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	

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.*

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 stabileste metodologia de realizare a backup-ului informatiilor electronice.

Copiile de backup se fac din motive de asigurare a continuitatii proceselor, prin asigurarea posibilității de restaurare a informației/ sistemelor/ proceselor în urma unor incidente care au generat pierderea, distrugerea sau alterarea acestora.

5. DOMENIUL DE APLICARE

Prezenta politica se aplică informațiilor de pe serverele de fișiere, informațiilor din baza de date cu donatori de celule stem hematopoietice și pacienți și informațiilor de pe serverele echipamentelor de supraveghere video (CCTV).

6. DOCUMENTE DE REFERINȚĂ

- SR EN ISO 9001: 2015, Sisteme de management al calităţii
- SR ISO/CEI 27001: 2013, Tehnologia informatiei. Tehnici de securitate. Sisteme de management al securitatii informatiei. Cerinte.
- SR ISO/CEI 27002:2008, Tehnologia informației. Tehnici de securitate. Cod de buna practica pentru managementul securității informaţiei.
- ISO/IEC 27000: 2014, Information technology - Security techniques - Information security management systems- Overview and vocabulary.
- Ordinul nr. 600/2018 pentru aprobarea Codului controlului intern/managerial al entitatilor publice. Standardul 11 - Continuitatea activităţii.

7. DEFINIȚII

Backup **–** procesul prin care se fac copii ale informației electronice în scopul de a asigura reconstituirea originalului, atunci cand apare o astfel de nevoie;

CCTV – echipament de supraveghere video;

VPN **-** Virtual Private Network - O reţea privată virtuală care asigură o modalitate de stabilire a unor comunicaţii securizate între componentele acesteia;

Perioada de retenție **–** reprezintă intervalul de timp pentru care este obligatoriu să fie pastrată informația din motive legale sau la cererea proprietarului informației.

Restaurare **–** procesul prin care informația electronică este refacută în urma pierderii, distrugerii sau alterării sale.

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. 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, confidenţial, neconfidenţial);
11. **S** - Standard;
12. **PO** - Procedură operațională;
13. **PS** - Procedură de sistem;

14. **M** - Manual;
15. **PL**- Politica.

9. DESCRIEREA PROCESULUI

9.1. Aspecte prealabile

Diferențierea între copiile de backup și copiile de arhivă se face prin:
I. Scop:
- copiile de backup se fac din motive de asigurare a continuității proceselor, prin asigurarea posibilității de restaurare a informației/ sistemelor/ proceselor în urma unor incidente care au generat pierderea, distrugerea sau alterarea acestora.
- copiile de arhivă se fac din motive de conformitate cu legea sau datorită cerințelor proprietarului informației, și sunt parte a sistemului de derulare a proceselor.

I. Perioada de păstrare:
Numărul de copii de backup se păstreaza conform cerințelor stabilite la nivel de compartiment.
Copiile de arhivă se pastrează pe perioada de retenție (stipulate legal sau de către proprietarul informației.

III. Periodicitate:
- copiile de arhivă se fac cu periodicitatea stabilită de lege / proprietar.
- copiile de backup se fac atât periodic (conform cerințelor de continuitate) cât și înaintea oricăror modificări care pot duce la pierderea continuității sistemelor.

IV. Locul de păstrare:
- copiile de backup se recomandă să se păstreze într-o locație fizic separată de locația unde au fost create.
- copiile de arhivă sunt parte a sistemului de desfășurare a activității în care sunt realizate și din operarea acestuia.

V. Conținut:
- copiile de arhivă conțin informațiile cerute de lege / proprietar;
- copiile de backup conțin informațiile necesare restaurării informației / procesului: informații de configurare, ID-uri utilizatori, profilele utilizatorilor, datele de lucru, etc
VI. Ciclare:
- copiile de arhivă vor fi păstrate pe toata perioada de retenție (nu se ciclează).
- copiile de backup pot fi ciclate, pentru a păstra numai informația utilă cea mai recentă.
- codificare / etichetare – vor fi codificate și etichetate în mod diferit, pentru a se face ușor distincție între ele.

Copiile de arhivă sunt realizate conform cerințelor proprietarilor și este responsabilitatea acestora să menționeze regulile de arhivare, în conformitate cu nevoile și constrângerile stabilite de reglementările interne.
Principiul general obligatoriu: pentru fiecare sistem IT trebuie să existe proceduri (plan) de backup, subordonat unei politici de backup.
Politica de backup este aprobată de Directorul General.
Politicile și instrucțiunile de lucru privind backupul sistemelor informatice vor fi întocmite de către Administratorul sistemelor IT la nivelul organizației, pe baza regulilor stabilite prin acest document.

9.2. DESCRIEREA PROCESULUI

Pentru fiecare sistem IT trebuie să existe planuri și proceduri de backup, pentru fiecare din următoarele tipuri de informație:

9.2.1. Software: Toate aplicațiile software, atat cele achiziționate de la terți, cât și cele create in-house trebuie să fie protejate împotriva pierderii, distrugerii sau alterării prin cel puțin o copie de backup, care sa poată asigura refacerea integrală a functionalității aplicației.

9.2.2. Datele de sistem: Datele folosite/ procesate de sistemele IT trebuie să fie protejate prin copii de backup care să asigure o copie full cel puțin o dată pe lună.

9.2.3. Datele de aplicație: Datele folosite/procesate de aplicațiile IT trebuie să fie protejate prin copii de backup care să asigure o copie full cel puțin o dată pe lună si care sa respecte minim principiul celor trei generații.

Acolo unde este cazul, planul și politicile de backup trebuie să fie individualizate și particularizate pentru fiecare aplicație care se află pe un sistem IT, dacă acestea necesită strategii de backup diferite.

Copile de backup păstrează clasificarea privind confidențialitatea și integritatea întocmai ca și originalul / sursa copiilor.

Administratorul sistemelor IT are obligația să dezvolte politicile necesare procesului de backup și restaurare, în conformitate cu politica de backup aprobată pentru sistemul respectiv.

Administratorul sistemelor IT are obligația să dezvolte planuri de backup cât mai clare și detaliate care trebuie să permită unei terțe persoane cu cunoștințele tehnice corespunzătoare să poată restaura în intervalul de timp menționat de planul de continuitate informația, aplicațiile și datele necesare repornirii serviciului susținut de sistemul respectiv.

Administratorul sistemelor IT va folosi soluția tehnologică cea mai potrivită în vederea efectuării copiilor de backup și arhivă, astfel încât compatibilitatea cu politica de retenție și cu politica de ciclare să fie asigurată.

Nu sunt permise excepții de la politica de retenție / ciclare aprobată din motive tehnice / tehnologice. Dacă soluțiile tehnice / tehnologice existente nu mai asigură realizarea copiilor de backup și arhivă conform politicilor aprobate, este necesară fie revizuirea politicilor, fie revizuirea soluției tehnice folosite.

În lipsa altor cerințe specifice, principiul minim de asigurat pentru efectuarea copiilor de backup este principiul celor 3 generații, care cere ca să fie efectuate 3 copii diferite de backup înainte ca prima să fie rescrisă.

NOTA: O generație de backup este considerată a fi un set de backup care permite reconstruirea integrala a funcționalității sistemului.

Procesul de realizare a copiilor de backup / arhiva nu trebuie să afecteze procesul de furnizare a serviciilor pentru sistemele respective.

În lipsa delegării clare a unor responsabilități către alte categorii de personal tehnic (operatori de backup, arhivari etc), responsabilitatea procesului de realizare a copiilor de backup/arhiva revine administratorului sistemelor IT. Delegarea responsabilităților trebuie să fie facută și acceptată în mod formal, prin prevederi politicale.

Acolo unde cerințele privind confidențialitatea și integritatea datelor nu permit accesarea acestora de către persoanele implicate în procesul de backup / arhivare, se vor avea în vedere măsuri de protecție corespunzătoare (tehnici criptografice, controlul accesului logic etc).

9.3. STOCAREA / PĂSTRAREA CORESPUNZĂTOARE A COPIILOR DE BACKUP ȘI A MEDIILOR DE DATE

Ca regulă generală, mediile de date de backup trebuie stocate în încăperi separate de cea unde se află sistemele țintă, ca o măsura de protecție în cazul unor incidente de extindere medie.

Pentru sistemele critice, un al doilea set de backup trebuie să fie păstrat într-o locație fizic separată de cea de producție, ca o masură de salvare în cazul unor incidente majore - dezastru.

Mediile de date trebuie stocate astfel încât să fie ferite de condiții care pot altera /distruge informația (praf, umiditate, apă, foc, temperaturi ridicate). De asemenea, trebuie ferite de expunerea la amenințări cum ar fi furtul, distrugerea, vandalismul, neglijența.

Din aceste considerente, trebuie asigurat controlul accesului la mediile de date, precum și asigurarea unor parametri de mediu corespunzători pentru locația unde sunt stocate mediile de date.

Mediile de date (benzi, CD-uri, etc) trebuie stocate în dulapuri rezistente la foc. La rândul lor, aceste dulapuri trebuie amplasate în camere în care există sisteme de alarmă antiincendiu și sisteme automate de stingere a incendiilor.

Protecția antiefracție:
- numai persoanele autorizate trebuie să poată avea acces la mediile de stocare date, pentru a preîntâmpina furtul / expunerea acestora.
- măsurile de control ale accesului trebuie să fie clar cunoscute de personalul implicat în măsurile de control ale accesului, trebuie să se asigure o operativitate suficient de ridicată, pentru a nu deveni o piedică în cazurile în care e necesară restaurarea rapidă a datelor.

9.4. VERIFICAREA PERIODICĂ A RESTAURABILITĂȚII COPIILOR DE BACKUP/ ARHIVĂ

Pentru demonstrarea fezabilității lor, planurile de backup trebuie să cuprindă testarea restaurabilității datelor conținute în copiile de backup. Aceasta are ca scop depistarea defectelor / incidentelor ce pot surveni în procesul de restaurare a datelor înainte de apariția efectivă a nevoii de restaurare.

Este posibil ca din anumite cauze (defecte tehnice, parametrizare greșită, manipulare și management inadecvat al mediilor de date, nerespectarea politicilor sau neconformitatea acestora cu politica), procesul de restaurare a datelor să nu funcționeze conform planului.

Funcționalitatea planurilor de backup trebuie testată periodic. Testele privind restaurarea datelor nu trebuie să se facă la perioade mai mari de 12 luni. Rezultatele testelor de verificare privind restaurarea datelor vor fi documentate.

9.5. COPIILE DE BACKUP PENTRU SOFTWARE-UL UTILIZAT

Pentru software utilizat, pe lângă suportul original al acestuia, trebuie să se efectueze și să se păstreze:
- copie de backup, în vederea reinstalarii acestora în caz de nevoie.
- copii de distribuție – copiile de lucru utilizate în operarea curentă, în măsura în care nu contravine legislației.

Având în vedere prevederile legale privind drepturile de autor, se impune controlul accesului la kiturile de instalare, la originalul software-ului folosit, cât și la copiile acestuia, indiferent de scopul pentru care a fost făcută copia. Acest control al accesului este atât o măsură de protecție împotriva piratării, cât și o măsură de preîntâmpinare a incidentelor rezultate în urma modificărilor/instalarilor neautorizate a softului.

Pe cât este posibil, copiile de backup vor fi făcute pe medii la care se poate asigura fizic protecția la scriere. Având în vedere timpul limitat de viață al mediilor de date de tip CD, se vor asigura copii pe medii cu durată mare de viață.
Păstrarea și gestionarea copiilor de backup intră în atribuțiile de versiuni, care la înlocuirea versiunilor se va asigura de conformitatea copiei de backup cu originalul și de retragerea copiilor vechi de backup.

La restaurarea aplicațiilor trebuie să se folosească copiile de backup și nu originalele.
Copiile de backup al softului utilizat și originalul acestora trebuie să fie păstrate în locații diferite.
Se va înregistra și ține evidența copiilor făcute, locațiile și persoanele în gestiunea cărora se găsesc aceste copii.

Numai persoanele autorizate vor avea acces la softul utilizat (atât la original, cât și la copiile de backup sau la copiile operaționale).

Acolo unde din motive operaționale s-a decis paătrarea copiilor de distribuție pe harddisk, se vor lua măsuri de control al accesului logic, astfel că numai persoanele autorizate să aibă acces la softul utilizat.

10. RESPONSABILITĂȚI

10.1.Directorul General

10.1.1. Aprobă Politica de backup al informației electronice.
10.1.2 Asigura resursele necesare pentru realizarea politicii respective.

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

10.3. Responsabilul SMI

10.3.1. Elaborează, actualizează, gestionează și arhivează Politica de backup al informației electronice.
10.3.2. Actualizează secțiunile de evidență (istorie) a modificărilor documentelor.
10.3.3 Testează periodic, împreună cu RSI procesul de restaurare a datelor.
10.3.4 Integrează și aplică regulile referitoare la backup-ul informației electronice impuse de Directorul General.

10.4 Responsabilul cu Securitatea Informatica (RSI)

10.4.1. Intocmește Planul de backup pentru fiecare server CCTV.
10.4.2 Testează periodic, împreună cu Responsabilul SMI procesul de restaurare a datelor.
10.4.4. Păstrarea și gestionarea copiilor de backup ale software-ului utilizat.
10.4.5. Aplică regulile referitoare la backup-ul informației electronice impuse de Directorul General.

10.5. Personalul organizației

10.5.1. Își însușește prevederile politicii și le aplică în activitatea proprie.
10.5.2. Raportează Directorului General orice încălcare a acestei politici.

11. DISTRIBUIRE/DIFUZARE

	Scopul difuzarii	**Compartiment**	**Functia**
	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, INREGISTRARI, ARHIVARI

12.1 Analiza politicii