
 <p>Ministerul Sănătății Registrul Național al Donatorilor Voluntari de Celule Stem Hematopoietice</p>	Cod: PL-022	Ediția I	
	PROTECTIA ANTIVIRUS		Revizia I
Compartiment unde se aplică: IT	Valabil de la: 01.07.2020		Pag 1 din 4

1. LISTA RESPONSABILILOR CU ELABORAREA, VERIFICAREA ȘI APROBAREA

Nr. Crt.	Elemente privind responsabilii/ operațiunea	Numele și prenumele	Funcția	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	Președinte Comisie SCIM	29.06.2020	
1.4	Aprobat	Aurora Dragomirișteanu	Director general	30.06.2020	

Note:

1. Acest document contine informatii si date care sunt proprietatea RNDVCSH
2. Prezentul document este destinat utilizarii exclusive pentru propriile cerinte.
3. Utilizarea integrala sau partiala a acestui document in orice scop sau activitate sau reproducerea partiala/ integrala in orice publicatie si prin orice procedeu (electronic, mecanic, fotocopiere, microfilmare etc) este interzisa fara acordul scris al PROPRIETARULUI.
4. Versiunea aflata pe serverul companiei este cea oficiala. Orice copie electronica sau orice versiune tiparita sunt copii necontrolate. Utilizatorii documentului au obligatia de a se asigura ca utilizeaza ultima versiune a documentului, versiunea oficiala de pe server.


 <p>Ministerul Sănătății Registrul Național al Donatorilor Voluntari de Celule Stem Hematopoietice</p>	Cod: PL-022	Ediția I	
	PROTECTIA ANTIVIRUS		Revizia I
Compartiment unde se aplică: IT	Valabil de la: 01.07.2020		Pag 2 din 4

2. SITUAȚIA EDIȚIILOR ȘI A REVIZIILOR

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

3. CUPRINS

Numărul componentei în cadrul politicii	Denumirea componentei din cadrul politicii	Pagina
1	Lista responsabililor cu elborarea, avizarea, verificare și aprobarea ediției sau a reviziei în cadrul ediției politicii	1
2	Formular de evidență a modificărilor	2
3	Cuprins	2
4	Scopul politicii operaționale	3
5	Domeniul de aplicare a politicii operaționale	3
6	Documente de referință (reglementari) aplicabile	3
7	Definiții	3
8	Abrevieri	3
9	Descrierea politicii	3 - 4
10	Responsabilități	4
11	Distribuire și difuzare	4
12	Anexe, înregistrări, arhivări	4

 <p>Ministerul Sănătății Registrul Național al Donatorilor Voluntari de Celule Stem Hematopoietice</p>	Cod: PL-022	Editia I
	PROTECTIA ANTIVIRUS	
Compartiment unde se aplică: IT	Valabil de la: 01.07.2020	Pag 3 din 4

4. SCOP

Scopul acestei norme este sa stabileasca cerintele pentru sistemele IT/ calculatoarele din retea referitor la protectia antivirus , pentru a asigura o protectie eficienta contra virusilor si codurilor malitioase .

5. DOMENIUL DE APLICARE

Prezenta politica se aplica pentru toate sistemele IT / calculatoarele din retea RNDVCSH.

6. DOCUMENTE DE REFERINȚĂ

- SR EN ISO 9000/ 2015, Sisteme de management al calității. Principii fundamentale și vocabular.
- SR EN ISO 9001 / 2015, Sisteme de management al calității. Cerințe.
- SR ISO/CEI 27001: 2013, Tehnologia informației. Tehnici de securitate. Sisteme de management al securității informației. Cerințe.
- ISO 31000: 2009/ SR ISO 31000 :2010, Managementul riscului. Principii si linii directoare.
- Ordinul nr. 600/2018 pentru aprobarea Codului controlului intern/managerial al entitatilor publice. Standardul 8 - Managementul riscului
- SR ISO/CEI 27002:2013, Tehnologia informației. Tehnici de securitate. Cod de bună practică pentru managementul securității
- 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 calității (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. 600/2018 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, confidențial, neconfidențial);
11. **S** - Standard;
12. **PO** - Politică operațională;
13. **PS** - Politică de sistem;
14. **M** - Manual;
15. **PL**- Politica.

9. DESCRIEREA PROCESULUI

Aceasta politica se aplica tuturor calculatoarelor si include, dar nu se limiteaza la statii locale, laptop-uri, file/ftp/tftp/proxy servere.

Toate calculatoarele trebuie sa satisfaca standardele acestei norme, programul de antivirus trebuie sa fie instalat si programat pentru pornire automata. Baza de date a acestui program trebuie mentinuta la zi prin update-uri periodice. Calculatoarele virusate trebuie scoase din retea pana cand nu vor fi devirusate prin scanarea cu

 <p>Ministerul Sănătății Registrul Național al Donatorilor Voluntari de Celule Stem Hematopoietice</p>	Cod: PL-022	Ediția I
	PROTECTIA ANTIVIRUS	
Compartiment unde se aplică: IT	Valabil de la: 01.07.2020	Pag 4 din 4

programul de antivirus. Administratorul IT și RSI sunt responsabili pentru funcționabilitatea programului de antivirus, update-urile regulate și scanările periodice ale calculatoarelor.

Toate activitățile care au intenția sau pot crea sau distribui programe ce conțin viruși sau coduri malițioase în rețea (ex: *virus*, *trojan*, *email bombs*) sunt interzise, în conformitate cu politica de securitate.

La configurarea unui calculator nou, până la instalarea unui program de antivirus, se vor utiliza numai soft-uri originale.

Toate prezentările de soft-uri noi se vor face pe calculatoare de test și nu pe calculatoarele din producție.

Orice soft-uri comerciale trebuie scanate de antivirus înainte de a fi instalate.

Pentru a putea proteja datele în cazul virusării calculatorului, pentru fiecare stație se face un back-up periodic.

În cazul virusării calculatorului sau pentru orice explicații referitoare la protecția antivirus adresate-va administratorului IT.

Această politică nu se referă la stații ce rulează alt sistem de operare decât WINDOWS.

Orice angajat este obligat să respecte prevederile acestei norme. Nerespectarea lor poate fi subiectul unei acțiuni disciplinare sau poate duce la concedierea angajatului.

10. RESPONSABILITĂȚI

10.1. Directorul general

10.1.1. Aprobă Politica operațională de protecție antivirus.

10.2. Directorul financiar- contabil

10.2.1. Verifică modul de punere în aplicare a prezentei proceduri;

10.3. Compartimentul IT

10.3.1. Stabilește cerințele pentru sistemele IT din rețea pentru a asigura o protecție eficientă contra virușilor și codurilor malițioase.

10.3.2. Se asigură că toate stațiile locale, laptop-uri, file/ftp/tftp/proxy servere beneficiază de protecție antivirus.

10.4. Personalul organizației

10.4.1. Își însușește prevederile politicii și le aplică în activitatea proprie.

10.4.2. Raportează compartimentului IT orice încălcare a acestei politici.

11. DISTRIBUIRE/DIFUZARE

	Scopul difuzării	Compartiment	Funcția
	1	2	3
11.1	Aplicare	Compartiment informatic	Analist (programator) ajutor IA
11.2	Aplicare	Compartiment informatic	Analist (programator) ajutor II
11.3	Aplicare	Compartiment informatic	Informatician gradul II
11.4	Arhivare	Conducere	Director general

12. ANEXE, ÎNREGISTRĂRI, ARHIVĂRI

12.1 Analiza politicii