor

4.5.9. Parolele asociate cu identificatorii tehnici/administrativi

4.5.10. Suportul tehnic

4.5.11. Controlul parolelor

4.6. AUTORIZAREA

4.6.1. Principii generale

4.6.2. Definirea drepturilor de acces

4.6.3. Administrarea drepturilor de acces

4.6.4. Acordarea drepturilor de acces

4.6.5. Retragerea drepturilor de acces

4.6.6. Administrarea drepturi de acces privilegiate

4.6.7. Delegarea drepturilor de acces

4.6.8. Controlul drepturilor de acces

4.7. TRASABILITATEA

4.8. MODUL DE SELECTARE AL APLICAȚIILOR

4.9. MĂSURI ADĂUGĂTOARE DE SECURITATE

4.10. ADMINISTRAREA EXCEPȚIILOR

4.11. RESPONSABILITĂȚI

4.12. CONTROL PERMANENT

4.12.1. Controale operaționale

4.12.2. Supravegherea managerială

4.13. PREVEDERI FINALE

Content info

**4.1. PREVEDERI GENERALE**

Prezenta Instrucţiune este elaborată în corespundere cu bunele practici referitor la modul de accesare a informaţiei în sistemele și resursele informaţionale ale Companiei.

Implementarea sistemelor de administrare a autorizărilor şi sistemelor de autentificare este una din măsurile care vor contribui la îmbunătăţirea securităţii informaţionale prin:

• Asigurarea disponibilităţii, integrităţii şi confidenţialităţii resurselor informaţionale;

• Limitarea riscurilor de eroare sau de intenţii de rea voinţă: fraude; divulgării datelor confidenţiale; deconectării sistemelor; ştergerii sau sustragerii informaţiei; şi în termeni generali, a riscurilor de acces neautorizat;

• Acordarea asistenţei în căutarea şi analiza dovezilor şi stabilirea certă a responsabilităţii pentru acţiunile efectuate cu resursele informaţionale, prin utilizarea LOG-urilor de acces.

**4.1.1. Obiectul Instrucţiunii**

Instrucţiunea defineşte normele de acces la informaţia, care circulă/ este prelucrată/ este stocată în sistemele informaţionale ale Companiei; stabileşte modalitatea de acordare/modificare/retragere a drepturilor de acces.

Instrucţiunea descrie principiile de securitate şi regulile care se aplică în vederea:

• organizării procesului de accesare a sistemelor informaţionale;

• modalitatea de alegere şi de păstrare a factorilor de autentificare (parole).

• implementării recomandărilor de securitate care urmează a fi aplicate de către fiecare utilizator al sistemului informaţional;

**4.1.2. Domeniul de aplicare**

Prezenta Instrucţiune se aplică şi este obligatorie pentru toate subdiviziunile Companiei. Prevederile prezentei Instrucţiuni, inclusiv cerințele pentru parole, sunt aplicabile pentru aplicaţiile și sistemele informatice gestionate de Companiei.

Securitatea identificării şi autentificării clienţilor companiei nu este prevăzută de această Instrucţiune. Această Instrucţiune nu se răsfrânge asupra: administrării autorizării accesului la resursele fizice, registrelor datelor de identificare a utilizatorilor şi sistemelor de autentificare a accesului fizic.

**4.1.3. Scopul Instrucțiunii**

Scopul Instrucţiunii este de a stabili modalitatea de accesare a informaţiilor în sistemele informaţionale ale Companiei.

**4.2. GLOSAR**

În prezenta Instrucţiune se utilizează următoarele noţiuni:

|  |  |
| --- | --- |
| Accesibilitatea informaţiei | Asigurarea unui nivel suficient de accesibilitate pentru resursele și sistemele informaţionale ale companiei |
| Administrator SI | Utilizatorul autorizat să efectueze administrarea sistemului informaţional (echipament de reţea, calculator, server, etc.), adică persoana care poartă răspundere pentru integritatea sistemului şi funcţionarea lui corespunzătoare. |
| Administrator drepturi  de acces | Conducătorul subdiviziunii (Departament), care defineşte drepturile de acces pentru subalternii săi.. |
| Help Desk | Serviciul Help Desk din cadrul Departamentului Tehnologii Informaţionale |
| Administrator delegat | Angajat al Departamentului tehnologii informaţionale, care pune în aplicare un program/sistem/aplicaţie, implementează şi supraveghează drepturile de acces |
| Aplicaţia (informatică) | Set de programe (software), fişiere şi proceduri elaborate şi organizate pentru procesarea automată a funcţiilor prestabilite. |
| Autentificare | Confirmarea identităţii unui utilizator al sistemului informaţional |
| Identificator/ identificare | Cod care permite constatarea identităţii unui utilizator dintr-un număr de persoane prealabil înregistrate în aplicație |
| Cod confidenţial (parolă) | Serie de caractere utilizate pentru autentificarea utilizatorului, astfel încât acesta să se conecteze la un sistem informaţional, la unul sau la mai multe resurse informaționale. |
| Confidenţialitate | Proprietatea datelor cu privire la difuzarea, obţinerea, menţinerea acestora şi la atribuirea drepturilor de acces unor persoane autorizate |
| Dreptul de acces | Autorizarea de utilizare a unei resurse (aplicaţii, date, resurse informatice) conform unui mod determinat (consultare, actualizare, procesare) |
| Dreptul de acces privilegiat | Autorizarea de utilizare manageriale sau administrative a unei resurse (aplicaţii, date, resurse informatice) |
| Incident de securitate | Înseamnă un incident asociat cu securitatea sistemelor informaţionale, marcat de unul sau mai multe evenimente nedorite sau neaşteptate, care afectează securitatea sistemului informaţional, care prezintă pericol pentru operaţiunile asociate cu activităţile companiei şi ameninţă securitatea sistemului informaţional. Acesta declanşează procedura de analiză şi măsurile corective conform „Procedura cu privire la managementul incidentelor de securitate a informaţiei” |
| Integritate | Garanţia de nedeteriorare a datelor sau a programelor în timpul transportării, stocării sau procesării. |
| Nivelul de securitate | Reprezintă vulnerabilitatea unui nod informațional |
| Interfaţare de aplicaţii | Conectarea aplicaţiilor între ele, pentru schimb de date |
| Nod informaţional | Nod al sistemului informaţional (de ex. staţie de lucru) |
| Non repudierea | Imposibilitatea negării unor acţiuni săvârşite |
| Utilizator | Persoană, care are acces la sistemele și/sau resursele informatice ale companiei |
| Resursă | O resursă înseamnă un activ (în sensul contabil al noţiunii) în cadrul sistemelor informaţionale, mai ales care se referă la securitatea lor (securitatea informaţiei, proceselor, componentelor de aplicaţii, infrastructură tehnică). O resursă sensibilă reprezintă un activ care are o anumită valoare pentru întreprindere. Stabilirea sensibilităţii resursei este sarcina subdiviziunii responsabile. |
| Drepturi individuale | Prezintă drepturi de acces la sistemul informațional conform rolului utilizatorului (funcției deținute). |
| Privilegii | Prezintă Managementul riscurilor asociate cu o resursă permite generarea cerinţelor de securitate aferente acesteia. Permisiuni de a utiliza/modifica |
| Business owner | Deținătorul resurselor informatice, persoană cu funcție de răspundere, în competențele cui intră luarea deciziilor aferente resurselor respective și validarea riscurilor aferente. |
| SSI | Secția Securitate Informațională |
| IT | Departamentul Tehnologii Informaționale |
| DPO | Departamentul Proiecte si Organizare |
| HR | Departamentul Resurse Umane |
| COO | Chief Operating Officer |

**4.3. PRINCIPIILE DE BAZĂ**

**4.3.1.** Obiectivul este de a obţine un control al accesului care să conducă la:

identificare autentică unică al utilizatorului;

gestionare unificată a autorizaţiilor.

Prevederile prezentei Instrucţiuni se aplică cât aplicaţiilor/sistemelor noi, atât şi versiunilor noi ale aplicațiilor/sistemelor existente.

**4.3.2**.În cazul accesului privilegiat al administratorilor delegați, accesului de mentenanță sau accesului din exterior măsurile de securitate trebuie să fie întărite. Accesul extern la resursele informaţionale ale companiei se va efectua prin utilizarea echipamentului şi a tehnicilor, care asigură securitatea maximală a transferului datelor.

**4.3.4**. Toate sistemele/aplicaţiile sensibile trebuie să fie supuse revizuirii periodice (cel puţin o dată la 12 luni). La dispoziţia conducerii companiei acelaşi proces poate fi implementat şi pentru resursele ne sensibile.

**4.3.5**.Utilizatorii resurselor informaționale ale companiei trebuie să fie periodic informați despre prevederile curentei instrucțiuni precum și bunele practice în domeniu.

**4.4 IDENTIFICAREA**

**4.4.1. Principii generale**

**4.4.1. Principii generale**

**4.4.1.1.** Utilizatorii resurselor informaționale sunt identificați în mod individual, după criterii unice și după anumite norme. Orice utilizator trebuie să aibă un identificator unic. Identificarea este cerută de către resursele informaționale în mod automat, fiind confirmată de un factor de autentificare.

**4. 4.1.2.** Ca excepție de la regula de identificare unică, un angajat poate dispune simultan de o altă identificare în vederea:

* Pregătirii pentru verificarea abilităților, care vor trebui utilizate în cadrul unei noi aplicații;
* Posibilității de gestionare a extinderii unei misiuni funcționale spre o unitate, alta decât cea de atașare.

**4. 4.1.3.** Trebuie să existe posibilitatea de a face legătură dintre identificator și numărul de tabel atribuit fiecărui angajat în aplicația de gestiune a resurselor umane, pentru ca utilizatorul căruia i-a fost atribuit identificatorul să poată fi identificat și responsabilizat.

**4. 4.1.4.** Toți utilizatorii externi anonimi (de ex. persoanele ce acordă mentenanță la distanță) trebuie să fie asociați cu identificatori specific pentru fiecare contractant extern. Evidența acestor identificatori va fi efectuată de către SSI. Regulile privind utilizarea acestor identificatori trebuie să fie prevăzute în contractele de colaborare.

**4. 4.1.5.** Identificatorii asociați cu servicii temporare (prestări de servicii, stagiari, etc) trebuie să aibă o data fixă de expirare ce se stabilește până la creare utilizatorului. După data de expirare identificatorul va deveni inactiv (acest proces trebuie să fie automatizat, dacă nu este posibil atunci va fi efectuat manual).

**4. 4.1.6.** Identificatorii nu pot fi atribuiți sau reutilizați de alți angajați cu scopul de a fi menținută în timp pista de audit (să există certitudinea privind angajatul ce a efectuat o anumită operațiune).

**4. 4.1.7.** Strict se interzice utilizarea neautorizată a identificatorului și a factorului de autentificare corespunzător de către terțele persoane.

**4.4.2. Formatul identificatorului**

**4.4.2.1.** În dependență de posibilitățile resursei informaționale identificatorul poate fi diferit de regula generală, care presupune următoarele:

|  |  |
| --- | --- |
| **Structură:** | „Prenume.Nume” al angajatului |
| **Lungime:** | Minimum 6 caractere (de la „A” la „Z”, de la „a” la „z”). |
| **Controlul asupra structurii:** | Obligatorie la creare: dacă sunt necesare literele mici, majusculele vor fi interzise |
| **Reguli de codificare pentru Contractori externi :** | „X” urmat de 6 poziţii numerice atribuite prin înscrierea în Baza de contractori externi. Fiecare identificator neputând fi folosit decât de un singur contractor. |

**4.4.2.2.** În cazul când numele şi prenumele angajatului coincide cu unul existent în resursa informațională, numele sau prenumele lui se modifică în aşa mod ca să fie unice.

**4.4.3. Gestionarea identificatorilor**

**4.4.3.1.** Fiecare etapă din ciclul de viață a unui identificator (de la înregistrarea inițială a unui utilizator nou în cadrul unei resurse informaționale, schimbare de funcție, până la ștergerea identificatorului după încetarea raportului de muncă cu angajatul sau contractului cu furnizorul extern) trebuie să fie formalizate.

**4.4.3.2.** Help Desk-ului/Administratorului delegat îi revin următoarele funcții:

* Crearea și lichidarea identificatorilor
* Dezactivarea, reactivarea identificatorilor

**4.4.3.3.** În Active Directory identificatorii se creează/lichidează automat în baza informației din aplicația de gestiune a resurselor umane , în celelalte resurse informaționale identificatorii se creează/lichidează in conformitate cu fluxul stabilit pentru autorizarea drepturilor de acces descris în punctele 6.4 și 6.5.

**4.4.3.4.** Identificarea autentificată reușită este o condiție necesară pentru realizarea accesului la sistemul informațional, dar totuși această măsură nu este suficientă. Este necesar ca identificatorul să fie activ:

* Identificarea și autentificarea trebuie să asigure că doar utilizatorii autorizați pot accesa resursele informaționale
* Sistemul trebuie să prevină accesul dacă identificatorul este declarat inactiv de către Administratorul utilizatorilor (de ex. lipsa angajatului fie din motiv de boală, fie din motivul concediului anual, etc.).
* Identificatorul poate fi dezactivat sau considerat ca inactiv de către sistem dacă acesta prevede unele date de limitare a accesului (data de sosire prevăzută, data de plecare prevăzută).
* Accesul poate fi suspendat de către sistem:

– Sistemul va memoriza cauza suspendării accesului.

– Drepturile de acces vor fi suspendate după un număr definit (de obicei 3-5) de încercări consecutive eronate de introducere a parolei. Sistemul duce evidenta tentativelor eșuate.

– Contorul nu va fi repus la zero decât în cazul când se va utiliza parola corectă (după una sau două tentative eronate) sau se va reinițializa de către Help Desk.

– Accesul este suspendat de către sistem după expirarea termenului de grație.

– Accesul este suspendat de către sistem în cazul absenței oficiale a angajatului de la locul de muncă (de ex. concediu), în baza informației de la HR

**4.4.3.5.** IT va duce evidența identificatorilor tehnici și administrativi. Registrul identificatorilor tehnici și administrativi va cuprinde: codul identificatorului, numele sistemului, identificatorul și data sigilării plicului cu parolă. Cel puțin o dată pe an, persoanele responsabile din IT vor efectua reconcilierea dintre Registrul identificatorilor/tehnici și utilizatorii tehnici/administrativi de facto. Anomaliile vor fi raportate către COO, SSI și înlăturate.

**4.4.3.6.** Identificatorii ce sunt inactivi mai mult de 90 de zile vor fi blocați și ulterior șterși din sistemele informaționale ale companiei, după coordonare cu Administratorul drepturilor de acces