1. LISTA RESPONSABILILOR CU ELABORAREA, VERIFICAREA ŞI APROBAREA

Nr. Crt.	**Elemente privind responsabilii/ operaţiunea**	**Numele şi prenumele**	**Funcţia**	**Data**	**Semnătură**
	1	2	3	4	5
1.1	Elaborat	Răzvan Constantin Georgescu	Analist IT	29.05.2020	
1.2	Verificat	Berteanu Cristina Mihaela	Responsabil sistem de management integrat	01.06.2020	
1.3	Avizat	Simion Nicoleta	Preşedinte Comisie SCIM	29.06.2020	
1.4	Aprobat	Aurora Dragomirișteanu	Director general	30.06.2020	

2. SITUAŢIA EDIŢIILOR ŞI A REVIZIILOR

Nr. Crt.	**Ediţia/ revizia**	**Componenta modificată**	**Descrierea modificării**	**Data aplicării**
	1	2	3	4
2.1.	Ediţia 1/ Revizia 0		Versiune iniţială	01.11.2017
2.2.	Ediţia 1/ Revizia I	Componentele 5,6,7,8 și 12	Structura politicii conform Ordinului SGG nr.600/2018	01.07.2020

3. CUPRINS

4. SCOP

Prezenta politica se refera la stabilirea unor reguli de buna practica pentru securitatea fizica in locatia RNDVCSH pentru prevenirea accesului neautorizat, a daunelor si a intervenţiilor in locatia fizica a RNDVCSH.

5. DOMENIUL DE APLICARE

Prezenta politica se aplica in locatia RNDVCSH.

6. DOCUMENTE DE REFERINȚĂ

- LEGEA nr. 333 / 2003 privind paza obiectivelor, bunurilor, valorilor şi protecţia persoanelor actualizata
- ORDONANŢA DE URGENŢĂ nr. 16 / 2005
- HOTARAREA nr. 301 / 2012 pentru aprobarea Normelor metodologice de aplicare a Legii nr. 333/2003
- INSTRUCŢIUNI nr. 9 / 2013 privind efectuarea analizelor de risc la securitatea fizică
- Registrul National al Evaluatorilor de Risc la Securitatea Fizica
- SR ISO/CEI 27001:2013, Tehnologia informaţiei. Tehnici de securitate. Sisteme de management al securităţii informaţiei. Cerinţe.
- SR ISO/CEI 27002:2013, Tehnologia informaţiei. Tehnici de securitate. Cod de bună practică pentru managementul securităţii
- Ordinul nr. 600/2018 pentru aprobarea Codului controlului intern/managerial al entitatilor publice. Standardul 11 - Continuitatea activităţii.
- ISO/IEC 27000: 2014, Information technology - Security techniques - Information security management systems- Overview and vocabulary.
- Standardele Asociației Mondiale a Donatorilor de Măduvă 2020

7. DEFINITII

Sunt valabile si definitiile din standardul SR ISO/CEI 27001:2013.

8. ABREVIERI

1. **SMC** - Sistem de management al calităţii (componenta a SMI);
2. **SMSI** - Sistem de management al securitatii informatiei
3. **SMI** - Sistem de management integrat (include SCIM) ce cuprinde documentele generate în baza standardelor : SR EN ISO 9001:2015, SR ISO/CEI 27001:2013 și a standardelor prevăzute în Ordinul nr. 400/2015 pentru aprobarea Codului controlului intern/managerial al entităților publice
4. **MSMI** - Manualul sistemului de management integrat;
5. **SCIM** – Sistem de control intern/managerial;
6. **RSMI** – Responsabil al sistemului de management integrat;
7. **RSI** – Responsabil securitatea informațională;
8. **TD** - Tipul informatiei documentate (original sau copie);
9. **TC** - Nivelul de control aplicat informatiei documentate;
10. **NC** - Nivelul de clasificare aplicat informatiei documentate (public, confidenţial, neconfidenţial);
11. **S** - Standard;
12. **PO** - Procedură operațională;
13. **PS** - Procedură de sistem;
14. **M** - Manual;
15. **PL**- Politica.

9. DESCRIEREA POLITICII

Echipamentele tehnice de procesare a informaţiei critice sau sensibile pentru desfasurarea activitailor RNDVCSH trebuie gazduite in zone sigure, protejate de un perimetru de securitate definit, cu reguli de securitate si control la intrare corespunzatoare.

Locatia RNDVCSH trebuie protejată fizic faţa de accesul neautorizat, daune si interferenţe.
Protecţia oferita trebuie sa fie gradata, pe masura riscurilor identificate.

Se recomanda aplicare regulilor specifice “biroului curat si a ecranului curat”, pentru a reduce riscul accesului neautorizat sau pe cel de distrugere a documentelor, suporturilor media si echipamentelor tehnice de procesare a informaţiei.
Aceste bariere pot fi de urmatorul tip: un perete, o poarta incuiata, usi cu sisteme de inchidere eficiente, gratii la geamuri, birou de receptie cu paza umana, senzori de prezenta etc.

Protecţia fizica poate fi realizata prin crearea catorva bariere fizice in jurul amplasamentelor activitaţii si a echipamentelor tehnice de procesare a informaţiei.

Fiecare bariera stabileste un perimetru de securitate, care furnizeaza o crestere a protecţiei totale.

RNDVCSH foloseaste perimetre de securitate pentru a proteja zone care conţin echipamente de procesare a informaţiei.

De amplasarea si taria fiecarei bariere depinde rezultatul evaluarii riscului.

In RNDVCSH se ia in considerare si sunt implementate, acolo unde este cazul, urmatoarele controale:
- perimetrul de securitate este clar definit;
- perimetrul unei cladiri sau al unei incaperi unde sunt instalate echipamente tehnice de procesare a informaţiei este izolat fizic (nu trebuie sa existe goluri in acest perimetru sau zone pe unde se poate intra usor).
Pereţii exteriori sunt dintr-un material solid si toate usile exterioare sunt protejate adecvat impotriva accesului neautorizat, prin intermediul mecanismelor de control, bare, alarme, incuietori etc;
- este amplasat un birou de recepţie pazit si alte mijloace de control al accesului fizic in cladire sau incaperi/ monitorizare video, senzori de prezenta, alarma.
Accesul in incapere sau cladire este permis doar persoanelor autorizate sau vizitatorilor validati de reprezentantii RNDVCSH;
- barierele fizice, daca este necesar, sunt extinse de la podea pana la plafon pentru a preveni intrarile neautorizate si contaminarea mediului, cum ar fi in caz de incendiu sau inundaţie;
- toate iesirile de incendiu dintr-un perimetru de securitate au senzori de alarmare.

Zone de securitate sunt protejate prin controale de intrare adecvate, pentru a se asigura numai accesul persoanelor autorizate. Urmatoarele controale sunt luate in considerare:
- vizitatorii in zonele de securitate sunt supravegheaţi sau au permisiunea de acces, iar data si ora intrarii si plecarii sunt inregistrate. Accesul se va autoriza numai pentru scopuri precise, determinate, si accesul va fi emis impreuna cu instrucţiuni privind cerinţele de securitate ale zonei si privind politicile in caz de urgenţe;
- accesul la informaţii sensibile si la echipamente tehnice de procesare a informaţiei este controlat si limitat doar la persoanele autorizate.

Se vor lua in considerare controalele de autentificare, cum ar fi carduri de acces cu pin, trebuie utilizate pentru a autoriza si valida toate intrarile si iesirile. Un registru de audit al supravegherii accesului trebuie menţinut permanent;
- intregul personal va fi obligat sa poarte unele forme de identificare vizibile si trebuie incurajat sa someze persoanele straine neinsoţite sau pe toţi cei care nu poarta un identificator vizibil;
- drepturile de acces in zonele securizate trebuie periodic revazute si innoite.

O zona sigura in cadrul RNDVCSH poate fi un birou incuiat sau cateva incaperi in interiorul unui perimetru de securitate fizica, care poate fi incuiat si poate conţine dulapuri etc ce se pot incuia.

Selecţia si proiectarea unei zone de securitate sigure trebuie sa ţina cont de posibilitatea de distrugere cauzată 0de incendiu, inundaţie, explozie, miscari civile si de alte forme de dezastru natural sau dezastre cauzate de om. Se va ţine seama si de reglementarile si standardele de interes din domeniul sanataţii si siguranţei. De asemenea, sunt luate in considerare orice ameninţari de securitate venite din mediul inconjurator, cum ar fi scurgerea de apa din alte zone.

Sunt luate in considerare urmatoarele controale:
- echipamentele tehnice importante sunt situate astfel incat sa fie evitat accesul publicului;
- cladirea nu trebuie sa iasa in evidenţa si trebuie sa existe o minima indicaţie referitoare la scopul lor, fara semne evidente care sa indice, in afara sau in interiorul cladirii, existenţa unor activitaţi de procesare a informaţiei;
- funcţiunile de suport si echipamentul accesoriu, cum ar fi fotocopiatoare, faxuri, trebuie situate corespunzator, intr-o zona sigura, pentru a evita cererile de acces care ar putea compromite informaţia;
- usile si ferestrele trebuie inchise, atunci cand nu sunt supravegheate si trebuie luata in considerare asigurarea protecţiei externe pentru ferestre (gratii), mai ales pentru cele de la parter;
- sisteme de monitorizare si de detectare a intrusilor, profesionale si testate periodic, pentru a putea supraveghea toate usile exterioare si ferestrele accesibile.
Zonele neocupate trebuie sa aiba setata alarma tot timpul. Trebuie sa se asigure o acoperire si pentru alte zone, cum ar fi camera serverelor;
- echipamentele de procesare a informaţiei gestionate de catre organizaţie sunt separate fizic de cele gestionate de terţi;
- indrumarele si listele de telefoane interne prin care se identifica localizarea echipamentelor tehnice de procesare a informaţiilor sensibile nu trebuie sa fie usor accesibile publicului;
- materialele periculoase sau combustibile sunt pastrate in siguranţa la distanţa corespunzatoare faţa de o zona de securitate.
Aprovizionarile in cantitati mari, cum ar fi obiectele de papetarie, nu trebuie pastrate in zona sigura decat in cazul in care sunt necesare;
- echipamentele de rezerva si mediile care conţin copii de siguranţa trebuie situate la o distanţa sigura (alta locatie/ data center etc), pentru a evita distrugerile in cazul unui dezastru la sediul principal.

10. RESPONSABILITĂȚI

10.1. Directorul general
10.1.1. Aprobă Politica opearţională de cerințe privind securitatea fizica.
10.1.2. Asigură resursele necesare pentru realizarea politicii respective.
10.1.3. Coordonează soluţionarea accidentelor majore.
10.1.4. În cazul în care incidentul implică aplicarea legilor civile sau penale, va sesiza organele statului şi va acţiona ca persoană de legatură cu acestea.

10.1.5. În cazul în care mass-media solicită o opinie despre un incident petrecut la RNDVCSH, acesta va colabora cu purtătorul de cuvânt în vederea transmiterii de informații către mass-media.

10.2. Directorul financiar- contabil
10.2.1. Verifică modul de punere în aplicare a prezentei proceduri;

10.3. Compartimentul IT

10.3.1. Stabileşte un set de reguli de buna practica pentru securitatea fizica in locatia RNDVCSH pentru prevenirea accesului neautorizat, a daunelor si a intervenţiilor in locatia fizica a RNDVCSH.
10.3.2. Organizează spațiile de lucru și de depozitare cu sisteme de securitate pentru a reduce riscul accesului neautorizat sau pe cel de distrugere a documentelor, suporturilor media si echipamentelor tehnice de procesare a informaţiei.

10.4. Personalul organizaţiei

10.4.1. Îşi însuşeşte prevederile politicii şi le aplică în activitatea proprie.
10.4.2. Raportează Compartimentului IT sau Directorului General orice încălcare a acestei politici.

11. DISTRIBUIRE/DIFUZARE

	Scopul difuzarii	**Compartiment**	**Functia**
	1	**2**	**3**
11.1	Aplicare	Conducere	Director financiar contabil
11.2	Aplicare	Compartiment juridic	Consilier juridic gradul IA – secretar al comisiei de monitorizare SCIM
11.3	Aplicare	Compartiment resurse umane	Referent de specialitate gradul II
11.4	Aplicare	Compartiment audit intern	Auditor gradul I
11.5	Aplicare	Compartiment financiar-contabilitate	Economist specialist IA
11.6	Aplicare	Compartiment financiar-contabilitate	Economist specialist IA
11.7	Aplicare	Compartiment achiziţii si administrativ	Referent de specialitate gradul I
11.8	Aplicare	Compartiment informatic	Analist (programator) ajutor IA
11.9	Aplicare	Compartiment informatic	Analist (programator) ajutor II
11.10	Aplicare	Compartiment informatic	Informatician gradul II
11.11	Aplicare	Compartiment donatori	Medic primar
11.12	Aplicare	Compartiment donatori	Medic primar
11.13	Aplicare	Compartiment donatori	Medic primar
11.14	Aplicare	Compartiment donatori	Asistent medical principal
11.15	Aplicare	Compartiment donatori	Referent de specialitate gradul I
11.16	Aplicare	Compartiment donatori	Referent I
11.17	Aplicare	Compartiment pacienţi români	Medic primar
11.18	Aplicare	Compartiment pacienţi români	Medic primar
11.19	Aplicare	Compartiment pacienţi români	Medic primar
11.20	Aplicare	Compartiment pacienţi români	Medic primar
11.21	Aplicare	Compartiment pacienţi români	Medic primar
11.22	Aplicare	Compartiment pacienţi români	Medic specialist

	Scopul difuzarii	**Compartiment**	**Functia**
	1	**2**	**3**
11.23	Aplicare	Compartiment pacienţi români	Medic specialist
11.24	Aplicare	Compartiment pacienţi români	Asistent medical principal
11.25	Aplicare	Compartiment pacienţi străini	Referent de specialitate gradul I
11.26	Aplicare	Compartiment pacienţi străini	Medic primar
11.27	Arhivare	Conducere	Director general

12. ANEXE, INREGISTRĂRI, ARHIVARI

12.1 Formulare

Nr. Crt.	**Cod Formular**	**Denumire Formular**	**Persoana responsabilă de păstrare a documentelor**	**Termenul de păstrare**	**Observaţii**
1	FPL-015-1	Lista perimetre de securitate			
2	FPL-015-2	Registrul de controlul accesului in camera serverelor			
3	FPL-015-3	Registrul de testare a senzorior			

12.2 Analiza politicii