

VIMERCATI EAST EUROPE SRL	PROCEDURA DE LUCRU: CONTROLUL ACCESULUI IN SISTEMUL INFORMATIC	Pagina 1 din 7
	Cod document: PL-SMSI-08	Versiunea 1.0

DATA	22.07.2018	SEMNATURA
ELABORAT	CONSULTANT – LIVIU MINCIUNA	
VERIFICAT	RPD - COJOCARU ROXANA	
APROBAT	DIRECTOR GENERAL – CONSTANTIN HUMA	

1. SCOP

Procedura are drept scop stabilirea de masuri pentru controlul accesului la informatiile si procesele VIMERCATI EAST EUROPE SRL si prevenirea accesului neautorizat la sistemul informatic.

2. DOMENIUL DE APLICARE

Procedura delimiteaza cadrul si drepturile de acces pentru toate mijloacele de procesare a informatiilor (MPI) din VIMERCATI EAST EUROPE SRL.

3. DOCUMENTE DE REFERINTA

- ISO/IEC 27001:2013 - Tehnologia informatiei - Tehnici de securitate - Sisteme de management pentru securitatea informatiilor - Cerinte
- ISO/IEC 27002:2013 - Tehnologia informației - Tehnici de securitate - Cod de practica pentru managementul securitatii informatiilor
- REGULAMENTULUI nr. 679 din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor).

4. DEFINIȚII SI PRESCURTARI

4.1. Definitii

N/A

4.2. Prescurtari

- **AS:** Administrator de Sistem
- **CEO:** Chief Executive Officer (Director General)
- **RPD:** Responsabil Protectia Datelor

5. RESPONSABILITATI

- **Manageri si coordonatori:** Stabilesc drepturile de acces necesare angajatilor din subordine, precum si revocarea acestora si solicita aprobarea.
- **CEO:** Aproba autorizarea / revocarea drepturile de acces solicitate de manageri si coordonatori pentru personalul din subordine.
- **AS:** Acorda / revoca drepturile de acces aprobate, in baza formularului *F-SMSI-05 Autorizare/revocare acces in sistem*.
- **RPD** verifica anual drepturile de acces in cadrul VIMERCATI EAST EUROPE SRL, cat si lista utilizatorilor autorizati. Daca modificarile in cadrul proceselor companiei o cer. Propune modificarea drepturilor de acces.

VIMERCATI EAST EUROPE SRL	PROCEDURA DE LUCRU: CONTROLUL ACCESULUI IN SISTEMUL INFORMATIC	Pagina 2 din 7
	Cod document: PL-SMSI-08	Versiunea 1.0

6. DESCRIEREA PROCEDURII

6.1. Cerinte organizationale

Atunci cand sunt stabilite regulile de control al accesului trebuie avute in vedere urmatoarele:

- Stabilirea regulilor pe baza premizei “Totul este interzis, daca nu este permis in mod explicit”, fata de regula mai putin eficienta “Totul este permis, daca nu este interzis in mod explicit
- Acordarea permisiunilor utilizatorului, functie de rolul sau in cadrul proceselor.

6.2. Accesul utilizatorului

Activarea si dezactivarea utilizatorului trebuie sa tina seama de urmatoarele:

- Verificare daca utilizatorul are aprobarea managerului sau cordonatorului in subordinea caruia se afla, pentru utilizarea sistemului sau serviciului informatic;
- Verificarea daca nivelul de acces este in concordanta responsabilitatile utilizatorului in cadrul proceselor;
- Completarea formularului “Autorizare/Revocare acces sistem” cod F-SMSI-05 de catre managerul sau coordonatorul unitatii functionale impreuna cu utilizatorul in cauza si aprobarea acestuia de catre CEO;
- Revocarea sau blocarea imediata a drepturilor de acces ale persoanelor care au schimbat rolul, postul sau au parasit organizatia;
- Verificarea periodica, revocarea sau blocarea conturilor redundante ale utilizatorilor;
- Asigurarea neutilizarii contului de catre alti utilizatori.

RPD va analiza cel putin anual, impreuna cu AS, persoanele autorizate in sistemul informatic al VIMERCATI EAST EUROPE SRL si drepturile de acces ale acestora, urmand a lua masurile necesare, dupa caz. Motivele revizuirilor in cadrul, dar si in afara perioadelor stabilite, pot consta in:

- Utilizatori noi sau demisionari,
- Acordarea sau retragerea de privilegii,
- Modificarea clasificarii informatiilor,
- Modificarea necesarului de cunoastere a utilizatorilor,
- Modificari in fluxul informatiilor sau ale activitatilor organizatiei.

Procesul de revizuire se va inregistra, urmand ca drepturile de acces ale acestora sa se modifice corespunzator, dupa caz.

Privilegiile se alocă angajatilor pe baza necesitatii de cunoastere prin satisfacerea cerintelor minime pentru rolul functional indeplinit, si numai atunci cand este necesar, pentru fiecare eveniment in parte. Acordarea drepturilor de acces privilegiate se va face numai in urma autorizarii date de catre CEO, cu avizul tehnic al AS. Obiectul acordarii privilegiilor include:

- Sisteme de operare,

VIMERCATI EAST EUROPE SRL	PROCEDURA DE LUCRU: CONTROLUL ACCESULUI IN SISTEMUL INFORMATIC	Pagina 3 din 7
	Cod document: PL-SMSI-08	Versiunea 1.0

- Sisteme de gestionare a bazelor de date,
- Aplicatii critice sau confidentiale.

Modificarea atributiilor si responsabilitatilor de serviciu atrage dupa sine reanalizarea privilegiilor acordate si, dupa caz, retragerea acestora.

Pentru evitarea situatiilor critice privind lipsa disponibilitatii informatiilor, cand este nevoie de existenta drepturilor privilegiate iar persoana autorizata lipseste din companie, CEO va desemna o a doua persoana autorizata cu drepturi de acces privilegiate, ca rezerva. Interventiile de urgenta asupra unui sistem, care ar necesita utilizarea drepturilor privilegiate, vor fi inregistrate, evaluate si revizuite, luandu-se toate masurile asiguratorii asupra faptului ca integritatea sistemului a fost restabilita.

In momentul inregistrarii demisiei unui angajat, CEO, impreuna cu reprezentatul pentru resurse umane si managerul sau cordonatorul angajatului in cauza, va analiza si hotara daca mentinerea drepturilor de acces in sistem constituie un risc inacceptabil pentru VIMERCATI EAST EUROPE SRL si, in caz afirmativ, drepturile de acces vor fi revocate. La parasirea organizatiei, in cazul in care angajatul nu a avut drepturile de acces revocate in momentul depunerii demisiei, acestea vor fi revocate de AS, asigurandu-se ca fostul angajat nu mai poate accesa in nici un fel sistemul informatic.

6.3. Managementul parolelor

Parolele vor fi utilizate in cadrul VIMERCATI EAST EUROPE SRL pentru: conturile utilizatorilor (uzuale sau privilegiate), conturile de e-mail, cat si pentru conectarea la alte facilitati ce necesita o parola (smartphone, scanner, imprimanta etc).

Parolele temporare (de unica folosinta) vor fi furnizate in mod securizat de AS. Angajatii vor lua la cunostinta la primirea parolei de conditiile de utilizare si drepturile lor de acces.

SELECTIE

Utilizatorii vor manifesta atentie necesara selectiei unei parole sigure, avand urmatoarele caracteristici:

- Contine minim 6 caractere;
- Contine atat caractere uppercase cat si lowercase;
- Contine numere, semne de punctuatie, caractere speciale si litere;
- Nu este un cuvant din vreo limba straina, dialect, jargon etc.;
- Nu se bazeaza pe informatii personale, nume din familie, numar auto etc.;
- Va fi usor de retinut dar dificil de descifrat;
- La introducerea parolelor acestea nu trebuie să fie afișate în clar pe monitor.

UTILIZARE

VIMERCATI EAST EUROPE SRL	PROCEDURA DE LUCRU: CONTROLUL ACCESULUI IN SISTEMUL INFORMATIC	Pagina 4 din 7
	Cod document: PL-SMSI-08	Versiunea 1.0

Parolele vor fi schimbate la fiecare 90 de zile. Nu vor putea fi reutilizate ultimele 5 de parole.

Se vor utiliza parole diferite pentru accesarea diferitelor sisteme informatice sau sisteme de operare diferite.

Parolele temporare (de unica folosinta) vor fi schimbate la prima accesare a sistemului. Alocarea acestui tip de parola se va face de regula de catre AS, intr-o maniera confidentiala si securizata. Parolele generice, furnizate impreuna cu software-ul sau aplicatiile noi achizitionate, vor fi schimbate imediat dupa instalare.

In gestionarea si utilizarea parolelor sunt INTERZISE:

- Folosirea facilitatii de memorare a parolei a diferitelor aplicatii sau sisteme;
- Transmiterea parolei prin telefon sau e-mail;
- Furnizarea catre alte persoane de detalii despre parola sau indicii despre modul de selectie a acesteia;
- Dezvaluirea parolei in chestionare sau formulare de securitate, ori membrilor familiei;
- Transmiterea parolei colegilor de serviciu pe perioadele de absenta din firma.

Daca o persoana solicita o parola altei persoane, se va face trimitere la aceasta procedura si va fi informat de urgenta RPD.

Parolele nu vor fi stocate pe hartii volante nesecurizate sau in fisiere nesecurizate in cadrul sistemelor. Daca un cont sau o parola sunt suspectate de a fi fost compromise, incidentul va fi raportat AS sau RPD, iar contul si/sau parola vor fi schimbate imediat.

Conturile de acces se vor bloca automat dupa trei incercari nereusite de introducere a parolei corecte, intr-un interval de maxim 30 de minute. Deblocarea se va face de catre AS sau specialistul desemnat de acesta, ori contul se va reseta automat dupa un interval de 30 de minute. Incercarile nereusite sunt inregistrate in log-uri si sunt investigate de AS si RPD.

Anual sau la solicitare, AS va proceda la teste de vulnerabilitate prin sondaj ale parolelor utilizate in companie. Daca o anumita parola va fi decriptata, utilizatorului in cauza i se va cere sa o schimbe imediat.

Utilizatorul isi va putea schimba parola prin intermediul mecanismului de reconfirmare a parolei, pentru inregistrarea erorilor de introducere.

Utilizatorii vor manifesta atentie deosebita la selectia si utilizarea parolelor in cazul accesarilor de la distanta prin intermediul echipamentelor mobile de calcul, cat si in cazul desfasurarii activitatii la distanta (teleworking). Aceste conturi intra in categoria conturilor privilegiate. Conturile privilegiate si parolele acestora vor fi tratate cu observarea prevederilor prezentei proceduri in materie de drepturi privilegiate.

VIMERCATI EAST EUROPE SRL	PROCEDURA DE LUCRU: CONTROLUL ACCESULUI IN SISTEMUL INFORMATIC	Pagina 5 din 7
	Cod document: PL-SMSI-08	Versiunea 1.0

6.4. Obligatiile utilizatorilor

Toti utilizatorii trebuie constientizati in ceea ce priveste cerintele de securitate si regulile pentru protejarea echipamentelor nesupravegheate, cat si asupra responsabilitatilor privind respectarea unor asemenea masuri de protectie. Utilizatorii trebuie indrumati:

- Sa inchida sesiunile active la terminare, in afara de cazul in care se pot proteja printr-un mecanism de deconectare adecvat;
- Sa securizeze calculatorul sau terminalul cand acesta nu este utilizat, prin blocarea tastaturii sau o masura de securitate echivalenta.

La parasirea locului de munca – temporar sau la sfarsitul programului de lucru – utilizatorii vor avea in vedere urmatoarele:

- Informatiile restrictionate sau confidentiale, precum si datele cu caracter personal, cum ar fi cele tiparite sau stocate pe medii electronice, trebuie incuiate (ideal in safe-uri, dulapuri sau alt mobilier securizat) daca nu este nevoie de acestea sau in afara programului de lucru;
- Calculatoarele si terminalele trebuie deconectate din retea ori protejate cu un mecanism de blocare a monitorului sau a tastaturii, controlat prin parola, cheie hardware sau un mecanism de autentificare similar, atunci cand acestea sunt lasate nesupravegheate;
- Trebuie prevenita utilizarea neautorizata a fotocopiatoarelor si a altor tehnologii de reproducere;
- Documentele tiparite trebuie luate imediat din imprimanta sau copiator.

6.5. Controlul accesului in retea

Utilizatorilor trebuie sa li se permita accesul numai la serviciile furnizate de reseaua VIMERCATI EAST EUROPE SRL pentru care au fost anume autorizati sa le utilizeze.

Pentru controlul accesului de la distanta al utilizatorilor autorizati din cadrul VIMERCATI EAST EUROPE SRL, autentificarea se va face doar cu user name si parola.

AS va lua masurile necesare pentru controlul asupra accesului fizic si logic la porturile de diagnoza si configurare de la distanta.

AS va implementa masuri de securitate privind rutarea in retele, pentru a se asigura ca fluxurile informationale si conexarile la calculator nu incalca procedura de control a accesului. Masurile de securitate privind rutarea trebuie sa aiba la baza mecanisme de verificare reala a adreselor sursa si destinatie.

6.6. Controlul accesului la sistemul de operare, aplicatii si informatii

Accesul la sistemele de operare si la utilitarele de sistem, atat din interiorul cat si din exteriorul VIMERCATI EAST EUROPE SRL, trebuie restrictionat.

VIMERCATI EAST EUROPE SRL	PROCEDURA DE LUCRU: CONTROLUL ACCESULUI IN SISTEMUL INFORMATIC	Pagina 6 din 7
	Cod document: PL-SMSI-08	Versiunea 1.0

Mecanismele de autentificare utilizate vor permite confirmarea identitații pretinse de un utilizator. Aceasta masura de securitate trebuie aplicata tuturor tipurilor de utilizatori (incluzand personalul tehnic de asistenta).

Activitatile obisnuite ale utilizatorului nu trebuie desfasurate de pe conturile privilegiate.

Accesul personalului de mentenanta extern la informatii si la functiile sistemelor de aplicatii trebuie restrictionat, iar atunci cand este totusi permis, se va face in concordanta preznta procedura pentru controlul accesului.

Sistemele importante trebuie sa dispuna de un mediu de procesare dedicat (izolat).

7. INREGISTRARI

Denumire document (cod identificare)	Responsabil cu realizarea inregistrarii	Durata de pastrarea inregistrarilor	Locul pastrarii inregistrarii
Autorizare/Revocare acces sistem cod F-SMSI-05	AS	Pe durata angajarii + 1 an	Resurse Umane

8. ANEXE

- Autorizare/Revocare acces sistem

Formular cod F-SMSI-05

VIMERCATI EAST EUROPE SRL	PROCEDURA DE LUCRU: CONTROLUL ACCESULUI IN SISTEMUL INFORMATIC	Pagina 7 din 7
	Cod document: PL-SMSI-08	Versiunea 1.0

ACTUALIZARI

Nr. Crt.	Sinteza actualizarii	Versiunea curenta	Data
1.			
2.			
3			