MINISTERUL TRANSPORTURILOR SI INFRASTRUCTURII
SPITALUL CLINIC CĂI FERATE CRAIOVA
ISO 9001:2015 Certif. 21260C
ISO 14001:2015 Certif. 21260M
ISO 45001:2018 Certif. 21260SS
website: www.scfcv.ro
Blv. Ştirbei Vodă, nr. 6, Craiova
C.I.F.: 4332169
Tel.: 0351.733.144
E-mail: office@scfcv.ro
ANMCS
unitate aflată în
SUPRAVEGHEREA
Autorității Naționale de Management al Calității în Sănătate

Nr. 9313 din 21.10.2026

APROBAT,

Manager
Dr. Aurelia-Maria Gîngioveanu

MINISTERUL TRANSPORTURILOR SPITALUL CLINIC C.F. CRAIOVA 9

STRATEGIA DE SECURITATE CIBERNETICĂ A SPITALULUI CLINIC CĂI FERATE CRAIOVA ÎN PERIOADA 2026-2031

1. SCOPUL

Strategia de securitate cibernetică a Spitalului Clinic Căi Ferate Craiova are scopul de a defini şi de a menţine un mediu cibernetic sigur, cu un înalt grad de rezilienţă şi de încredere.

Totodată, Strategia de securitate cibernetică prezintă principiile, obiectivele şi direcţiile principale de acţiune pentru cunoaşterea, prevenirea şi contracararea ameninţărilor, vulnerabilităţilor şi riscurilor la adresa securităţii cibernetice a instituţiei, în deplină concordanţă cu natura activităţii sale specifice.

2. DOMENIU APLICARE

Strategia de securitate cibernetică a Spitalului Clinic Căi Ferate Craiova acoperă toate activităţile specifice şi se adresează întregului personal al instituţiei, tuturor partenerilor/ colaboratorilor, furnizorilor şi terţilor, precum şi pacienţilor/ clienţilor săi.

3. DOCUMENTE DE REFERINŢĂ (REGLEMENTĂRI)

3.1. Reglementări internaţionale

- SR EN ISO 9001:2015 – Sisteme de management al calităţii. Cerinţe;
- SR EN ISO/IEC 27001:2023 – Securitatea informaţiei, securitate cibernetică şi protecţia vieţii private. Sisteme de management al securităţii informaţiei;
- SR EN ISO/IEC 27002:2023 – Securitatea informaţiei, securitate cibernetică şi protecţia vieţii private. Controale de securitate a informaţiei;
- Directiva (UE) 2022/2555 a Parlamentului European şi a Consiliului din 14 decembrie 2022 privind măsuri pentru un nivel comun ridicat de securitate cibernetică în Uniune, de modificare a Regulamentului (UE) nr. 910/2014 şi a Directivei (UE) 2018/1972 şi de abrogare a Directivei (UE) 2016/1148 (**Directiva NIS 2**);

- Regulamentul (UE) nr. 679 din 27 aprilie 2016 privind protecţia persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal şi privind libera circulaţie a acestor date şi de abrogare a Directivei 95/46/CE (Regulamentul General privind Protecţia Datelor).

3.2. Legislaţie primară

- HG nr. 1.321/2021 privind aprobarea Strategiei de securitate cibernetică a României, pentru perioada 2022—2027, precum şi a Planului de acţiune pentru implementarea Strategiei de securitate cibernetică a României, pentru perioada 2022—2027;
- OUG nr.155, din 30.12.2024, privind instituirea unui cadru pentru securitatea cibernetică a reţelelor şi sistemelor informatice din spaţiul cibernetic naţional civil;
- Legea nr.124 din 7 iulie 2025 pentru aprobarea Ordonanţei de urgenţă a Guvernului nr. 155/2024 privind instituirea unui cadru pentru securitatea cibernetică a reţelelor şi sistemelor informatice din spaţiul cibernetic naţional civil;
- Legea nr.58 din 14 martie 2023 privind securitatea şi apărarea cibernetică a României;
- Legea 362/ 2018 privind asigurarea unui nivel comun ridicat de securitate a reţelelor şi sistemelor informatice;
- Legea nr. 333, din 2003. privind paza obiectivelor, bunurilor, valorilor şi protecţia persoanelor;
- Legea nr. 95/2006 privind reforma în domeniul sănătăţii, cu modificările şi completările ulterioare;
- Legea nr. 273/2006 privind finanţele publice locale cu modificări şi completări ulterioare;
- Legea nr. 500/2002 privind finanţele publice cu modificări şi completări ulterioare;
- Legea nr. 544 din 12 octombrie 2001 privind liberul acces la informaţiile de interes public;
- Legea nr. 190/ 2018 privind măsuri de punere în aplicare a Regulamentului (UE) 2016/ 679 al Parlamentului European şi al Consiliului.

3.3. Legislaţie secundară

- Ordinul ministrului sănătăţii Nr. 446/2017, din 18 aprilie 2017, privind aprobarea Standardelor, Procedurii şi metodologiei de evaluare şi acreditare a spitalelor;
- OSGG 600/ 2018 – privind aprobarea Codului controlului intern managerial al entităţilor publice;
- Ordinul 1537/2018 privind stabilirea atribuţiilor principale ale responsabililor cu managementul calităţii din cadrul Ministerului Sănătăţii şi unităţilor aflate în subordinea, coordonarea sau sub autoritatea acestuia pentru implementarea şi gestionarea Sistemului de management al calităţii bazat pe standardul SR EN ISO 9001:2015, cu completarile si modificarile ulterioare.
- Ordinul Ministrului Sănătăţii si al Presedintelui Autoritatii Nationale de Management al Calităţii în Sănătate nr. 1312/250/2020 privind organizarea şi funcţionarea structurii de management al calităţii serviciilor de sănătate în cadrul unităţilor sanitare cu paturi şi serviciilor de ambulanţă, în procesul de implementare a sistemului de management al calităţii serviciilor de sănătate şi siguranţei pacientului, cu modificările si completările ulterioare;
- Ordinul Directorului DNSC nr. 1/2026, pentru aprobarea Măsurilor de gestionare a riscurilor de securitate cibernetică aferente reţelelor şi sistemelor informatice utilizate de entităţile esenţiale şi importante şi a Metodologiei de autoevaluare a maturităţii măsurilor de gestionare a riscurilor de securitate cibernetică şi pentru modificarea Metodologiei privind evaluarea nivelului de risc al entităţilor, aprobată prin Ordinul directorului Directoratului Naţional de Securitate Cibernetică nr. 2/2025 pentru aprobarea Criteriilor şi pragurilor de determinare a gradului de perturbare a unui serviciu şi a Metodologiei privind evaluarea nivelului de risc al entităţilor;
- Ordinul Directorului DNSC nr. 3/2025, pentru aprobarea Normelor de aplicare a dispoziţiilor privind supravegherea, verificarea şi controlul respectării prevederilor Or-

donanței de urgență a Guvernului nr. 155/2024 privind instituirea unui cadru pentru securitatea cibernetică a rețelelor și sistemelor informatice din spațiul cibernetic național civil și a Metodologiei de prioritizare pe bază de risc a activităților de supraveghere, verificare și control;

3.4. Alte documente, inclusiv reglementări interne

- Regulamentul intern (RI) al Spitalului Clinic Căi Ferate Craiova;
- Regulamentul de organizare și funcționare (ROF) al Spitalului Clinic Căi Ferate Craiova ;

4. DEFINIȚII ȘI ABREVIERI ALE TERMENILOR UTILIZAȚI

4.1. Definiții ale termenilor

Nr. crt.	Termenul	Definiția și/sau, dacă este cazul, actul care definește termenul
1.	Managementul riscului	Un proces complex, continuu și flexibil de identificare, evaluare și contracarare a riscurilor la adresa securității cibernetice, bazat pe utilizarea unor tehnici și instrumente complexe, pentru prevenirea pierderilor de orice natură
2.	Apărare cibernetică	Asigurarea managementului incidentelor de securitate, precum și detectarea și tratarea incidentelor care afectează securitatea rețelelor și sistemelor informatice.
3.	Securitatea cibernetică	Starea de normalitate rezultată în urma aplicării unor măsuri proactive și reactive care asigură confidențialitatea, integritatea, disponibilitatea, autenticitatea și nonrepudierea informațiilor în format electronic din spațiul cibernetic.
4.	Securitatea informației	Păstrarea confidențialității, integrității și a disponibilității informației, la care se pot adăuga autenticitatea, responsabilitatea, nerepudierea și fiabilitatea.
5.	Rețea și sistem informatic	Înseamnă: 1. O **rețea de comunicații electronice** respectiv: • **sistemele de transmisie**, bazate sau nu pe o infrastructură permanentă sau pe o capacitate de administrare centralizată, și, acolo unde este cazul, echipamentele de comutare sau rutare și alte resurse, inclusiv elementele de rețea care nu sunt active, care permit transportul semnalelor prin cablu, prin unde radio, prin mijloace optice ori alte mijloace electromagnetice, incluzând rețelele de comunicații electronice prin satelit, rețelele terestre fixe, cu comutare de circuite și cu comutare de pachete, inclusiv internet, și mobile, • **rețelele electrice**, în măsura în care sunt utilizate pentru transmiterea de semnale, • **rețelele utilizate pentru transmisia serviciilor media audiovizuale** și • **rețelele de televiziune prin cablu**, indiferent de tipul de informație transmisă 2. Orice **dispozitiv** sau **ansamblu de dispozitive interconectate** sau aflate în relație funcțională, dintre care unul sau mai multe asigură prelucrarea automată a datelor digitale cu ajutorul unui program informatic; 3. **Datele digitale** stocate, prelucrate, recuperate sau transmise de elementele unei rețele sau unui sistem informatic, în vederea funcționării, utilizării, protejării și întreținerii lor;

Nr. crt.	Termenul	Definiția și/sau, dacă este cazul, actul care definește termenul
6.	Resurse informatice și de comunicații	Toate dispozitivele și activitățile asociate stației de lucru care permit primirea și transmiterea de e-mailuri, navigarea pe site-uri web, stocarea, administrarea și transmiterea datelor și informațiilor în format electronic: servere, calculatoare personale, laptop-uri, smartphone-uri, imprimante, echipamente de laborator și medicale conectate la rețea, resurse de telecomunicații, medii de rețea, telefoane și faxuri, precum și procedurile, programele și datele aferente.
7.	Confidențialitate	Proprietatea ca informația să nu fie făcută disponibilă sau divulgată unor persoane, entități, sau procese neautorizate.
8.	Integritate	Proprietatea de a proteja acuratețea și completitudinea resurselor.
9.	Disponibilitate	Proprietatea de a fi accesibil și utilizabil la cerere de către o entitate autorizată.
10.	Securitatea fizică	Domeniul securității care prezintă atât măsuri pentru prevenire cât și pentru împiedicarea atacatorilor să aibă acces la obiective, resurse sau informații și recomandări privind proiectarea infrastructurii pentru a opune rezistență la actele ostile.
11.	Protecție	Acțiune care are în vedere obiectivele domeniului, respectiv: ➢ asigurarea securității rețelelor și sistemelor informatice, ➢ securitatea fizică și a persoanei; ➢ administrarea și mentenanța resurselor rețelelor și sistemelor informatice; ➢ controlul accesului la elementele/ componentele rețelelor și sistemelor informatice.
12.	Atac	Încercare de a distruge, a expune, a modifica, a dezactiva, a fura sau a obține accesul neautorizat sau a utiliza în mod neautorizat o resursă.
13.	Amenințare	Cauză potențială a unui incident nedorit care poate produce daune unui sistem sau organizații.
14.	Vulnerabilitate	Slăbiciune a unei resurse sau a unui mijloc de control care poate fi exploatată de o amenințare.
15.	Spațiul cibernetic	Mediul virtual, generat de infrastructurile cibernetice, incluzând conținutul informațional procesat, stocat sau transmis, precum și acțiunile derulate de utilizatori în acesta.
16.	Eveniment privind securitatea informației	Fapt identificat în legătură cu starea unui sistem, a unui serviciu, sau a unei rețele indicând o posibilă încălcare a politicii de securitate a informației, un eșec al mijloacelor de control sau o situație ignorată anterior dar care poate fi relevantă din punct de vedere al securității.
17.	Incident privind securitatea informației	Unul sau o serie de evenimente privind securitatea informației nedorite sau neprevăzute care au o probabilitate semnificativă de compromitere a operațiunilor de business și de amenințare a securității informației.
18.	Reziliența infrastructurilor cibernetice	Capacitatea componentelor infrastructurilor cibernetice de a rezista unui incident sau atac cibernetic și de a reveni la starea de normalitate

4.2. Abrevieri ale termenilor

Nr. crt.	Abrevierea	Termenul abreviat
1.	ISO	Organizația Internațională pentru Standardizare
2.	IEC	Comisia Electrotehnică Internațională (International Electrotechnical Commission)
3.	SR	Standard român
4.	UE	Uniunea Europeană
5.	NIS	Network and Information Security (în română Securitatea rețelei și a informațiilor)
6.	SIC	Sistem Informatic și de Comunicații

7.	IT&C	Tehnologia Informațiilor și Comunicațiilor
8.	DNSC	Directoratul Național de Securitate Cibernetică
9.	RI	Regulamentul intern
10.	ROF	Regulamentul de organizare și funcționare
11.	EN	Standard european (European Norm)
12.	HG	Hotărârea Guvernului
13.	OUG	Ordonanța de urgență a Guvernului
14.	OSGG	Ordinul Secretarului General al Guvernului
15.	SCIM	Sistemul de control intern managerial
16.	RSRSI	Responsabilul cu securitatea rețelelor și sistemelor informatice
17.	CyFun	Cyber Fundamentals (cadrul de măsuri de gestionare a riscurilor de securitate cibernetică)

5. STRATEGIA DE SECURITATE CIBERNETICĂ

5.1. Introducere

Evoluția rapidă a domeniului tehnologic și dinamica amenințării cibernetice sunt condiții determinante pentru actualizarea și dezvoltarea permanentă a cadrului normativ instituțional pe componenta gestionării amenințărilor cibernetice și asigurării securității cibernetice.

Atacurile cibernetice, în special asupra serviciilor esențiale ori a infrastructurilor critice pot avea, datorită interconectivității, un impact major asupra serviciilor furnizate.

Strategia națională de securitate cibernetică obligă Spitalul Clinic Căi Ferate Craiova să dezvolte, să mențină și să implementeze propria Strategie de securitate cibernetică, document care va constitui temelia întregului cadru normativ instituțional privind securitatea cibernetică.

Strategia de securitate cibernetică se adresează întregului personal al Spitalului Clinic Căi Ferate Craiova, inclusiv colaboratorilor și partenerilor, furnizorilor de servicii și echipamente IT&C, precum și pacienților, clienților, publicului și terților.
Strategia de securitate cibernetică se actualizează ori de câte ori intervin schimbări semnificative în context, riscuri, tehnologie sau cadrul legal.

5.2. Principii

În vederea asigurării securității cibernetice a Spitalului Clinic Căi Ferate Craiova trebuie respectate următoarele **principii**:

- Securitatea cibernetică a Spitalului Clinic Căi Ferate Craiova este responsabilitatea tuturor actorilor implicați:
  - instituții ale administrației publice,
  - personalul desemnat pentru asigurarea securității cibernetice,
  - utilizatorii sistemului informatic al instituției,
  - furnizorii de servicii IT&C,
- Securitatea cibernetică sprijină funcționarea Spitalului Clinic Căi Ferate Craiova;
- Securitatea cibernetică se bazează pe stabilirea unui cadru normativ și procedural adecvat;
- Securitatea cibernetică a Spitalului Clinic Căi Ferate Craiova garantează:
  - menținerea unui spațiu cibernetic deschis, liber, stabil și sigur;
  - protejarea valorilor - politicile de securitate cibernetică vor asigura echilibrul între nevoia de creștere a securității în spațiul cibernetic și prezervarea dreptului la intimitate și alte valori și libertăți fundamentale ale cetățeanului și a statului de drept, în special în ceea ce privește libertatea de opinie, libertatea de exprimare, dreptul de a accesa și de a primi informații;

- protejarea datelor cu caracter personal.

5.3. Viziunea

Viziunea Spitalului Clinic Căi Ferate Craiova este ca, în fața unei amenințări cibernetice din ce în ce mai complexe, Spitalul Clinic Căi Ferate Craiova să își dezvolte și să își consolideze capabilitățile proprii de prevenire, descurajare și răspuns, precum și reziliența, inclusiv printr-o abordare proactivă, adecvată cadrului național de cooperare în domeniu.

Acțiunile conjugate ale actorilor implicați (managementul instituției; personalul cu responsabilități în asigurarea securității cibernetice; furnizorii de servicii IT&C; autoritățile desemnate ale statului) trebuie să vizeze:

- Prevenirea și descurajarea - dezvoltarea permanentă a capabilităților de detecție, investigare, combatere și atribuire a atacurilor cibernetice;
- Apărarea și contracararea - dezvoltarea și implementarea unor capabilități eficiente de apărare și a unor mecanisme proactive, de răspuns la atacuri cibernetice;
- Dezvoltarea și consolidarea - creșterea nivelului de securitate cibernetică și reziliență prin:
    - prioritizarea investițiilor în domeniul securității cibernetice;
    - dezvoltarea programelor educaționale;
    - consolidarea culturii de securitate cibernetică;
    - cooperarea cu părțile interesate și terții.

5.4. Misiunea

Misiunea Spitalului Clinic Căi Ferate Craiova este, în esență, **îmbunătățirea continuă a calității vieții pacienților** prin oferirea de **servicii medicale profesioniste, sigure și centrate pe nevoile acestora**, folosind tehnologii avansate și echipe dedicate, având ca scop final **siguranța pacientului** și **dezvoltarea calitativă a sistemului de sănătate**.

Elementele cheie ale misiunii noastre sunt:

- Centrarea pe pacient: Punerea nevoilor și siguranței pacientului pe primul loc;
- Calitatea actului medical: Asigurarea unor servicii bazate pe:
    - Specialiști cu înaltă calificare;
    - Cele mai bune protocoale și ghiduri medicale;
- Inovație și profesionalism: Achiziția și utilizarea tehnologiei de ultimă generație și dezvoltarea constantă a serviciilor furnizate;
- Îmbunătățire continuă: Optimizarea constantă a tuturor aspectelor, de la actul medical la relația cu pacienții;
- Prevenție și informare: Implicarea în programe de informare și prevenție pentru sănătatea publică pentru construirea unei relații de încredere cu cetățenii/ beneficiarii serviciilor furnizate.

Pentru aceasta și pentru acreditarea sistemelor informatice care asigură furnizarea serviciilor medicale, Spitalul Clinic Căi Ferate Craiova a instituit și aplică un **Sistem de Management al Securității Cibernetice**, pentru asigurarea:

- Securității informațiilor;
- Securității cibernetice;
- Protecției datelor cu caracter personal.

5.5. DECLARAȚIA privind Strategia de securitate cibernetică

Spitalul Clinic Căi Ferate Craiova este o entitate publică angajată deplin în:

- Dezvoltarea activității specifice în deplin acord cu nevoile de sănătate ale beneficiarilor serviciilor furnizate de instituție;
- Asigurarea și furnizarea de servicii medicale integrate, aliniate la principiul „îmbunătățirii continue";
- Implicarea întregului personal în creșterea eficienței și calității serviciilor furnizate;
- Protejarea sistemelor și rețelelor informatice, precum și a datelor și informațiilor de atacuri cibernetice;
- Asigurarea, consolidarea și promovarea rezilienței NIS;
- Asigurarea unui mediu digital sigur, prin elaborarea și implementarea de:
  - politici de securitate din Registrul de politici și proceduri;
  - proceduri operaționale de securitate IT&C din același registru;
  - măsuri tehnice și organizatorice pentru protecția, prevenirea, detectarea, investigarea și răspunsul la incidente de Securitate cibernetică;
- Cooperarea interinstituțională în domeniul securității NIS;
- Implicarea tuturor părților interesate în protecția ecosistemului/ mediului/ spațiului cibernetic;
- Promovarea culturii de securitate cibernetică în rândul angajaților proprii, furnizorilor și terților;
- Organizarea corespunzătoare a securității NIS;
- Asigurarea Managementului resurselor/ activelor NIS;
- Asigurarea Managementului riscurilor de Securitate;
- Asigurarea Securității personalului/ utilizatorilor SIC cu drepturi limitate de acces;
- Asigurarea Securității lanțului de aprovizionare;
- Asigurarea Securității fizice și a mediului de lucru;
- Asigurarea Controlului accesului;
- Asigurarea Managementului comunicațiilor și operațiunilor;
- Achiziționarea, dezvoltarea și mentenanța sistemelor informatice și de comunicații;
- Asigurarea Managementului incidentelor de securitate;
- Asigurarea Conformității cu cerințele legale de asigurare a securității informațiilor și cibernetice;
- Asigurarea Cooperării și colaborării cu părțile interesate și autoritățile desemnate ale statului.

Conducerea Spitalului Clinic Căi Ferate Craiova are în vedere îndeplinirea rolului deținut de instituție în sistemul național de sănătate și se preocupă, permanent, de menținerea, aplicarea și îmbunătățirea continuă a eficacității sistemului de management al resurselor și infrastructurii IT&C pentru furnizarea de servicii medicale prompte, eficiente și de înaltă calitate, în vederea satisfacerii cerințelor pacienților, aparținătorilor, precum și a terților.

5.6. Obiectivele privind securitatea cibernetică

5.6.1. Obiective generale pentru îndeplinirea misiunii și viziunii Spitalului Clinic Căi Ferate Craiova

- Asigurarea confidențialității, integrității și disponibilității datelor și informațiilor ce aparțin instituției sau pacienților/clienților săi;
- Protejarea datelor cu caracter personal care sunt stocate și procesate la nivelul sistemelor IT&C proprii instituției;
- Asigurarea faptului că datele fiecărui pacient/ client/ beneficiar vor putea fi accesate doar de entitățile autorizate de pacient/ client/ beneficiar și nimeni altcineva;
- Asigurarea securității serviciilor IT&C, monitorizarea și îmbunătățirea continuă a siguranței acestora pentru beneficiarii serviciilor furnizate de instituție;
- Asigurarea disponibilității serviciilor IT&C și a capacității de recuperare, în timp util, a acestora în situații de incident major;

- Utilizarea și dezvoltarea unor sisteme și rețele informatice sigure și reziliente, cu o capacitate sporită de detectare și răspuns la incidente;
- Creșterea nivelului de cunoaștere și competență cibernetică în rândul personalului Spitalului Clinic Căi Ferate Craiova;
- Îmbunătățirea cooperării cu toate părțile interesate pentru contracararea amenințărilor cibernetice.

5.6.2. Obiective specifice privind asigurarea securității cibernetice a Spitalului Clinic Căi Ferate Craiova

Pentru atingerea **obiectivelor generale**, managementul Spitalului Clinic Căi Ferate Craiova susține coerent, oferă suport managerial și alocă resursele necesare în vederea realizării următoarelor **obiective specifice:**

- Definirea, implementarea, operarea, menținerea, revizuirea și îmbunătățirea continuă a Sistemului de Management al Securității Cibernetice în cadrul instituției, conform reglementărilor din capitolul 3 privind securitatea cibernetică;
- Identificarea, analiza, evaluarea, tratarea și monitorizarea continuă a riscurilor de securitate cibernetică pentru toate resursele informaționale ale instituției;
- Implementarea soluțiilor/ măsurilor de securitate pentru prevenirea, eliminarea sau diminuarea riscurilor de securitate cibernetică actuale;
- Organizarea, într-o manieră securizată, a activității specifice Spitalului Clinic Căi Ferate Craiova, a proceselor interne și a celor de interacțiune cu pacienții/ autoritățile/ furnizorii/ clienții, pentru protejarea informației și securitatea serviciilor IT&C;
- Pregătirea planurilor de acțiune la incidente de securitate cibernetică, inclusiv prin conlucrarea cu furnizorii de servicii IT&C sau terții pentru asigurarea unor acțiuni coordonate și eficiente;
- Elaborarea și implementarea Planului de continuitate a activității IT&C și a Planului de recuperare IT&C;
- Formarea și menținerea competențelor și calificărilor necesare, la nivelul resurselor de personal, pentru securitatea cibernetică.

5.7. Planul de acțiune strategic

Planul de acțiune strategic acționează ca un „ghid procedural" care, pentru atingerea/ îndeplinirea fiecăruia dintre obiectivele strategice ale Spitalului Clinic Căi Ferate Craiova, va specifica, cel puțin:

- măsurile stabilite pentru asigurarea unui mediu digital sigur
- principalele acțiuni planificate
- participanții
- responsabilul/ coordonatorul acțiunilor și
- termenul de implementare.

5.8. Bugetul pentru securitatea cibernetică

Bugetul pentru securitate cibernetică își propune să asigure resursele financiare necesare pentru implementarea:

- **Planului de acțiune strategic** și a
- **Obiectivelor și direcțiilor de acțiune privind securitatea cibernetică**.

5.8.1. Bugetul pentru securitatea cibernetică trebuie să îndeplinească următoarele **caracteristici:**

- să fie conform cu politicile, cerințele legislative și de reglementare, ordinele și deciziile relevante în determinarea bugetului pentru securitate cibernetică, astfel încât să asigure disponibilitatea tehnologiilor și instrumentelor de securitate cibernetică;

- să fie precis, rațional și să includă toate cheltuielile preconizate pentru asigurarea securității cibernetice;
- să se bazeze pe ciclul bugetar anual al Spitalului Clinic Căi Ferate Craiova;
- să fie supus revizuirii regulate în conformitate cu politicile și procedurile Spitalului Clinic Căi Ferate Craiova.

5.8.2. Componentele bugetare

Bugetul pentru securitate cibernetică va fi compus din:

- **Bugetul pentru operarea funcției de securitate cibernetică**, inclusiv:
  - Costuri cu resursele umane
  - Costuri cu serviciile de consultanță
  - Costuri cu tehnologia
  - Alte costuri.
- **Bugetul pentru inițiativele și programele de securitate cibernetică**, inclusiv:
  - Costuri unice pentru configurarea funcției de securitate cibernetică și a proceselor aferente pentru implementarea Strategiei de securitate cibernetică.
  - Costuri recurente care acoperă măsurile de securitate cibernetică (de exemplu, gestionarea securității cibernetice, monitorizarea, raportarea, conformitate, audituri de securitate, etc.)
  - Costul programelor specializate de dezvoltare a competențelor și al instruirilor necesare pentru personalul de securitate cibernetică, cum ar fi cursuri de instruire și conferințe.
  - Costuri de externalizare.

6. RESPONSABILITĂȚI

6.1. Managerul Spitalului Clinic Căi Ferate Craiova are următoarele responsabilități:

- stabilește și aprobă **Strategia de securitate cibernetică**;
- asigură disponibilitatea resurselor (financiare, tehnologice și umane) necesare pentru aplicarea Strategiei de securitate cibernetică, precum și a politicilor și procedurilor de securitate IT&C;
- aprobă **Planul de acțiune pentru implementarea Strategiei de Securitate Cibernetică;**
- alocă, cu eficiență, resursele financiare, tehnologice și umane necesare aplicării Strategiei de securitate cibernetică.

6.2. Responsabilul cu securitatea rețelelor și sistemelor informatice (RSRSI)/ Responsabilul IT&C (angajat al organizației sau angajat al unui furnizor de servicii IT&C) are următoarele responsabilități:

- propune revizuiri/ modificări/ actualizări ale **Strategiei de securitate cibernetică**;
- elaborează **Planul de acțiune pentru implementarea Strategiei de securitate cibernetică** și monitorizează îndeplinirea acestuia;
- elaborează și propune spre aprobare politici și proceduri operaționale de securitate în conformitate cu Strategia de securitate cibernetică;
- propune **Bugetul pentru securitate cibernetică** care să asigure resursele financiare necesare pentru implementarea **Planului de acțiune pentru implementarea Strategiei de securitate cibernetică.**

6.3. Șefii structurilor/ entităților organizatorice sunt responsabili pentru:

- implementarea de zi cu zi a:
  - Strategiei de securitate cibernetică,
  - Planului de acțiune pentru implementarea Strategiei de securitate cibernetică;
  - politicilor și procedurilor operaționale de securitate aferente strategiei;

- asigurarea că obiectivele şi direcţiile de acţiune stabilite în Strategia de securitate cibernetică sunt implementate şi aplicate în mod corespunzător şi de către tot personalul din subordine;
- asigurarea resurselor necesare pentru ca Strategia de securitate cibernetică să fie aplicată în mod corespunzător în zona lor de responsabilitate.

6.4. Utilizatorii autorizaţi ai sistemelor (angajaţi şi terţi care acţionează într-o modalitate similară, cum ar fi furnizori de servicii) sunt responsabili pentru:

- cunoaşterea şi respectarea Strategiei de securitate cibernetică.

6.5. Colaboratorii şi angajaţii furnizorilor de servicii au următoarele responsabilităţi:

- respectă Strategia de securitate cibernetică a Spitalului Clinic Căi Ferate Craiova, pe timpul derulării contractului.

	Numele şi prenumele	Funcţia	Semnătura
Elaborat:	**Total Data Management SRL** **Dan Iordache**	**Responsabil Securitatea Reţelelor şi Sistemelor Informatice**	
Verificat:	**Ing. Iosif Bidin Florian Micu**	**Compartiment IT**	
Avizat:	**Dr. Mirela – Dulcineia Mateaş**	**Director Medical**	
Avizat:	**Ec. Loreta Magla**	**Director Financiar Contabil**	