Nr. înregistrare SMC ...10.../27.11.2019

POLITICA

PRIVIND SECURITATEA INFORMAȚIILOR

ID GDPR -01

	Elementele privind responsabilii/ operațiunea	Numele și Prenumele	Funcția	Data	Semnătura
0	1	2	3	4	5
1.1	Elaborat	Dan Iordache	**Responsabil protecția datelor-** Total Data Management S.R.L.	27.11.2019	
1.2	Verificat	Cătălin Voicu	Compartiment IT	27.11.2019	
1.3	Avizat	Dr.Simin Aysel Florescu	Președinte SCIM	27.11	
1.4	Aprobat	Dr. Emilian Ioan Imbri	Manager	27	

Cuprins

1. Introducere 4
2. Scop 4
3. Domeniu de aplicare 4
4. Documente de referință (reglementări), politici și proceduri asociate 5
4.1.Documente de referință 5
4.2.Politici și proceduri asociate 5
5. Definiții și abrevieri ale termenilor utilizați în politica de securitate 6
5.1. Definiții ale termenilor 6
5.2. Abrevieri ale termenilor 6
6. Politică 7
6.1. Declarație 7
6.2. Clasificarea informațiilor 7
6.3. Securitatea fizică și a mediului de lucru 8
6.4. Securitatea resurselor umane 8
6.5. Securitatea documentelor utilizate 8
6.6. Administrarea conturilor 9
6.7. Acordare și retragere accesului la date, sisteme informatice și site-uri web 9
6.8. Identificare și autentificare 10
6.9. Acces administrativ 10
6.10. Accesul la rețeaua de comunicații 11
6.11. Configurarea sistemelor informatice pentru accesul la rețeaua de comunicații 12
6.12. Utilizarea echipamentelor 13
6.13. Securitatea echipamentelor și resurselor în afara locației organizației 13
6.14. Utilizarea echipamentelor proprietate personală 14
6.15. Securizarea serverelor 15
6.16. Detectarea accesului neautorizat 15
6.17. Modificări ale configurației sistemului 16
6.18. Utilizarea rețelei Internet și Intranet 16
6.19. Site-uri web aparținând Spitalului de Boli Infecțioase și Tropicale "Dr. Victor Babeș" 17
6.20. Mijloace de comunicație 17
6.21. Utilizarea resurselor informatice în scop personal 18
6.22. Detectarea virușilor 18

6.24. Protecția datelor cu caracter personal 19
6.25. Conștientizare și instruire cu privire la securitatea informației 19
6.26. Relațiile cu furnizorii 19
6.27. Managementul evenimentelor legate de încălcărea securității datelor 20
6.28. Măsuri disciplinare 20
7. Responsabilități 20
7.1. Comitetul Director 20
7.2. Responsabilul IT 21
7.3. Șefii structurilor organizatorice 21
7.4. Angajații Spitalului de Boli Infecțioase și Tropicale "Dr. Victor Babeș" 21
7.5. Colaboratorii și angajații furnizorilor de servicii 22
8. Formular de evidență a modificărilor 22

1. INTRODUCERE

În activitățile desfășurate în cadrul Spitalului de Boli Infecțioase și Tropicale "Dr. Victor Babeș" se creează, colectează, stochează și prelucrează cantități mari de date. Informațiile și procesele, sistemele și rețelele asociate, precum și personalul implicat în exploatarea, manipularea și protecția acestora sunt resurse importante pentru Spitalul de Boli Infecțioase și Tropicale "Dr. Victor Babeș" și, în consecință, merită sau necesită protecție împotriva diverselor pericole.

Resursele sunt expuse atât amenințărilor intenționate, cât și celor accidentale, iar procesele, sistemele și rețelele asociate, precum și personalul pot prezenta vulnerabilități inerente. Schimbările intervenite în modul de desfășurare a activităților, în cadrul sistemelor utilizate sau alte schimbări externe (cum ar fi, legi și reglementări noi) pot crea noi riscuri de securitate a informației. Prin urmare, dată fiind multitudinea de moduri în care amenințările pot profita de vulnerabilități pentru a dăuna organizației, riscurile de securitate a informației sunt întotdeauna prezente. O securitate a informației eficace reduce aceste riscuri prin protejarea organizației împotriva amenințărilor și vulnerabilităților și apoi reduce impactul asupra resurselor ei.

Securitatea informațiilor este obținută prin implementarea unui set adecvat de mijloace de control, incluzând politici, procese, proceduri, structuri organizatorice și funcții software și hardware. Aceste mijloace de control necesită să fie stabilite, implementate, supravegheate, revizuite și îmbunătățite, dacă este necesar, pentru a se asigura atingerea obiectivelor de securitate ale organizației.

Pe lângă bunele practici stabilite la nivelul organizației, anumite categorii de date sunt supuse și reglementărilor legislației naționale și este vital ca personalul să recunoască toate detaliile legate de manipularea informațiilor Spitalului de Boli Infecțioase și Tropicale "Dr. Victor Babeș".

2. SCOP

Politica de securitate a informațiilor are ca scop asigurarea integrității, confidențialității și disponibilității informației.

Confidențialitatea se referă la protejarea informațiilor împotriva accesului neautorizat. Fiecare utilizator răspunde personal de confidențialitatea informațiilor încredințate sau create.

Integritatea se referă la măsurile și procedurile utilizate împotriva modificărilor sau distrugerii neautorizatea tuturor informațiilor în format letric sau electronic necesare desfășurării activităților din cadrul organizației.

Disponibilitatea se realizează prin asigurarea accesului la informațiile necesare desfășurării activităților din cadrul organizației.

De asemenea, Politica de securitate are ca scop stabilirea cadrului necesar pentru elaborarea politicilor și procedurilor de securitate a informațiilor.

3. DOMENIU DE APLICARE

Politica se aplică tuturor angajaților Spitalului de Boli Infecțioase și Tropicale "Dr. Victor Babeș", colaboratorilor și angajaților furnizorilor de servicii care accesează resursele informaționale ale Spitalului de Boli Infecțioase și Tropicale "Dr. Victor Babeș".

4. DOCUMENTE DE REFERINȚĂ (REGLEMENTĂRI), POLITICI ȘI PROCEDURI ASOCIATE

4.1.Documente de referință

- OSSG 600/2018 – privind aprobarea Codului controlului intern managerial al entităților publice;
- SR ISO/CEI 27001: 2013 – Tehnologia informației. Tehnici de securitate. Sisteme de management a securității informației;
- SR ISO/CEI 27002: 2018 - Tehnologia informației. Tehnici de securitate. Cod de bună practică pentru managementul securității informației;
- Ghidul de securitate informatică pentru funcționarii publici, CERT-RO;
- Regulamentul (UE) 679/ 2016 al Parlamentului European și al Consiliului (GDPR).

4.2.Politici și proceduri asociate

4.2..1. Politicile și procedurile ar trebui să fie consultate împreună cu *Politica privind securitatea informațiilor*. Politici și proceduri asociate *Politicii privind securitatea informațiilor* a Spitalului de Boli Infecțioase și Tropicale "Dr. Victor Babeș":

- Procedura privind securitatea resursele umane;
- Politica privind securitatea fizică și a mediului de lucru;
- Politici privind biroul curat, protejarea ecranului și tipărirea documentelor;
- Politică privind relațiile cu furnizorii;
- Politica privind rolurile și responsabilitățile personalului legate de securitatea datelor;
- Politica privind dispozitivele mobile și lucrul de la distanța;
- Politica privind managementul resurselor informatice;
- Procedura privind controlul accesului logic;
- Procedura privind gestionarea dispozitivelor criptografice;
- Procedura privind backup-ul și arhivarea;
- Procedura privind stocarea și transmiterea de informații;
- Procedura privind utilizarea serviciilor cloud;
- Procedura privind managementul parolelor;
- Politica utilizării sistemelor informatice și comunicațiilor;
- Politica privind utilizarea echipamentelor proprietate personală;
- Procedura instalare echipamente;
- Procedura privind accesul angajaților la sistemele informatice;
- Politica privind site-urile web;
- Procedura privind supravegherea video;
- Procedura privind eliminarea înregistrărilor;
- Politica management incidente de securitate.

4.2.2 *Politica Spitalului de Boli Infecțioase și Tropicale "Dr. Victor Babeș" privind protecția datelor* și procedurile asociate acesteia:

- Procedura desemnare Responsabil protecția datelor;
- Procedura Evidența prelucrărilor de date cu caracter personal;
- Procedura de evaluare a impactului privind protecția datelor;
- Procedura de evaluare a interesului legitim;
- Procedura privind acordarea și retragerea consimțământului;
- Procedura privind managementul persoanelor împuternicite;
- Procedura privind informarea persoanelor vizate;

- Procedura utilizare colaboratori;
- Procedura privind instruirea;
- Procedura solicitare persoană vizată;
- Procedura privind managementul încălcărilor securității datelor cu caracter personal;
- Procedura de notificare a încălcării confidențialității datelor.

5. DEFINIȚII ȘI ABREVIERI ALE TERMENILOR UTILIZAȚI ÎN POLITICA DE SECURITATE

5.1. Definiții ale termenilor

Nr. crt.	Termenul	Definiția și/sau, dacă este cazul, actul care definește termenul
1.	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.
2.	Securitatea informației	Păstrarea confidențialității, integrității și a disponibilității informației.
3.	Confidențialitate	Proprietatea ca informația să nu fie făcută disponibilă sau divulgată unor persoane, entități, sau procese neautorizate.
4.	Integritate	Proprietatea de a proteja acuratețea și completitudinea resurselor.
5.	Disponibilitate	Proprietatea de a fi accesibil și utilizabil la cerere de către o entitate autorizată.
6.	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.
7.	Amenințare	Cauză potențială a unui incident nedorit care poate produce daune unui sistem sau organizații.
8.	Vulnerabilitate	Slăbiciune a unei resurse sau a unui mijloc de control care poate fi exploatată de o amenințare.
9.	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.
10.	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.

5.2. Abrevieri ale termenilor

Nr. crt.	Abrevierea	Termenul abreviat
1.	GDPR	Regulamentul General pentru Protecția Datelor personale
2.	CERT-RO	Centrul național de răspuns la incidente de securitate cibernetica
3.	ISO	

6. POLITICĂ

6.1. Declarație

Informațiile în format olografic, letric sau electronic utilizate în activitățile desfășurate în cadrul Spitalului de Boli Infecțioase și Tropicale "Dr. Victor Babeș" sunt bunuri strategice ale acesteia și trebuiesc administrate ca atare.

Compromiterea securității acestor resurse poate afecta capacitatea Spitalului de Boli Infecțioase și Tropicale "Dr. Victor Babeș" de a oferi servicii de calitate și poate conduce la fraude, incidente legate de confidențialitatea informațiilor, distrugerea informațiilor, violarea unor clauze contractuale sau afectarea credibilității organizației în fața partenerilor săi.

Această politică este stabilită astfel încât:

- să fie în conformitate cu statutul, regulamentele, legile și alte documente oficiale în vigoare privind administrarea resurselor informaționale;
- să stabilească practici prudente și acceptabile privind utilizarea resursele informaționale ale Spitalului de Boli Infecțioase și Tropicale "Dr. Victor Babeș";
- să instruiască utilizatorii care au dreptul de folosire a acestor resurse privind responsabilitățile asociate unei astfel de utilizări.

Politica de securitate a informațiilor se aplică nediscriminatoriu tuturor angajaților, colaboratorilor și angajaților furnizorilor de servicii cărora li s-a permis accesul la orice resursă informațională a Spitalului de Boli Infecțioase și Tropicale "Dr. Victor Babeș". Fiecare angajat, colaborator sau angajat al furnizorilor de servicii este răspunzător pentru aplicarea întocmai în activitatea sa a politicilor și procedurilor de securitate interne în vigoare, elaborate și aprobate, conform cu legislația specifică și reglementările interne de funcționare. De asemenea, fiecare angajat, colaborator sau angajat al furnizorilor de servicii are obligația raportării oricărui incident de securitate sesizat.

6.2. Clasificarea informațiilor

Clasificarea informațiilor este necesară pentru a permite atât alocarea resurselor necesare protejării acestora, cât și pentru a determina pierderile potențiale ca urmare a modificărilor, pierderii/ distrugerii sau divulgării acestora.

Managementul Spitalului de Boli Infecțioase și Tropicale "Dr. Victor Babeș" răspunde de evaluarea periodică a schemei de clasificare a informațiilor.

Toate informațiile din organizație trebuie să se regăsească în una din următoarele categorii:

- Publice: Acestea sunt informații accesibile oricărui utilizator din interiorul sau exteriorul Spitalului de Boli Infecțioase și Tropicale "Dr. Victor Babeș". Divulgarea, utilizarea neautorizată a acestora nu produce efecte asupra organizației sau aceste efecte sunt nesemnificative. Utilizatorii care furnizează aceste informații sunt responsabili de asigurarea integrității și disponibilității acestora în raport cu cerințele Spitalului de Boli Infecțioase și Tropicale "Dr. Victor Babeș". Exemple: Informațiile de pe aviziere, informațiile de pe site-ul web, comunicate de presă ș.a.m.d.
- Confidențiale: Accesul la aceste informații va fi restricționat la persoanele care trebuie să le cunoască pentru îndeplinirea unor activități prevăzute în fișa postului sau în diferite contracte

managementului Spitalului de Boli Infecţioase şi Tropicale "Dr. Victor Babeş". Exemple: informaţii legate de angajaţi, chei criptografice, conturi administrative de pe serverele de gestiune a informaţiilor ş.a.m.d.

- Secrete: Informaţiile pe care Spitalul de Boli Infecţioase şi Tropicale "Dr. Victor Babeş" trebuie să le protejeze conform legislaţiei în vigoare. Aceste date vor fi copiate şi distribuite în cadrul Spitalului de Boli Infecţioase şi Tropicale "Dr. Victor Babeş" doar utilizatorilor autorizaţi.

6.3. Securitatea fizică şi a mediului de lucru

Prelucrările de date şi echipamentele de prelucrare a informaţiilor importante sau sensibile trebuie desfăşurate sau amplasate în zone sigure, protejate de un perimetru de securitate definit. Ele trebuie protejate fizic împotriva accesului neautorizat, deteriorărilor şi intervenţiilor.

Protecţia fizică este realizată prin crearea uneia sau mai multor bariere fizice în jurul incintelor Spitalului de Boli Infecţioase şi Tropicale "Dr. Victor Babeş" şi a sistemelor de prelucrare a informaţiilor. Folosirea barierelor multiple oferă o protecţie suplimentară, în sensul că eşecul unei singure bariere nu înseamnă compromiterea imediată a securităţii.

Spitalul de Boli Infecţioase şi Tropicale "Dr. Victor Babeş" aplică măsuri de protecţie fizică şi împotriva incendiilor, inundaţiilor şi a oricăror alte forme de dezastre naturale sau produse de oameni.

Toate utilităţile suport, precum electricitatea, încălzirea/ ventilaţia sau aerul condiţionat sunt dimensionate corespunzător sistemelor pe care le servesc. Utilităţile suport sunt verificate cu regularitate şi testate pentru a se asigura buna lor funcţionare şi pentru a se reduce riscul funcţionărilor incorecte sau al defectărilor.

Informaţii suplimentare despre securitatea fizică şi a mediului de lucru pot fi găsite în Politica privind securitatea fizică şi a mediului de lucru.

6.4. Securitatea resurselor umane

Spitalul de Boli Infecţioase şi Tropicale "Dr. Victor Babeş" trebuie să aplice măsuri astfel încât angajaţii, colaboratorii şi angajaţii furnizorilor de servicii:

- să înţeleagă responsabilităţile care le revin şi să fie corespunzători pentru rolurile alocate;
- să reducă riscul de furt, fraudă sau de folosire necorespunzătoare a activelor folosite la prelucrarea datelor;
- să fie pregătiţi să susţină şi să aplice politica de securitate a Spitalului de Boli Infecţioase şi Tropicale "Dr. Victor Babeş" pe durata contractului de muncă sau a contractului în baza căruia au acces la informaţii;
- să părăsească Spitalul de Boli Infecţioase şi Tropicale "Dr. Victor Babeş" sau să-şi schimbe locul de muncă într-o manieră reglementată.

Detalii despre măsurile adoptate în cazul resurselor umane pot fi găsite în Politica privind securitatea resurselor umane.

6.5. Securitatea documentelor utilizate

Angajaţii, colaboratorii şi angajaţii furnizorilor de servicii care utilizează documente în format olograf, letric sau pe suport electronic conţinând informaţii confidenţiale (inclusiv date cu caracter personal) sau

mod adecvat împotriva accesului neautorizat atunci când nu le utilizează sau le lăsă nesupravegheate.

Detalii despre măsurile de securitate aplicate în cazul documentelor utilizate pot fi găsite în Politica privind biroul curat, protejarea ecranului și tipărirea documentelor.

6.6. Administrarea conturilor

O mare parte din datele create, colectate sau stocate se bazează pe utilizarea resurselor informatice și de comunicații ale Spitalului de Boli Infecțioase și Tropicale "Dr. Victor Babeș". Organizația investește substanțial în resurse financiare și umane pentru a putea asigura integritatea, confidențialitatea și disponibilitatea acestor sisteme și de aceea aceste resurse trebuie utilizate și administrate corespunzător.

Prin contractul de muncă și/sau alte documente toți utilizatorii acceptă prevederile regulamentelor privind securitatea sistemului informatic și de comunicație.

Având în vedere utilizarea în comun a echipamentelor informatice, conturile de acces la acestea vor putea să fie de tip utilizator unic sau generic. În aces caz sunt aplicabile următoarele reguli:

- toate conturile create trebuie să aibă asociată o cerere și o aprobare corespunzătoare;
- în cazul în care sunt create conturi care identifică în mod unic un utilizator, acestea vor avea formatul prenume.nume sau abrevieri;
- în cazul conturilor generice, denumirea contului trebuie să permită identificarea entității organizatorice ce va utiliza utiliza contul;
- toate parolele pentru conturi trebuie să fie create și folosite în conformitate cu politica privind parolele de acces;
- indiferent de tipul de cont utilizat (unic sau generic), toți utilizatorii sunt obligați să păstreze confidențialitatea informațiilor privind contul de acces folosit.

În cazul conturile de acces în sistemele informatice de gestiune a pacienților, angajaților sau resurselor instituției sunt aplicabile următoarele reguli:

- toate conturile create trebuie să aibă asociată o cerere și o aprobare corespunzătoare;
- conturile trebuie să identifice în mod unic un utilizator;
- toate parolele pentru conturi trebuie să fie create și folosite în conformitate cu politica privind parolele de acces;
- orice cont neutilizat pentru o perioadă de 30 de zile se va bloca automat;
- toți utilizatorii sunt obligați să păstreze confidențialitatea informațiilor privind contul de acces folosit.

Responsabilul IT trebuie să aibă o documentație de modificare a conturilor de utilizator pentru situații precum schimbări ale numelor de familie, modificări privind contul (numele contului), modificări ale drepturilor de utilizator.

6.7. Acordare și retragere accesului la date, sisteme informatice și site-uri web

Acordarea accesului pentru angajați se va face de către Responsabilul IT în urma transmiterii de către Serviciul Resurse Umane a unui formular care va conține detalii legate de utilizator și drepturile acestuia. Formularul se va retrimite în cazul modificării numelui utilizatorului, a drepturilor utilizatorului ca urmare a schimbării postului de lucru sau în cazul încetării contractului de muncă.

Accesul la sistemele informatice și site-urile web utilizate de Spitalul de Boli Infecțioase și Tropicale "Dr. Victor Babeș" se va face conform

Mai multe detalii în Procedura privind accesul angajaților la sistemele informatice.

6.8. Identificare și autentificare

Utilizatorul este responsabil pentru securitatea datelor, a informațiilor de autentificare și a sistemelor aflate sub controlul său.
Utilizatorul trebuie să păstreze credențialele de acces (nume utilizator, parolă, token etc.) în siguranță și să nu le împărtășească nici unei alte persoane, inclusiv colegi, membri ai familiei sau prieteni.
Asigurarea accesului altei persoane, fie în mod deliberat, fie prin incapacitatea de a păstra în siguranță informațiile de autentificare, reprezintă o încălcare a acestei politici.
Nici un angajat nu trebuie, sub nici o formă, să acceseze neautorizat sau să permită accesul neautorizat la informații, fișiere, calculatoare sau alte dispozitive din rețeaua Spitalului de Boli Infecțioase și Tropicale "Dr. Victor Babeș". Acesta este considerat caz de fraudă majoră.

De asemenea sunt interzise:

- încercarea utilizatorilor de a vizualiza și deduce parolele altor utilizatori în timpul introducerii acestora;
- transmiterea de parole în clar prin intermediul sistemelor de comunicații (e-mail, mesagerie instant, SMS etc.);
- afișarea conturilor sau parolelor de acces la echipamente sau sistemul informatic.

La părăsirea calculatorului / aplicației folosite, fiecare utilizator trebuie să aplice măsuri precum blocarea sau închiderea echipamentului și blocarea sau închiderea aplicației utilizate în funcție de: durata de timp până la următoarea utilizare a echipamentului sau aplicației, de securitatea zonei în care este poziționat echipamentul, de folosirea în comun de către mai multe persoane a spațiului în care este poziționat echipamentul, de folosirea în comun de către mai multe persoane a echipamentului și aplicațiilor.

În situații justificate este permisă utilizarea de aplicații autorizate de management al parolelor; totuși folosirea acestor aplicații pentru a stoca parole de domeniu, parole administrative sau parole de acces la aplicații sau servicii critice este interzisă.

6.9. Acces administrativ

Entitățile organizatorice din cadrul Spitalului de Boli Infecțioase și Tropicale "Dr. Victor Babeș" trebuie să prezinte Responsabilului IT o listă cu persoanele de contact cu drept de administrator pentru toate sistemele informatice conectate la rețeaua de comunicații a Spitalului de Boli Infecțioase și Tropicale "Dr. Victor Babeș". Această listă trebuie refăcută și prezentată Responsabilului IT de fiecare dată când apar modificări de orice natură.

Utilizatorii trebuie să cunoască și să accepte toate regulamentele privind securitatea sistemului informatic înainte de a li se permite accesul la un cont.

Utilizatorii care au conturi de acces de tip administrativ trebuie să aibă instrucțiuni de administrare, documentare, instruire și autorizare a conturilor. Aceste instrucțiuni se vor elabora de către fiecare furnizor de sistem informatic și vor fi incluse în fișa postului.

Utilizatorii cu drepturi de acces administrative sau speciale nu trebuie să folosească în mod abuziv aceste drepturi și trebuie să facă investigații numai sub îndrumarea sefului direct.

Cei care utilizează conturi de acces cu drepturi administrative sau speciale trebuie să folosească tipul de privilegiu cel mai potrivit activității pe care o desfășoară

Parola pentru un cont cu acces privilegiat nu va fi utilizată de mai multe persoane decât cu acordul scris al sefului direct şi trebuie să fie schimbată atunci când persoana care utilizează acest cont îşi schimbă locul de muncă în cadrul Spitalului de Boli Infecţioase şi Tropicale "Dr. Victor Babeş", sau în cazul unei modificări a listei de personal care furnizează servicii din partea terţilor având contracte cu organizaţia.

Unele conturi sunt necesare pentru audit (verificare, control) intern sau extern, pentru dezvoltare sau instalare de software sau alte operaţiuni definite. Acestea trebuie să îndeplinească următoarele condiţii:

- trebuie să fie autorizate;
- trebuie create cu dată de expirare specifică;
- contul va fi şters atunci când nu mai este necesar.

6.10. Accesul la reţeaua de comunicaţii

Utilizatorilor le este permis să utilizeze numai parametrii pentru conectare la reţea specificaţi de către Responsabilul IT.

Şefii entităţilor organizatorice trebuie să aprobe, în scris, conectarea dispozitivelor de calcul la reţeaua de comunicaţii a Spitalului de Boli Infecţioase şi Tropicale "Dr. Victor Babeş". Pentru fiecare sistem conectat trebuie să existe o persoană care să răspundă de acesta, numele şi datele de identificare ale acesteia se vor comunica către Responsabilul IT.

Conectarea sistemelor de calcul care nu sunt proprietatea Spitalului de Boli Infecţioase şi Tropicale "Dr. Victor Babeş" se face numai cu aprobarea în scris a şefului direct al solicitantului.

Accesul de la distanţă la reţeaua Spitalului de Boli Infecţioase şi Tropicale "Dr. Victor Babeş" se va realiza numai prin echipamente aprobate, folosind protocoale aprobate de către Responsabilul IT şi managementul Spitalului de Boli Infecţioase şi Tropicale "Dr. Victor Babeş".

Utilizatorii din interiorul reţelei de comunicaţie a Spitalului de Boli Infecţioase şi Tropicale "Dr. Victor Babeş" nu se pot conecta la altă reţea.

Utilizatorii nu trebuie să extindă sau să retransmită serviciile de reţea în nici un fel (pe nici o cale). Nu este permisă instalarea de conexiuni de reţea neautorizate indiferent de motiv.

Utilizatorii nu trebuie să instaleze echipamente hardware sau programe care furnizează servicii de reţea fără aprobarea Responsabilului IT.

Sistemele computerizate din afara Spitalului de Boli Infecţioase şi Tropicale "Dr. Victor Babeş" care necesită conectare la reţea trebuie să se conformeze cu standardele reţelei interne ale Spitalului de Boli Infecţioase şi Tropicale "Dr. Victor Babeş".

Utilizatorii nu au dreptul să descarce, să instaleze sau să ruleze programe de securitate care pot dezvălui slăbiciuni în securitatea unui sistem. De exemplu, utilizatorii Spitalului de Boli Infecţioase şi Tropicale "Dr. Victor Babeş" nu au dreptul să ruleze programe de spargere a parolei, sustragere de pachete, scanare a porturilor, în timp ce sunt conectaţi la reţeaua Spitalului de Boli Infecţioase şi Tropicale "Dr. Victor Babeş".

Utilizatorii nu au dreptul să modifice, reconfigureze, instaleze, dezinstaleze echipamente de reţea, cabluri, prize de conexiuni.

Serviciul de administrare a numelor şi adreselor IP este deservit exclusiv de către Responsabilul IT.

Serviciile de interconectare a rețelei Spitalului de Boli Infecțioase și Tropicale "Dr. Victor Babeș" cu alte rețele sunt realizate exclusiv de către Responsabilul IT.

Nu este permisă instalarea și/sau modificarea echipamentelor utilizate pentru conectare la rețea (inclusiv plăci de rețea) fără aprobarea Responsabilului IT. Tipul și modelul plăcilor de rețea și tuturor echipamentelor care se pot conecta în rețea trebuie să fie aprobate de către Responsabilul IT.

6.11. Configurarea sistemelor informatice pentru accesul la rețeaua de comunicații

Infrastructura de comunicații și rețeaua de comunicații digitale a Spitalului de Boli Infecțioase și Tropicale "Dr. Victor Babeș" este administrată de către Responsabilul IT, care este responsabil cu întreținerea și dezvoltarea acesteia.

Pentru a furniza o infrastructură de comunicații unitară cu posibilități de modernizare, toate componentele acesteia sunt instalate de către Responsabilul IT sau de către un furnizor avizat explicit de către Responsabilul IT.

Toate echipamentele, fără excepție, conectate la rețeaua de comunicații trebuie configurate conform specificațiilor Responsabilului IT.

Toate dispozitivele hardware, inclusiv plăcile de rețea, care se vor conecta la rețeaua Spitalului de Boli Infecțioase și Tropicale "Dr. Victor Babeș", trebuie să fie însoțite de o aprobare tip (producător, model etc.) din partea Responsabilului IT.

Modificarea configurației oricărui dispozitiv activ conectat la rețeaua de comunicații se face numai cu aprobarea Responsabilului IT.

Infrastructura de comunicații de date a Spitalului de Boli Infecțioase și Tropicale "Dr. Victor Babeș" suportă un set definit de protocoale de rețea (TCP/IP). Orice utilizare a altui set de protocoale trebuie să fie aprobată în scris de către Responsabilul IT.

Adresele de rețea sunt alocate dinamic sau static numai de către Responsabilul IT.

Toate conectările în rețeaua de comunicații a Spitalului de Boli Infecțioase și Tropicale "Dr. Victor Babeș" reprezintă sarcină a Responsabilului IT, conectarea se va face numai în baza unei cereri standard aprobată de către șeful direct.

Toate conectările dintre rețeaua de comunicații a Spitalului de Boli Infecțioase și Tropicale "Dr. Victor Babeș" și alte rețele de comunicații, publice sau private, sunt responsabilitatea exclusivă a Responsabilului IT.

Echipamentele de protecție a rețelei de comunicație a Spitalului de Boli Infecțioase și Tropicale "Dr. Victor Babeș" (firewall) se vor instala de către Responsabilul IT.

Utilizatorii nu au dreptul să extindă sau să retransmită în nici un fel serviciile rețelei (este interzisă instalarea unui modem, router, switch, hub sau punct de acces la rețeaua Spitalului de Boli Infecțioase și Tropicale "Dr. Victor Babeș") fără aprobare din partea Responsabilului IT.

Utilizatorilor li se interzice instalarea de dispozitive hardware de rețea sau de programe care furnizează servicii de rețea fără aprobarea Responsabilului IT.

Utilizatorilor nu le este permis accesul la dispozitivele hardware ale rețelei.

6.12. Utilizarea echipamentelor

Utilizatorul este responsabil de păstrarea în siguranță și folosirea corectă în scopurile destinate și autorizate a echipamentelor care i-au fost puse la dispoziție de organizație. Acestea includ stații de lucru fixe și mobile, imprimante, telefoane mobile și fixe și alte mijloace de procesare a informațiilor, inclusiv software-ul asociat.

Toate stațiile de lucru trebuie să fie asigurate împotriva accesului neautorizat atunci când sunt lăsate nesupravegheate. Aceasta se poate face prin blocarea calculatorului, log off sau cu un screensaver protejat cu parolă, cu funcția de activare automată setată la 5 minute sau mai puțin. La sfârșitul programului de lucru acestea, precum și orice aparatură electrică și electronică, trebuie să fie oprite.

De asemenea:

- CD-urile, DVD-urile, alte medii de stocare nu trebuiesc lăsate la vedere atunci când nu sunt folosite.
- Daca ele conțin date de maximă confidențialitate, trebuie să fie ținute sub cheie.
- CD-urile, DVD-urile, mediile de stocare mobile trebuie păstrate departe de acțiunile mediului înconjurător cum ar fi: surse de căldura, lumina directă a soarelui și câmpuri magnetice.

Dispozitivele care nu aparțin Spitalului de Boli Infecțioase și Tropicale "Dr. Victor Babeș" și care se conectează la rețeaua organizației trebuie să se conformeze *Procedurii privind utilizarea echipamentelor de proprietate personală*. Echipamentele conectate fără autorizare sunt expuse monitorizării și vor fi blocate fără avertisment de îndată ce sunt detectate.

Următoarele acțiuni sunt strict interzise utilizatorilor:

- modificarea sau eliminarea măsurilor de securitate, inclusiv, dar fără a se limita la: dezinstalarea sau dezactivarea antivirusului ori modificarea setărilor de actualizare ale acestuia (actualizarea automată trebuie să fie activă), dezactivarea sau modificarea setărilor firewall-ului,
- instalarea de software neautorizat (vezi Lista de software autorizat) sau pentru care nu există licență valabilă la zi,
- interferența cu procedurile organizației referitoare la managementul dispozitivelor, inclusiv, dar fără a se limita la: schimbarea sau reinstalarea sistemului de operare, redenumirea calculatorului, scoaterea din domeniu, instalarea neautorizată de dispozitive suplimentare,
- modificarea configurației hardware a echipamentului,
- scoaterea echipamentului în afara locației fără autorizare prealabilă,
- introducerea și utilizarea de produse care pun în pericol securitatea informațiilor (dispozitive sau software de ascultare, conectare, înregistrare sau copiere neautorizată) sau a personalului (arme de orice fel, produse toxice sau explozive etc.),
- eliminarea nesigură a mediilor de stocare sau a echipamentelor care au în componență medii de stocare.

6.13. Securitatea echipamentelor și resurselor în afara locației organizației

Folosirea echipamentelor în afara locației organizației crește riscurile de securitate ale acestora, echipamentele fiind în special vulnerabile la daune fizice, pierdere și furt. În acest caz, se vor aplica următoarele măsuri de securitate:

1. Echipamentul va fi instalat conform *Procedură instalare echipamente* ;
2. În momentul părăsirii organizației, echipamentul poate fi utilizat pentru resursele online (ex. e-

3. Update-urile aplicaţiilor (de exemplu: sistem de operare, antivirus, Suita Office etc.) se vor face doar la revenirea cu echipamentul în reţeaua Spitalului de Boli Infecţioase şi Tropicale "Dr. Victor Babeş". Utilizatorul are obligaţia ca la un interval de maximum 2 săptămâni să introducă echipamentul în reţeaua internă a Spitalului de Boli Infecţioase şi Tropicale "Dr. Victor Babeş" pentru actualizări ;
4. Accesul la aplicaţiile de pe serverele Spitalului de Boli Infecţioase şi Tropicale "Dr. Victor Babeş" se va face prin VPN cu aprobarea şefului direct, aprobarea pentru utilizarea VPN-ului fiind comunicată Responsabilului IT;
5. Documentele personale (valabil pentru toate echipamentele) se vor ţine într-un folder "Personal".

Furtul sau pierderea unui echipament scos în afara Spitalului de Boli Infecţioase şi Tropicale "Dr. Victor Babeş" vor fi raportate imediat şefului ierarhic şi Responsabilului IT.

Detalii suplimentare în *Politica privind dispozitivele mobile şi lucrul de la distanţa.*

6.14. Utilizarea echipamentelor proprietate personală

Spitalul de Boli Infecţioase şi Tropicale "Dr. Victor Babeş" poate permite angajaţilor sau persoanelor terţe să folosească echipamente proprietate personală (EPP) pentru îndeplinirea sarcinilor de serviciu.

Următoarele echipamente proprietate personală sunt permise:

a) dispozitive de tip smartphone având sisteme de operare: iOS, Android, Blackberry sau Windows;
b) tablete având sisteme de operare: iOS, Android, Windows;
c) laptop-uri;
d) dispozitive de stocare portabile: stick-uri de memorie USB, carduri de memorie, hard-disk-uri portabile etc.

Utilizarea echipamentelor proprietate personală este asociată cu o serie de riscuri de securitate a informaţiilor, cum ar fi:

- pierderea, dezvăluirea sau alterarea informaţiilor Spitalului de Boli Infecţioase şi Tropicale "Dr. Victor Babeş" stocate pe EPP;
- incidente care implică ameninţări la adresa infrastructurii informatice a organizaţiei sau compromiterea acestei infrastructuri (de exemplu: viruşi, malware, hacking);
- nerespectarea legilor, reglementărilor şi obligaţiilor contractuale (de exemplu, protecţia datelor cu caracter personal, legislaţia anti-piraterie etc.);
- nerespectarea drepturilor de proprietate intelectuală pentru informaţiile organizaţiei create, stocate, procesate sau transmise pe EPP.

Angajaţii care folosesc EPP pentru îndeplinirea sarcinilor de serviciu trebuie să fie autorizaţi în mod explicit să facă acest lucru. Autorizarea va fi dată de Responsabilul IT la cererea şefului direct ca răspuns la o solicitare în care este explicat motivul solicitării. Pentru autorizare, Responsabilul IT va putea cere informaţii despre EPP care va fi utilizat.

Utilizatorii trebuie să asigure aceleaşi măsuri de protecţie a informaţiilor ca şi cele aplicate pentru echipamentele Spitalului de Boli Infecţioase şi Tropicale "Dr. Victor Babeş" şi nu trebuie să introducă riscuri inacceptabile (exemplu: malware) în reţeaua organizaţiei prin utilizarea de echipamente nesigure.

Spitalul de Boli Infecţioase şi Tropicale "Dr. Victor Babeş" îşi rezervă dreptul de a refuza sau de a retrage autorizarea în cazul în care consideră că echipamentul nu este adecvat și/sau nu este folosit în interesul

În timp ce utilizatorii au o așteptare rezonabilă de intimitate asupra informațiilor lor personale pe propriul echipament, dreptul Organizației de a controla propriile date și de a gestiona EPP poate duce ocazional la accesul neintenționat al personalului de asistență la informațiile lor personale. Pentru a reduce posibilitatea unui astfel de acces, utilizatorii trebuie să păstreze datele lor personale separat de datele Organizației, în directoare separate, denumite în mod sugestiv.

6.15. Securizarea serverelor

Un server nu trebuie conectat la rețeaua Spitalului de Boli Infecțioase și Tropicale "Dr. Victor Babeș" până când nu se află într-o stare sigură, acreditată de către Responsabil IT.

Procedura de securizare a serverelor trebuie să includă obligatoriu următoarele:

- Instalarea sistemului de operare dintr-o sursă aprobată;
- Aplicarea patch-urilor furnizate de producător;
- Înlăturarea programelor, a serviciilor sistem și a driver-lor care nu sunt necesare;
- Setarea/activarea parametrilor de securitate, a protecțiilor pentru fișiere și activarea jurnalelor de monitorizare;
- Dezactivarea sau schimbarea parolelor conturilor predefinite;
- Securizarea accesului fizic la aceste echipamente.

Responsabilul IT va monitoriza obligatoriu pentru serverele principale, procesul de instalare și aplicarea regulată a patch-urilor de securitate.

6.16. Detectarea accesului neautorizat

Procesele de înregistrare și verificare a activității sistemelor de operare, conturilor utilizator și programelor trebuie să fie funcționale pe toate sistemele active (host, server, echipamente de rețea).

Trebuie activate funcțiile de anunțare a persoanelor responsabile oferite de firewall-uri și sistemele de control al accesului la rețea.

Trebuie activate funcțiile de înregistrare a evenimentelor pe dispozitivele firewall și pe toate sistemele de control al accesului.

Înregistrările de verificare ale dispozitivelor de control al accesului trebuie monitorizate/revizuite (examinate) zilnic de către Responsabilul IT.

Verificările privind integritatea fiecărui sistem trebuie să se facă periodic. Această activitate este obligatorie și pentru dispozitivele de tip firewall sau dispozitive de control al accesului.

Înregistrările de verificare pentru serverele din rețeaua internă trebuie revizuite cel puțin săptămânal.

Se vor verifica periodic programele utilitare pentru detectarea tentativelor de acces neautorizat.

Toate rapoartele privind incidentele trebuie verificate în vederea detectării de indicii ce ar putea implica o activitate de acces neautorizat.

Toate indiciile suspecte sau confirmate de accesări sau încercări de accesare neautorizate trebuie raportate imediat către Responsabilul IT.

Utilizatorii sunt obligați să raporteze orice anomalii în performanța sistemelor utilizate cât și orice semne ale unor posibile infracțiuni la Responsabilul IT.

6.17. Modificări ale configurației sistemului

Orice modificare asupra unei componente a configurației sistemului din cadrul Spitalului de Boli Infecțioase și Tropicale "Dr. Victor Babeș", cum ar fi: sisteme de operare, componente hardware, echipamente și componente de rețea, aplicații, este supusă prezentului regulament și trebuie să urmeze procedurile în vigoare.

Toate modificările care afectează mediul de funcționare a sistemelor componente ale sistemului informatic (ex: aparate de aer condiționat, instalații de apă, încălzire, instalații electrice și alarme) trebuie să fie anunțate și aprobate în scris de departamentul care administrează resursele afectate.

Toate propunerile de modernizare și extindere a elementelor de infrastructură ale sistemului informatic vor fi documentate și aprobate de către Responsabilul IT. Nu este permisă modificarea de către utilizatori a elementelor de infrastructură ale sistemului informatic.

Modificările și modernizările sistemelor de calcul vor fi documentate de către utilizator și aprobate de către conducerea departamentului sau de către managementul organizației.

Modificările planificate trebuie anunțate cu cel puțin 48 ore înainte de a fi executate.

Cererile de modificare planificate pot fi respinse în următoarele cazuri: planificare inadecvată, planuri de refacere a serviciilor inadecvate, durata modificării poate afecta în mod negativ o activitate importantă a Organizației sau resursele corespunzătoare necesare nu pot fi disponibile imediat.

Se va întocmi un raport pentru orice modificare, indiferent dacă a fost planificată sau neplanificată, sau dacă s-a realizat sau nu cu succes.

Trebuie întreținută o bază de date care să cuprindă toate modificările. Aceasta trebuie să conțină cel puțin următoarele informații:

- data la care s-a făcut cererea pentru modificare și data la care s-a făcut modificarea;
- informații de contact pentru utilizator;
- natura modificării;
- indicarea succesului sau nereușitei modificări.

6.18. Utilizarea rețelei Internet și Intranet

Programele pentru acces la rețeaua Internet sunt destinate utilizatorilor autorizați pentru a fi folosite în scopul desfășurării activității specificate în fișa postului.
Utilizatorul care folosește Internetul, e-mail-ul sau resurse de pe Internet este obligat:

1. să se asigure că toate comunicațiile se fac în scopuri profesionale și nu interferează cu productivitatea personală.
2. să fie responsabili pentru conținutul materialelor – text, imagine, audio sau de altă natură care plasează sau trimite pe Internet. Toate comunicațiile vor avea atașate numele angajatului.
3. angajatul este obligat să cunoască și să respecte politica privind securitatea informațiilor și politicile și procedurile asociate acesteia și de asemenea să păstreze secretul înregistrărilor la nivel personal sau de grup definit prin această politică.

Toate programele utilizate pentru acces la rețeaua Internet trebuie să facă parte din pachetul de programe aprobat de către Responsabilul IT. Aceste programe trebuie să includă toate patch-urile de securitate puse la dispoziție de către producător.

Toate fişierele care provin din reţeaua Internet trebuie să fie scanate cu un program antivirus care să fie actualizat cel puţin o dată la 24 ore.

Toate programele pentru acces Internet/Intranet trebuie să permită folosirea sistemelor proxy şi/sau firewall.

Orice activitate a utilizatorilor folosind sistemul informatic poate fi înregistrată şi ulterior examinată.

Nu este permisă utilizarea sistemelor informatice ale Spitalului de Boli Infecţioase şi Tropicale "Dr. Victor Babeş" în scop personal sau pentru solicitări personale ce nu au legătură cu organizaţia.
Angajaţilor ce utilizează Internetul nu le este permis să copieze, transfere, redenumească, adauge sau să şteargă informaţii sau programe ce aparţin altor persoane exceptând situaţia când li s-a permis acest lucru. Încălcarea drepturilor de autor sau a contractelor de licenţe vor duce la sancţiuni disciplinare din partea Spitalului de Boli Infecţioase şi Tropicale "Dr. Victor Babeş" şi/sau acţiuni în instanţă ale deţinătorului dreptului de autor.

6.19. Site-uri web aparţinând Spitalului de Boli Infecţioase şi Tropicale "Dr. Victor Babeş"

Toate site-urilor web aparţinând Spitalului de Boli Infecţioase şi Tropicale "Dr. Victor Babeş" trebuie să se supună regulilor stabilite la nivelul organizaţiei din punct de vedere al aspectului şi al securităţii.
Nu se vor publica pe site-urile web ale Spitalului de Boli Infecţioase şi Tropicale "Dr. Victor Babeş" materiale cu caracter ofensiv sau de hărţuire.
Orice material confidenţial al Spitalului de Boli Infecţioase şi Tropicale "Dr. Victor Babeş" transmis prin reţeaua Internet trebuie criptat.

6.20. Mijloace de comunicaţie

Adresa de e-mail furnizată de Spitalul de Boli Infecţioase şi Tropicale "Dr. Victor Babeş" şi mailbox-ul asociat acesteia, adresa IP şi, după caz, numărul de telefon fix, telefon mobil şi conexiunea de date mobile sunt resurse puse la dispoziţia utilizatorilor de organizaţie pentru a fi folosite la îndeplinirea sarcinilor de serviciu. Utilizarea ocazională în scop personal a acestora este permisă numai dacă nu afectează într-o măsură perceptibilă consumul de resurse al organizaţiei şi nu introduce riscuri suplimentare pentru organizaţie.

Următoarele acţiuni sunt strict interzise utilizatorilor:

- utilizarea necorespunzătoare a mijloacelor de comunicare, inclusiv, dar fără a se limita la: sprijinirea activităţilor ilegale, procurarea şi distribuirea de materiale sau mesaje cu caracter ofensator, rasist, obscen, discriminator sau în scop de hărţuire, defăimare sau ameninţare,
- procurarea şi distribuirea neautorizată de materiale protejate de drepturile de autor (imagini, muzică, filme, mărci şi logo-uri ale altor companii preluate din reviste, ziare, cărţi sau de pe Internet),
- transmiterea de materiale protejate prin legea dreptului de autor fără permisiunea expresă,
- utilizarea mijloacelor de comunicare pentru publicitate neautorizată, relaţii de afaceri care nu implică sau sunt contrare intereselor Spitalului de Boli Infecţioase şi Tropicale "Dr. Victor Babeş", campanii politice, utilizarea în scop distractiv sau orice alte scopuri care nu au legătură cu activitatea organizaţiei,
- trimiterea de spam sau bombe e-mail prin intermediul sistemului de e-mail, mesajelor text, mesageriei instant, mesageriei vocale sau altor forme de comunicare electronică utilizate,

- falsificarea, denaturarea, ascunderea, suprimarea sau înlocuirea unei identități de utilizator, pe orice mijloc de comunicare electronică, cu scopul de a induce în eroare destinatarul cu privire la identitatea expeditorului,
- postarea sau transmiterea de mesaje non-business identice sau similare către un număr mare de destinatari (news-group spam),
- transmiterea de informații confidențiale sau secrete de serviciu altor destinatari decât cei autorizați să primească aceste informații,
- utilizarea adresei de e-mail sau a adresei IP pentru a se angaja în activități care încalcă politicile sau orientările organizației; postarea pe grupuri publice de știri, forumuri sau rețele sociale folosind adresa de e-mail sau adresa IP ale organizației, reprezintă compania în fața publicului și prin urmare trebuie efectuată cu discernământ pentru a evita reprezentarea greșită sau depășirea autorității de a reprezenta poziția organizației.

Orice mesaj și/sau informație trimisă prin intermediul rețelelor publice pot fi identificate și atribuite Spitalului de Boli Infecțioase și Tropicale "Dr. Victor Babeș". Din acest motiv, postarea pe forumuri sau alte site-uri de informații care implică numele sau adrese de e-mail ale Spitalului de Boli Infecțioase și Tropicale "Dr. Victor Babeș" se va face fără furnizarea de informații confidențiale sau care pot afecta reputația organizației. Părerile personale exprimate pe astfel de site-uri sau forumuri vor fi însoțite de nota: "Părerile exprimate sunt personale și nu reprezintă poziția oficială a Spitalului de Boli Infecțioase și Tropicale "Dr. Victor Babeș". "

6.21. Utilizarea resurselor informatice în scop personal

Mijloacele de procesare a informației puse la dispoziție de Spitalul de Boli Infecțioase și Tropicale "Dr. Victor Babeș" sunt destinate în primul rând îndeplinirii sarcinilor de serviciu.

Utilizarea limitată în scopuri personale, ocazională sau accidentală, a mijloacelor de procesare a informației este de înțeles și acceptabilă, cu condiția ca ea să se facă într-o manieră care să nu afecteze negativ utilizarea acestora pentru scopul principal. Utilizatorii trebuie să demonstreze simț de responsabilitate și să nu abuzeze de acest drept.

Stocarea e-mail-urilor, documentelor și altor fișiere personale nu este încurajată. În cazul în care acestea sunt totuși păstrate, vor fi stocate local și nu pe serverele organizației, în locații separate de cele care conțin informații ce aparțin organizației. Toate mesajele și fișierele personale aflate în sistemul informatic pot fi supuse verificării de conformitate cu politica privind securitatea informațiilor.

Spitalul de Boli Infecțioase și Tropicale "Dr. Victor Babeș" nu își asumă nicio responsabilitate cu privire la securitatea acestor informații, întreaga responsabilitate (inclusiv realizarea copiilor de siguranță) revenind utilizatorului.

6.22. Detectarea virușilor

Toate stațiile de lucru de sine stătătoare sau conectate la rețeaua de comunicații a Spitalului de Boli Infecțioase și Tropicale "Dr. Victor Babeș", trebuie să utilizeze programe antivirus aprobate de către Responsabilul IT.

Programele antivirus nu trebuie dezactivate.

Configurația programului antivirus trebuie să nu fie modificată într-un mod care să reducă eficacitatea programului

Frecvența actualizărilor automate a programului antivirus trebuie asigurată de către utilizator.

Orice server de fișiere conectat la rețeaua organizației trebuie să utilizeze un program antivirus aprobat în scopul detectării și curățirii virușilor care pot infecta fișierele puse la dispoziție.

Orice server sau gateway pentru e-mail trebuie să folosească un program antivirus pentru e-mail aprobat și trebuie să respecte regulile de instalare și utilizare a acestui program.

Orice virus care nu a putut fi înlăturat automat de către programul antivirus constituie un incident de securitate și trebuie raportat imediat Responsabilului IT.

6.23. Returnarea resurselor la terminarea contractului

Utilizatorul va returna organizației, la încetarea contractului de muncă sau de servicii, orice informații și orice mijloace de procesare a informațiilor puse la dispoziția sa în scopul îndeplinirii atribuțiilor de serviciu sau obligațiilor contractuale. Acestea includ și nu se limitează la: credențialele de acces la sisteme critice, primite sau modificate pe perioada contractului ș.a.m.d.

6.24. Protecția datelor cu caracter personal

În activitățile din cadrul Spitalului de Boli Infecțioase și Tropicale "*Dr. Victor Babeș*" se creează, colectează, stochează și prelucrează cantități mari de date din diverse categorii de date cu caracter personal, aparținând unor tipuri diferite de persoane vizate, cum ar fi angajați, candidați posturi vacante, pacienți, clienți/ furnizori sau alte categorii de persoane.

Protecția datelor personale este o componentă importantă a oricărei activități, astfel că toate informațiile trebuie să fie prelucrate în siguranță și în conformitate cu politica stabilită. Pe lângă bunele practici stabilite la nivelul instituției, anumite categorii de date sunt supuse și reglementărilor legislației naționale și este vital ca personalul să recunoască toate detaliile legate de manipularea informațiilor și datelor Spitalului de Boli Infecțioase și Tropicale "*Dr. Victor Babeș*".

Respectarea cerințelor legate de protecția datelor cu caracter personal este responsabilitatea tuturor membrilor Spitalului de Boli Infecțioase și Tropicale "*Dr. Victor Babeș*". Orice încălcare deliberată a acestei politici poate conduce la măsuri disciplinare, la retragerea accesului la facilitățile Spitalului de Boli Infecțioase și Tropicale "*Dr. Victor Babeș*" sau chiar la urmărirea penală. Informații suplimentare despre protecția datelor cu caracter personal pot fi găsite în *Politica privind protecția datelor și în procedurile aferente acesteia.*

6.25. Conștientizare și instruire cu privire la securitatea informației

Toți angajații Spitalului de Boli Infecțioase și Tropicale *"Dr. Victor Babeș"*, colaboratorii sau angajații furnizorilor de servicii trebuie să fie conștientizați sau instruiți cu privire a politicile și procedurile organizaționale corespunzătoare fiecarui loc de muncă sau activități desfășurate. În acest scop, șefii entităților organizatorice trebuie să stabilească un program de instruire a personalului din subordine cu privire la cerințele legate de securitatea informațiilor aplicabile pentru fiecare loc de muncă sau activități desfășurate.

6.26. Relațiile cu furnizorii

Unele din activitățile desfășurate în cadrul Spitalului de Boli Infecțioase și Tropicale "*Dr. Victor Babeș*"

Victor Babeș" recurge doar la furnizori de servicii care oferă garanții suficiente pentru punerea în aplicare a măsurilor tehnice și organizatorice prevăzute de politica de securitate și de politicile și procedurile asociate acesteia.

Activitatea desfășurată de către un furnizor de servicii trebuie reglementată printr-un contract sau alt act juridic care are caracter obligatoriu pentru furnizorul de servicii și care trebuie să stabilească cel puțin durata desfășurării activităților, natura activităților desfășurate și măsurile tehnice și organizatorice ce trebuie implementate de furnizor sau respectate de către angajații furnizorului de servicii.

În cazul în care o prelucrare de date cu caracter personal urmează să fie realizată în asociere între doi sau mai mulți operatori, trebuie încheiat un acord, contract sau alt act juridic care să precizeze responsabilitățile fiecărei părți în ceea ce privește îndeplinirea obligațiilor care le revin în temeiul *Regulamentului GDPR*, în special cu privire la modul de exercitare a drepturilor persoanelor vizate și îndatoririle fiecărei parti de furnizare a informațiilor către persoanele vizate de prelucrări.

Detalii despre măsurile de securitate aplicate în cazul relațiilor cu furnizorii pot fi găsite în *Politica privind relațiile cu furnizorii.*

6.27. Managementul evenimentelor legate de încălcărea securității datelor

Toți angajații Spitalului de Boli Infecțioase și Tropicale "Dr. Victor Babeș", colaboratorii, persoanele împuternicite trebuie să ia cunoștință despre procedurile de raportare a diverselor tipuri de evenimente legate de încălcărea securității datelor cu caracter personal, si, în cazul identificarii unui eveniment legat de încălcărea securității datelor, să le raporteze, în cel mai scurt timp, în punctul de contact desemnat, într-un mod care să permită luarea măsurilor corective necesare în timp util precum și anuntarea, în cazul în care este necesar, Autorității Naționale de Supraveghere sau a persoanelor vizate.

6.28. Măsuri disciplinare

Toți angajații Spitalului de Boli Infecțioase și Tropicale "Dr. Victor Babeș", colaboratorii sau angajații furnizorilor de servicii sunt obligați să respecte această politică de securitate a informațiilor precum și politicile și procedurile asociate acesteia.

Încălcarea prevederilor politicii de securitate a informațiilor sau a politicilor și procedurile asociate acesteia poate face obiectul unor măsuri disciplinare, civile, contravenționale ori penale, în raport cu gravitatea faptei săvârșite.

7. RESPONSABILITĂȚI

7.1. Comitetul Director

Managementul Spitalului de Boli Infecțioase și Tropicale "Dr. Victor Babeș" are următoarele responsabilități:

- Stabilește și aprobă *Politica generală de securitate a informațiilor*, politicile subsecvente și obiectivele de securitate a informațiilor;
- Asigură disponibilitatea resurselor necesare pentru managementul securității informațiilor;
- Comunică importanța unei gestionări eficiente a securității informației și a respectării cerințelor sistemului de management al securității informațiilor.

7.2. Responsabilul IT

Responsabilul IT are următoarele responsabilități:

- Propune modificări ale politicilor legate de IT și procedurilor aferente acesteia;
- Tratează incidentele de securitate în scopul minimizării efectului distructiv al acestora asupra resurselor informatice și de comunicații;
- Informează conducerea în caz de incidente, intervenție și rezolvarea incidentelor de securitate a informațiilor;
- Asigură existența jurnalelor și a traseelor auditării pentru orice tip de acces în sistem conform procedurilor asociate;
- Planifică, implementează și verifică soluțiile de securitate a informațiilor: server antivirus, firewall, server de actualizări de securitate, backup, acces securizat la camera tehnică, asigurare aer condiționat, asigurare alimentare cu energie electrică/UPS;
- Menține înregistrări privind configurația, aplicațiile și serviciile instalate, pentru a se putea reface sistemul în caz de dezastru;
- Inventariază periodic aplicațiile și serviciile instalate și verifică dacă sunt autorizate;
- Administrează sistemele IT și aplică măsurile de securitate și alte cerințe ale programului de securitate a informațiilor pentru sistemele informatice pentru care are atribuită responsabilitatea.

7.3. Șefii structurilor organizatorice

Șefii entităților organizatorice sunt responsabili pentru:

- Implementarea de zi cu zi a politicilor si procedurile de securitate a informațiilor;
- Instruirea personalului din subordine cu privire la cerințele legate de securitatea informațiilor aplicabile pentru fiecare loc de muncă;
- Asigurarea că măsurile de securitate tehnice, fizice și procedurale adecvate sunt implementate în conformitate cu politicile și procedurile de securitate și sunt aplicate în mod corespunzător și de către tot personalul;
- Asigurarea resurselor și efectuarea analizelor necesare pentru a se asigura că informațiile și activele informaționale sunt protejate în mod corespunzător în zona lor de responsabilitate;
- Informarea persoanei desemnate cu managementul incidentelor de securitate despre încălcările reale sau presupuse ale politicilor de securitate care afectează securitatea informațiilor din zona lor de responsabilitate (incidentele de securitate a informațiilor);
- Identificarea și clasificarea informațiilor și activelor informaționale semnificative din zona lor de responsabilitate și desemnarea deținătorilor (responsabililor) pentru acestea;
- Informarea *Responsabilului IT* la schimbarea responsabililor de active informaționale.

7.4. Angajații Spitalului de Boli Infecțioase și Tropicale "Dr. Victor Babeș"

Angajații au următoarele responsabilități:

- Respectă toate politicile și procedurile privind securitatea informațiilor aplicabile pentru locurile lor de muncă;
- Participă la instruirile legate de securitatea informațiilor;
- Sunt responsabili pentru menținerea securității si confidențialității tuturor informațiilor încredințate;
- Informează șefii entităților organizatorice despre încălcările reale sau presupuse ale politicilor de securitate și confidențialitate a datelor din zona lor de responsabilitate (incidente privind securitatea sau confidențialitatea datelor).

7.5. Colaboratorii și angajații furnizorilor de servicii

Colaboratorii și angajații furnizorilor de servicii, au următoarele responsabilități:

- Respectă toate politicile și procedurile privind securitatea informațiilor și de protecție a datelor aplicabile pentru informațiile la care au acces;
- Răspund direct de securitatea și conținutul informațiilor și resursele informatice și de comunicații încredințate direct sau indirect;
- Informează persoanele de contact despre încălcările reale sau presupuse ale securității sau confidențialității datelor;
- Returnează informațiile încredințate în momentul încheierii relației contractuale sau în momentul solicitării returnării acestora de către organizație.

8. FORMULAR DE EVIDENȚĂ A MODIFICĂRILOR

	Ediția sau, după caz revizia din cadrul ediției	Componenta revizuită	Modalitatea reviziei	Data la care se aplică prevederile ediției sau reviziei ediției
0	1	2	3	4
1.1	Ediția I, Revizia 0	-	-	După aprobarea dată de managerul instituției, se afișează pe site-ul SVB și în rețeaua spitalului, în *Documente SVB.*