

VIMERCATI EAST EUROPE SRL	PROCEDURA DE SISTEM: MANAGEMENTUL INCIDENTELOR DE SECURITATE A INFORMATIEI	Pagina 1 din 13
	Cod document: PS-SMSI-04	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 asigurarea unui raspuns rapid, eficient si organizat in cazul producerii unui eveniment si/sau incident de securitate.

Procedura documenteaza un proces centralizat si omogen de management al incidentului. Acest proces trebuie sa furnizeze suficiente informatii astfel incat VIMERCATI EAST EUROPE SRL sa se asigure ca:

- Pe cat posibil, asemenea evenimente si/sau incidente nu vor mai avea loc;
- Au fost restabilite masurile de securitate existente.

2. DOMENIUL DE APLICARE

Prevederile prezentei proceduri sunt aplicabile tuturor angajatilor VIMERCATI EAST EUROPE SRL, in mod special personalului tehnic de specialitate responsabil de administrarea sistemului informatic.

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.
- REGULAMENTUL 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

- **Eveniment de Securitate** – un eveniment identificat privind starea unui sistem, serviciu sau retea, care indica o posibila breșa in politica de securitate a informatiilor sau caderea unei masuri de securitate, ori o situatie necunoscuta anterior, relevanta in materie de securitate.
- **Incident de Securitate** – unul sau o serie de evenimente de securitate a informatiilor nedorite sau neasteptate, care au o probabilitate semnificativa de a compromite operatiunile organizatiei si de a ameninta securitatea informatiilor.

4.2. Prescurtari

- **FRIS:** Formular de Raportare a Incidentelor de Securitate
- **CEO:** Chief Executive Officer (Director General)
- **CRIS:** Colectivul de Raspuns la Incidentele de Securitate
- **RPD:** Responsabil Protectia Datelor

VIMERCATI EAST EUROPE SRL	PROCEDURA DE SISTEM: MANAGEMENTUL INCIDENTELOR DE SECURITATE A INFORMATIEI	Pagina 2 din 13
	Cod document: PS-SMSI-04	Versiunea 1.0

5. RESPONSABILITATI

- CEO desemneaza membrii CRIS.
- RPD este persoana unica de contact pentru raportarea incidentelor si evenimentelor de securitate si coordoneaza CRIS.
- RPD asigura instruirea si constientizarea personalului privind modul de actiune in cazul aparitiei unor incidente sau evenimente de securitatea informatiilor.
- RPD inregistreaza incidentele de securitate in FRIS si in Registrul incidentelor de securitate.
- CRIS investigheaza cauzele incidentelor de securitate si stabileste masuri de eliminare a reaparitiei acestora.
- RPD notifica ANSPDCP si persoanele vizate privind producerea incidentului si impactul acestuia in cazul in care acesta implica date cu caracter personal si urmareste actiunile de eliminare a reaparitiei acestora.

6. DESCRIERE

Exemple de incidente de securitatea informatiei:

- Caderea oricarei masuri de securitate;
- Incendii, explozii sau inundatii;
- Caderi de tensiune;
- Acces neautorizat in incinta organizatiei sau in sistemul informatic;
- Furt de date, informatii sau echipamente;
- Divulgarea datelor si informatiilor confidentiale sau datelor cu caracter personal;
- Existenta unor brese in confidentialitate;
- Scanarea porturilor retelei de catre persoane neautorizate;
- Atac cu virusi sau software delictual;
- Compromiterea conturilor utilizatorilor sau a parolelor;
- Coruperea datelor sau informatiilor;
- Incercari repetate de acces sau utilizare neautorizate;
- Trafic extern al retelei, sau activitati ale sistemului informatic, fara legatura cu activitatea organizatiei;
- Incercari repetate de a transmite e-mail unor conturi interne necunoscute sau inexistente;
- Caderi ale sistemului informatic sau ale serviciilor acestuia etc.

Orice eveniment de securitate sau incident de securitate va fi raportat prompt catre RPD, in mod confidential.

Elementele procedurale incluse in managementul incidentelor constau in:

- Analiza si identificarea cauzelor;
- Actiuni de prevenire a reaparitiei;
- Colectarea probelor;
- Comunicarea cu personalul afectat sau implicat;
- Escaladarea incidentului, in caz de necesitate.

In cazul probelor, inregistrările vor fi colectate securizat si corespunzător pentru a se asigura:

VIMERCATI EAST EUROPE SRL	PROCEDURA DE SISTEM: MANAGEMENTUL INCIDENTELOR DE SECURITATE A INFORMATIEI	Pagina 3 din 13
	Cod document: PS-SMSI-04	Versiunea 1.0

- Analizarea problemei interne;
- Utilizarea probei in legatura cu o potentiala incalcare a clauzelor contractuale, incalcare normelor interne sau legale, cat si utilizarea acestora in cadrul unui proces civil sau penal sau a procesului disciplinar;
- Posibilitatea de negociere a compensarilor cu furnizorii de software sau servicii.

Pentru ca probele colectate sa poata fi folosite in cazul unei actiuni judecatoresti civile sau penale se vor avea in vedere, dupa caz, urmatoarele reguli:

- a) Admisibilitatea probelor – daca o proba poate sau nu fi admisa in instanta. Pentru asigurarea admisibilitatii este necesar ca sistemul informatic al organizatiei sa contina mecanismele standard recunoscute pentru producerea unor asemenea probe (ex. log-uri).
- b) Importanta probelor – calitatea si completitudinea probei. Pentru asigurarea acestei conditii este necesara asigurarea unei supravegheri stricte a probelor, astfel:
 - Documentele tiparite: originalul va fi pastrat in siguranta si se va inregistra cine l-a gasit, unde, cand si cine a fost martor. Orice investigatie trebuie sa asigure integritatea originalului;
 - Informatii pe medii electronice de stocare: se vor face copii ale mediilor de stocare, pentru asigurarea disponibilitatii acestora. Se va efectua inregistrarea actiunilor de copiere, procesul in sine urmand sa se desfasoare in prezenta martorilor. Copia mediului de stocare si inregistrarea procesului se vor pastra securizat;
 - Izolarea zonei delictuale si colectarea probelor, inclusiv cele fizice, numai de catre organele abilitate.
- c) Dovezi adecvate care sa demonstreze ca masurile de securitate au functionat corect si constant, pe toata perioada cat proba in cauza a fost stocata si procesata de sistemul informatic.

Actiunile de recuperare in urma producerii incidentelor de securitate si de corectare a neconformitatilor se vor intreprinde asigurandu-se ca:

- Toate operatiunile de urgenta intreprinse sunt documentate in detaliu;
- Actiunile sunt raportate managementului de la cel mai inalt nivel, urmand a fi analizate intr-o maniera organizata;
- Integritatea sistemelor organizatiei si a masurilor de securitate existente este confirmata in cel mai scurt timp posibil;
- Numai personalul de specialitate, desemnat si autorizat, poate accesa sistemele functionale si datele acestora.

Daca in cadrul procesului de solutionare a incidentului de securitate se constata cu certitudine ca este vorba de o neconformitate a sistemului informatic ce nu poate fi rezolvata cu resursele organizatiei, sau interventia presupune o cat de mica alterare a software-ului original in cauza, incidentul va fi escaladat la nivelul asistentei tehnice a producatorului, conform clauzelor licentelor de utilizare sau a contractelor incheiate cu acesta.

In cazul in care incidentul este provocat de o actiune delictuala, se vor strange probe si/sau se vor securiza zonele de unde se pot obtine probe concludente, urmand a se face demersurile necesare la autoritatile competente, pentru finalizarea cercetarilor.

VIMERCATI EAST EUROPE SRL	PROCEDURA DE SISTEM: MANAGEMENTUL INCIDENTELOR DE SECURITATE A INFORMATIEI	Pagina 4 din 13
	Cod document: PS-SMSI-04	Versiunea 1.0

Raportarea, evaluarea, investigarea, solutionarea si inregistrarea incidentului de securitate se vor face conform Schemei de Tratare a Incidentului (Anexa 1), adaptate conform fiecarei categorii de incidente de securitate.

In cazul in care sunt afectate date cu caracter personal, incidentul va fi raportat catre Autoritatea Nationala de Supraveghere a Prelucrării Datelor cu Caracter Personal in termen de 72 ore de la identificarea acestuia (*F-GDPR-03b Notificare privind producerea unui incident de securitate – ANSPDCP*).

In cazul in care incidentul implica posibile riscuri ridicate asupra vietii private, sunt notificate persoanele vizate, fara intarziere (*F-GDPR-03a Notificare privind producerea unui incident de securitate – persoana vizata*).

7. INREGISTRARI

Denumire document (cod identificare)	Responsabil cu realizarea inregistrarii	Durata de pastrarea inregistrarilor	Locul pastrarii inregistrarii
FSI-01 Fisa de raportare a incidentului de securitate (FRIS)	RPD	3 ani	RPD
FSI-02 Registrul incidentelor de securitate	RPD	3 ani	RPD
F-GDPR-03a Notificare privind producerea unui incident de securitate – persoana vizata	RPD	3 ani	RPD
F-GDPR-03b Notificare privind producerea unui incident de securitate – ANSPDCP	RPD	3 ani	RPD

8. ANEXE

- Schema de Tratare a Incidentului Anexa 1
- FSI-01 Fisa de raportare a incidentului de securitate Anexa 2
- FSI-02 Registrul incidentelor de securitate Anexa 3

VIMERCATI EAST EUROPE SRL	PROCEDURA DE SISTEM: MANAGEMENTUL INCIDENTELOR DE SECURITATE A INFORMATIEI	Pagina 5 din 13
	Cod document: PS-SMSI-04	Versiunea 1.0

- F-GDPR-03a Notificare privind producerea unui incident de securitate – persoana vizata
Anexa 4
- F-GDPR-03b Notificare privind producerea unui incident de securitate – ANSPDCP
Anexa 5

VIMERCATI EAST EUROPE SRL	PROCEDURA DE SISTEM: MANAGEMENTUL INCIDENTELOR DE SECURITATE A INFORMATIEI	Pagina 6 din 13
	Cod document: PS-SMSI-04	Versiunea 1.0

ANEXA 1

SCHEMA DE TRATARE A INCIDENTELOR

ETAPA	ACTIUNE						
1	Un incident de securitate este raportat si receptionat de RPD, care deschide FRIS						
2	<table><tr><td>NU</td></tr><tr><td>RPD transmite informatia pentru a fi rezolvata de personalul de specialitate</td></tr></table>	NU	RPD transmite informatia pentru a fi rezolvata de personalul de specialitate	<table><tr><td>DA</td></tr><tr><td>Este notificat CEO</td></tr></table>		DA	Este notificat CEO
NU							
RPD transmite informatia pentru a fi rezolvata de personalul de specialitate							
DA							
Este notificat CEO							
3	<table><tr><td>NU</td></tr><tr><td>Procesul este oprit</td></tr></table>	NU	Procesul este oprit	<table><tr><td>DA</td></tr><tr><td>Este notificat CRIS Se inregistreaza incidentul in FRIS</td></tr></table>		DA	Este notificat CRIS Se inregistreaza incidentul in FRIS
NU							
Procesul este oprit							
DA							
Este notificat CRIS Se inregistreaza incidentul in FRIS							
4	<table><tr><td>NU</td></tr><tr><td>Este initiata recuperarea</td></tr></table>	NU	Este initiata recuperarea	<table><tr><td>DA</td></tr><tr><td>Este initiata investigatia</td></tr></table>	DA	Este initiata investigatia	
NU							
Este initiata recuperarea							
DA							
Este initiata investigatia							
5	Initierea recuperarii si investigatiei Sistemul afectat va fi izolat imediat de restul retelei companiei. Daca este vorba de o actiune delictuala, reseaua interna se va deconecta de la conexiunile externe. Decizia de deconectare apartine RPD.						
6	Prezervarea probelor, daca se decide de RPD Se va face un back-up complet al sistemului, mediile de stocare vor fi etichetate corespunzator si vor fi stocate securizat. Se vor utiliza utilitare eficiente si recunoscute.						

ETAPA	ACTIUNE
7	Identificarea problemei Daca anumite fisiere continand virusi sau software delictual pot fi identificate, acestea vor fi mutate intr-o locatie sigura. Se vor utiliza utilitare eficiente si recunoscute. Daca exista si alte locatii implicate, exista posibilitatea de strange si alte informatii utile investigatiei si solutionarii rapide a problemei.

VIMERCATI EAST EUROPE SRL	PROCEDURA DE SISTEM: MANAGEMENTUL INCIDENTELOR DE SECURITATE A INFORMATIEI	Pagina 7 din 13
	Cod document: PS-SMSI-04	Versiunea 1.0

ETAPA	ACTIUNE
8	Izolarea problemei Toate procesele suspectate vor fi oprite si indepartate din sistem. Vor fi indepartate toate fisierele suspectate a fi infectate.
9	Protejarea sistemului Vor fi implementate corectii sau module de corectie pentru protejarea sistemului impotriva unor atacuri viitoare. Imediat ce sistemul a fost adus in stare de functionare sigura, se vor testa corectiile implementate. Daca este posibil, virusul sau software-ul delictual va fi lasat functional pe sistemul izolat, pentru verificarea eficacitatii solutiilor abordate.
10	Revenirea la modul de operare normal Inainte de aducerea sistemului in modul de operare normal, vor fi notificati RPD si utilizatorii afectati.
11	Inregistrarea in BEIS RPD va documenta rezultatul investigatiei si va informa CEO. CEO va dispune inregistrarea incidentului in Registrul incidentelor de securitate si va propune sanctiuni disciplinare sau initierea unor actiuni in instanta, dupa caz.
12	Notificarea ANSPDCP si a persoanelor vizate In cazul in care incidentul afecteaza date cu caracter personal, RPD notifica in scris ANDSPCP asupra producerii acestuia si a impactului, in termen de 72 ore. In cazul in care incidentul implica posibil risc ridicat asupra vietii private, sunt notificate persoanele vizate, in cel mai scurt timp posibil.
13	Analize de urmarie Dupa ce un incident a fost complet solutinat si sistemele au fost readuse in stadiul de functionare completa si normala, se va efectua o analiza de urmarire. Toti cei implicati vor analiza intr-o sedinta de lucru, actiunile intreprinse si invatamintele desprinse din tratarea incidentului. Procedurile si politicile afectate vor fi evaluate si modificate, daca este cazul. In functie de necesitate, se va propune managementului companiei recomandari pertinente.

Nota: In cazul in care incidentul de securitate nu implica sistemul informatic, unele etape lipsesc.

VIMERCATI EAST EUROPE SRL	PROCEDURA DE SISTEM: MANAGEMENTUL INCIDENTELOR DE SECURITATE A INFORMATIEI	Pagina 8 din 13
	Cod document: PS-SMSI-04	Versiunea 1.0

ANEXA 2 – Fisa de raportare a incidentului de securitate (FRIS)

Cod FSI-01

FISA DE RAPORTARE A INCIDENTELOR DE SECURITATE - FRIS –

IDENTIFICAREA INCIDENTULUI

Informatii generale

Identificarea Raportorului:

Nume si prenume:

Functia:

Unitatea functionala:

Data si ora detectarii incidentului:

Unde a fost detectat incidentul:

Descrierea incidentului

Tipul de incident detectat:

☐ Acces neautorizat

☐ Soft delictual

☐ Utilizare neautorizata

☐ Altele:

Localizarea incidentului:

Unitatea Functionala:

Utilizator:

Data si ora la care echipa de interventie a sosit la fata locului:

Descrierea sistemului afectat (cate una pentru fiecare sistem, daca este cazul):

Model echipament:

Numarul de inventar:

Sistemul afectat este conectat la retea:

☐ Da

☐ Nu

Adresa de retea (IP):

Adresa fizica (MAC):

Izolarea incidentului

Izolarea sistemului afectat:

RSMI a aprobat deconectarea din retea a sistemului?

☐ Da

☐ Nu

Daca DA, data si ora deconectarii:

Daca NU, se detaliaza motivele:

Beackup-ul sistemului

Backup-ul sistemului s-a realizat cu succes?

☐ Da

☐ Nu

Nominalizarea persoanelor care au efectuat backup-ul:

Data si ora inceperii actiunii de backup:

Data si ora terminarii actiunii de backup:

VIMERCATI EAST EUROPE SRL	PROCEDURA DE SISTEM: MANAGEMENTUL INCIDENTELOR DE SECURITATE A INFORMATIEI	Pagina 9 din 13
	Cod document: PS-SMSI-04	Versiunea 1.0

Mediile de stocare au fost sigilate? ☐ Da ☐ Nu Data

sigiliului:
Backup-ul a fost predat catre (nume, prenume, functie):

Semnatura: Data:

Locatia de depozitare a backup-ului:

<i>Solutionarea Incidentului</i>

Numele si prenumele persoanelor care au efectuat investigarea sistemului:

A fost identificata vulnerabilitatea? ☐ Da ☐ Nu
Descriere:

Masuri de protectie intreprinse:
Descriere:

Sistemul a fost readus in stare normala de functionare
Data: Ora:

Actiuni Corective sau preventive? ☐ Da ☐ Nu
Descriere:

Responsabil:
Termen:

Intocmit:	Data:	Semnatura
------------------	--------------	------------------

VIMERCATI EAST EUROPE SRL	PROCEDURA DE SISTEM: MANAGEMENTUL INCIDENTELOR DE SECURITATE A INFORMATIEI	Pagina 10 din 13
	Cod document: PS-SMSI-04	Versiunea 1.0

ANEXA 3 – Registrul incidentelor de securitate

Cod: FSI-02

REGISTRU INCIDENTE DE SECURITATE

Nr. crt.	Tip / Natura Incident:	Proprietar:	Semnalat de:	Data Semnalarii:	Descriere Incident:	Impact / Severitate:	Actiuni Intreprinse:	Data Solutionare:	Responsabil:	Data Inchidere:

VIMERCATI EAST EUROPE SRL	PROCEDURA DE SISTEM: MANAGEMENTUL INCIDENTELOR DE SECURITATE A INFORMATIEI	Pagina 11 din 13
	Cod document: PS-SMSI-04	Versiunea 1.0

ANEXA 4 - Notificare privind producerea unui incident de securitate – persoana vizata

F-GDPR-03a

Catre: _____

Notificare privind producerea unui incident de securitate

VIMERCATI EAST EUROPE SRL, cu sediul în STR. GARII Nr.100, Bl. HALA B1, COM. HEMEIUȘ, JUD. BACAU, va aducem la cunostinta producerea urmatorului incident de securitate care a implicat datele dumneavoastra cu caracter personal:

Data si ora identificarii incidentului: _____

Descrierea incidentului: _____

Categoria de date cu caracter personal implicate: _____

Posibilul impact al producerii incidentului: _____

Masurile luate in vederea eliminarii / reducerii impactului si a prevenirii reaparitiei acestui tip de incident: _____

Totodata, va aducem la cunostinta ca am notificat Autoritatea Nationala de Supraveghere a Prelucrării Datelor cu Caracter Personal privind producerea incidentului.

Prelucrarea datelor cu caracter personal in cadrul VIMERCATI EAST EUROPE SRL se face in conformitate cu prevederile **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)**, iar dumneavoastra beneficiati de drepturile prevazute in **Capitolul III: Drepturile persoanei vizate**, respectiv: accesul la datele cu caracter personal proprii, rectificarea sau ștergerea acestora, restricționarea prelucrării sau a dreptul de a se opune prelucrării, precum și dreptul la portabilitatea datelor, in conditiile respectarii prevederilor ce constituie temei legal pentru prelucrarea datelor.

In situatia in care considerati ca drepturile dumneavoastra prevazute in Regulamentul nr. 679 / 2016 au fost incalcate, aveti dreptul de a depune plangere la Autoritatea Nationala de Supraveghere a Prelucrării Datelor cu Caracter Personal (www.dataprotection.ro).

Pentru informatii sau alte probleme legate de protectia datelor cu caracter personal va puteti adresa Ofiterului cu Protectia Datelor pe e-mail: _____ sau tel. _____.

VIMERCATI EAST EUROPE SRL	PROCEDURA DE SISTEM: MANAGEMENTUL INCIDENTELOR DE SECURITATE A INFORMATIEI	Pagina 12 din 13
	Cod document: PS-SMSI-04	Versiunea 1.0

ANEXA 5 - Notificare privind producerea unui incident de securitate – ANSPDCP

F-GDPR-03b

Catre: Autoritatea Nationala de Supraveghere a Prelucrării Datelor cu Caracter Personal

Notificare privind producerea unui incident de securitate

VIMERCATI EAST EUROPE SRL, cu sediul în STR. GARII Nr.100, Bl. HALA B1, COM. HEMEIUȘ, JUD. BACAU, va aducem la cunostinta producerea urmatorului incident de securitate date cu caracter personal:

Data si ora identificarii incidentului: _____

Descrierea incidentului: _____

Persoane vizate afectate: _____

Categoria de date cu caracter personal implicate: _____

Posibilul impact al producerii incidentului: _____

Masurile luate in vederea eliminarii / reducerii impactului si a prevenirii reaparitiei acestui tip de incident: _____

Totodata, va aducem la cunostinta ca

- ☐ am notificat / urmeaza sa notificam (*in cazul in care incidentul implica posibil risc ridicat asupra vietii private*)
- ☐ nu am notificat (*in cazul in care incidentul nu implica posibil risc ridicat asupra vietii private*) persoanele vizate privind producerea incidentului.

Prelucrarea datelor cu caracter personal in cadrul VIMERCATI EAST EUROPE SRL se face in conformitate cu prevederile **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).**

Pentru informatii sau alte probleme legate de protectia datelor cu caracter personal va puteti adresa Ofiterului cu Protectia Datelor pe e-mail: _____ sau tel. _____.

VIMERCATI EAST EUROPE SRL	PROCEDURA DE SISTEM: MANAGEMENTUL INCIDENTELOR DE SECURITATE A INFORMATIEI	Pagina 13 din 13
	Cod document: PS-SMSI-04	Versiunea 1.0

ACTUALIZARI

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