ISO 9001 • ISO 14001 • ISO 18001 • ISO 22000
LL-C (Certification)
ANMCS
unitate aflată în
PROCES DE ACREDITARE

CONSILIUL JUDEȚEAN HUNEDOARA
SPITALUL JUDEȚEAN DE URGENȚĂ DEVA
Deva, 330084, Bd. 22 Decembrie, nr.58, jud. Hunedoara
Cod fiscal: 4374385
Secretariat: tel.: 0254 214616, fax: 0254 212516
Centrala telefonică: 0254 227070, 0254 217799, 0734 661888
e-mail. spjudeva1@gmail.com

Nr.inreg: 27506 / 19.10.2021

Manager interimar
DR. EMIL STOICA-MARIȘ

REGULAMENT
privind utilizarea şi securitatea Sistemelor Informatice şi de Comunicaţii din cadrul SPITALULUI JUDEŢEAN DE URGENŢĂ DEVA

Capitolul 1. INTRODUCERE

În acord cu prevederile din prezentul regulament , Sistemele Informatice şi de Comunicaţii puse la dispoziţie şi administrate de către Serviciul de Informatică sunt bunuri strategice ale Spitalului Judeţean de Urgenţă Deva care trebuie administrate ca resurse ale statului român.

Compromiterea securităţii acestora poate afecta capacitatea spitalului de a oferi servicii informatice şi de comunicaţii, poate conduce la fraude sau distrugerea datelor, la violarea clauzelor contractuale, divulgarea secretelor, la afectarea credibilităţii şi imaginii SPJU Deva în faţa partenerilor săi.

Prin urmare, prezentul regulament este motivat tehnic de necesitatea menţinerii în funcţiune, în condiţii de securitate, a reţelei spitalului, precum şi de necesitatea dezvoltării normale a unei resurse de informare.

Reţeaua spitalului

Reţeaua de calculatoare din cadrul Spitalului Judeţean de Urgenţă Deva cuprinde totalitatea Sistemelor Informatice şi de Comunicaţie ale spitalului cu sau fără acces la reţeaua internet/intranet.

Orice activitate care se desfăşoară prin intermediul reţelei trebuie să respecte legislaţia în vigoare (internă şi internaţională): Legea nr.64/2004, Legea nr.285/2004, Legea nr.451/2004, Legea nr.496/2004, Legea nr.506/2004, Legea nr.51/2003, Legea nr.161/2003, Legea nr.196/2003, Legea nr.365/2002, Legea nr.455/2001, Legea nr.667/2001, Legea nr.8/1996,HG nr.1308/2002, Convenţia privind Criminalitatea Informatică a Consiliului Europei, Declaraţia privind libertatea comunicării pe Internet a Consiliului Europei etc.), regulamentul de funcţionare şi organizare al spitalului, precum şi prezentul Regulament.

Definiţii şi termeni

- **Internet:** reţeaua internaţională de calculatoare.Reguli ale acestei reţele se regasesc în prevederile inter NIC, RIPE, etc.;
- **Cont:** o entitate specificată printr-un identificator şi/sau o parolă pentru accesul la sistemul de comunicaţie şi/sau la o resursă de calcul;
- **Administrator de reţea:** o persoană calificată şi autorizată, responsabilă pentru gestionarea şi operarea unor resurse de calcul şi/sau de comunicaţie pentru uzul altor persoane;

- **Resurse Informatice şi de Comunicaţii (RIC):** toate dispozitivele de tipărire/imprimare, dispozitive de afişare, unităţi de stocare şi toate activităţile asociate calculatorului care implică utilizarea oricărui dispozitiv capabil să recepţioneze e-mail-uri, să navigheze pe site-uri web, capabil să transmită, stocheze, administreze date electronice, incluzând, dar fără a se limita la: servere, calculatoare personale, laptop-uri, smartphone-uri, sisteme de procesare distribuită, echipament de laborator şi medical conectat la reţea şi controlat prin calculator (tehnologie încapsulată), resurse de telecomunicaţii, medii de reţea, telefoane, faxuri, imprimante şi alte accesorii. La acestea se adaugă procedurile, echipamentele, facilităţile, programele şi datele care sunt proiectate, construite, puse în funcţiune (operaţionale) şi menţinute pentru a crea, colecta, înregistra, procesa, stoca, primi, afişa şi transmite informaţia;
- **Utilizator**: o persoana, o aplicaţie automatizată sau process, utilizator autorizat de către managementul organizaţiei, în conformitate cu procedurile şi regulamentele în vigoare, sa folosească resursel e informatice;
- **Abuz de privilegii**: orice acţiune intreprinsă în mod voit de un utilizator, care vine în contradicţie cu regulamentele şi/sau legislaţia în vigoare, inclusiv cazul în care, din punct de vedere tehnic, nu se poate preveni înfăptuirea de către utilizator a acţiunii respective.

Capitolul 2. POLITICA DE SECURITATE

Politica de securitate este alcătuită astfel încât să fie în conformitate cu statutul, regulamentele, legile şi alte documente oficiale în vigoare privind administrarea resurselor informatice publice, să stabilească practicii prudente şi acceptabile privind utilizarea Sistemelor Informatice şi de Comunicaţii şi să instruiască utilizatorii care au dreptul de folosire a Sistemelor Informatice şi de Comunicaţii privind responsabilităţiile asociate unei astfel de utilizări.

Audienţă

Politica de securitate a Sistemelor Informatice şi de Comunicaţii ale SPJU Deva se aplică nediscriminatoriu tuturor persoanelor cărora li s-a permis accesul la orice SIC a instituţiei. Nu există nici un fel de conotaţii politice, religioase, rasiale legate de prevederile politicii de securitate. Trebuie privită doar ca un instrument de protecţie a datelor din sistemul informatic şi nu ca un element restrictiv.

Scop

Scopul prezentului regulament este acela de a asigura:

- Stabilirea unor reguli concrete şi eficiente pentru utilizarea SIC;
- Asigurarea integrităţii, confidenţialităţii şi disponibilităţii informaţiilor tranzitate prin SIC;
- Protejarea informaţiilor stocate şi transportate folosind SIC;

Domeniu de aplicare

- Regulamentul privind securitatea SIC se aplică tuturor angajaţilor **SPJU DEVA** precum şi colaboratorilor (angajaţi ai altor societăţi) care au acces la SIC în baza unor contracte.

Confidenţialitatea se referă la protecţia datelor împotriva accesului neautorizat. Fişierele electronice create, trimise, primite sau stocate pe sistemele de calcul aflate în proprietatea, administrarea sau în custodia şi sub controlul SPJU Deva, sunt proprietatea SPITALULUI în condiţiile legilor în vigoare. Utilizatorul răspunde personal de confidenţialitatea datelor încredinţate prin procedurile de acces la sistemul RIC.

Integritatea se referă la măsurile şi procedurile utilizate pentru protecţia datelor împotriva modificărilor sau distrugerii neautorizate.

Disponibilitatea se asigură prin funcţionarea continuă a tuturor componentelor sistemului SIC. Diverse aplicaţii au nevoie de nivele diferite de disponibilitate în funcţie de impactul sau daunelor produse ca urmare a nefuncţionării corespunzătoare a sistemului SIC.

Clasificarea informaţiilor

Clasificarea informaţiilor este necesară pentru a permite atât alocarea resurselor necesare protejării acestora , cât şi pentru a determina pierderile potenţiale ca urmare a modificărilor, pierderii/distrugerii sau divulgărilor acestora.

Pentru a asigura securitatea şi integritatea informaţiilor, acestea se impart în trei categorii principale: publice, secrete şi strict secrete.

Publice: Acestea sunt informaţiile accesibile oricărui utilizator din interiorul sau exteriorul spitalului.Divulgarea, utilizarea neautorizată sau distrugerea acestora nu produce efecte asupra instituţiei sau aceste efecte sunt nesemnificative.Utilizatorii care furnizează aceste informaţii sunt responsabili de asigurarea integrităţii şi disponibilităţii acestora în raport cu cerinţele spitalului.

Exemple: informaţiile de pe aviziere, server web publice, ştire de presa, anunţuri publice.

Secrete: În această categorie se includ informaţiile care datorită valorii economice nu trebuie făcute publice. Datorită valorii economice asociate, aceste date trebuie distruse dacă au fost făcute publice.Aceste date vor fi copiate şi distribuite în cadrul spitalului doar utilizatorilor autorizaţii. Distribuirea acestor informaţii de către utilizatorii autorizaţi trebuie să se facă pe baza unei clauze de confidenţialitate.

Exemple: clauze contractuale, conturi şi parole folosite pe serverele sistemului informatic.

Strict Secrete sau Confidenţiale: În această categorie se include toate informaţiile care datorită valorii economice nu trebuie facute publice. Divulgarea, utilizarea sau distrugerea acestor date pot intra sub incidenţa Codului Civil, Penal sau legislaţiei fiscale.Accesul la aceste informaţii va fi restricţionat. Datele strict secrete nu pot fi copiate, distribuite sau şterşe fără acordul strict al conducerii spitalului.

Exemple: cheile criptografice, coduri administrative de pe serverele de gestiune a sistemului informatic.

Atribuţii şi responsabilităţi

Atribuţiile şi obligaţiile administratorului de reţea din spital

Administratorul de reţea/sistem/baze de date trebuie să asigure activarea tuturor mecanismelor de securitate. Adminstratorul de reţea şi sistem al spitalului este informaticianul din cadrul Serviciului de Informatică. Desemnarea Serviciului de Informatică ca administrator are ca scop stabilirea în mod clar a responsabilităţilor privind administrarea şi buna funcţionare a Sistemelor Informatice şi de Comunicaţii din cadrul reţelei spitalului, precum şi a responsabilităţilor privind crearea, modificarea şi aprobarea regulilor şi politicilor referitoare la activităţile de administrare şi utilizarea a Sistemelor Informatice şi de Comunicaţii.

Atribuţiile şi obligaţiile Serviciului de Informatică includ:

- Elaborarea şi propunerea pentru modificările politicii de securitate a sistemului SIC;
- Elaborarea şi propunerea pentru aprobarea planului de securitate (acesta conţine o listă a tuturor regulilor şi a procedurilor de securitate aplicabile la sistemul SIC);
- Elaborarea procedurilor pentru identificare a utilizatorilor SIC;
- Tratarea incidentelor de securitate în scopul minimizării efectului distructiv al acestora asupra SIC;
- Facilitarea evaluărilor legale, a cerinţelor de tip „cele mai bune practici" pe măsură ce acestea devin recunoscute.

Atribuţiile şi obligaţiile ale utilizatorilor reţelei din spital:

- Utilizatorii reţelei din spital pot fi reprezentaţi de: cadre medicale, personal administrativ, alţi angajaţi ai spitalului care solicită calitatea de utilizator;
- Utilizatorii standard nu au drept de administrare a reţelei şi pot folosi numai acele SIC pentru care sunt autorizaţi, indiferent dacă sunt resurse locale sau resurse accesibile în Internet;
- Să cunoască şi să respecte prevederilor politicii de securitate SIC;
- Să cunoască şi să respecte prevederile tuturor regulilor şi procedurilor privind securitatea SIC;
- Să răspundă direct de securitatea şi conţinutul informaţiilor şi resurselor informatice şi de comunicaţii încredinţate direct sau indirect.

Politica de securitate a spitalului impusă de dezvoltarea, gestionarea şi punerea în practică de proceduri şi/sau reguli specifice care să asigure integritatea, confidenţialitatea şi disponibilitatea informaţiei în utilizarea SIC. Toate procedurile şi/sau regulile aplicabile în sistemul Sistemele Informatice şi de Comunicaţii ale spitalului fac parte din Planul de Securitate şi sunt obligatorii pentru toţi utilizatorii.

Se recomandă ca prevederile politicii de securitate să fie incluse în contractul de muncă şi toate contractele cu terţii (dacă activitatea acestora are legătură cu Sistemul Informatic şi de Comunicaţii al spitalului).

Întreg personalul este responsabil privind modul de utilizare a SIC şi nu trebuie să facă abuz de privilegii, fiecare utilizator este direct responsabil pentru acţiunile care pot afecta securitatea Sistemelor Informatice şi de Comunicaţii.

Accesul la reţeaua de comunicaţii

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

Accesul de la distanţă la reţeaua **SPJU DEVA** se va realiza numai prin echipamente aprobate, folosind protocoale aprobate de către Responsabilul IT şi managementul **SPJU DEVA**.

Utilizatorii din interiorul reţelei de comunicaţie a **SPJU DEVA** 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 **SPJU DEVA** care necesită conectare la reţea trebuie să se conformeze cu standardele reţelei interne ale **SPJU DEVA**.

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 **SPJU DEVA** nu au dreptul să ruleze programe de spargere a parolei, sustragere de pachete, scanare a porturilor, în timp ce sunt conectaţi la reţeaua **SPJU DEVA**.

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

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

Departamentele şi Secţiile trebuie să ofere facilităţii corespunzatoare şi de control al accesului în scopul monitorizării SIC, protejării datelor şi programelor împotriva întrebuinţării greşite, în concordanţă cu necesităţile stabilite de acestea.

Serviciul de Informatică îşi rezervă dreptul de a şterge orice produs fără licenţă de pe orice sistem din cadrul Sistemelor Informatice şi de Comunicaţii.

Serviciul de Informatică îşi rezervă dreptul de a şterge de pe orice sistem, orice program sau fişier care nu are legătură cu scopul muncii respective.

Utilizatoriii trebuie să raporteze orice slăbiciune în sistemul de securitate al calculatoarelor din cadul spitalului, orice incident de posibilă întrebuinţare greşită sau încălcare a acestui regulament (prin contactarea Serviciului Informatică).

Capitolul 3. PLANUL DE SECURITATE

Planul de securitate contine toate regulile şi procedurile aplicabile in Sistemele Informatice şi de Comunicaţii a **SPJU Deva**. Acestea sunt elaborate pentru a stabili un cadru corect, legal şi eficient de utilizare a tehnologiei informaţiei si comunicaţiilor în spital.

Planul de securitate are ca scop principal protejarea utilizatorilor şi colaboratorilor împotriva atacurilor de orice tip (cu sau fără intenţie). De asemenea acesta are ca scop protejarea imaginii spitalului şi a investiţiilor acestuia pentru dezvoltarea sistemului informatic şi de comunicaţii, protejarea proprietăţii intelectuale şi a tuturor informaţiilor stocate şi transportate cu ajutorul sistemelor informatice şi de comunicaţii ale utilizatorilor autorizati: cadre medicale, personal administrativ, colaboratori, etc.

Regulile (vezi **anexele** prezentului Regulament) au fost elaborate pentru fiecare activitate specifică domeniului şi au fost concepute în aşa fel încât fiecare să poată fi folosită cvasi-independent de celelalte.

Regulile şi procedurile din planul de securitate au rolul:

- De a fi corecte, echitabile şi eficiente pentru folosirea RIC în vederea sprijinirii procesului educaţional şi al cercetării ştiinţifice ;
- De a educa utilizarii SIC în ceea ce priveşte responsabilităţile asociate cu utilizarea acestora;
- De a fi compatibile cu regulamentele, statului şi atribuţiile stabilite pentru administrarea resurselor informatice şi de comunicaţii.

Regulile de utilizarea a Resurselor Informatice şi de Comunicaţii ale spitalului se aplică nedescriminatoriu tuturor persoanelor cărora li s-a permis accesul la acestea.

Capitolul 4. MĂSURI DISCIPLINARE

Administratorul reţelei spitalului are dreptul să ia măsuri de restricţionare (blocare parţială sau totală), fără notificare a accesului la Resursele Informatice şi de Comunicaţii în cazul utilizatorilor care încalcă prevederilor politicii de securitate şi regulile aplicabile în sisitemul de RIC (din planul de securitate) sau legislaţia în vigoare şi care, astfel, pun în pericol funcţionarea şi/sau securitatea reţelei spitalului.

Toate acţiunile care contravin legilor vor fi raportate organelor competente.

Capitolul 5. DISPOZIŢII FINALE

Regulamentul va fi disponibil în format electronic pe reţeaua internă şi pe site-ul web al spitalului.

Modificarea prevederilor Regulamentului se face numai cu aprobarea conducerii spitalului. Fiecare modificare a conţinutului va conduce la modificarea versiunii documentului şi a informaţiilor de identificare. Versiunea rămâne în vigoare până în momentul în care o nouă versiune intră în vigoare.

Anexa 1 - REGULI DE ACCES ADMINISTRATIV

Amplasarea şi protejarea echipamentelor

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

Pentru protecţia echipamentelor trebuie avute în vedere următoarele:

- echipamentele de prelucrare vor fi amplasate astfel încât să fie minimizat accesul inutil în zona de lucru;
- echipamentele de prelucrare a informaţiilor care utilizează date sensibile trebuie astfel amplasate, iar unghiul de vedere trebuie astfel limitat, încât să se reducă riscul ca informaţiile să poată fi văzute în timpul utilizării de persoane neautorizate, iar mijloacele de stocare trebuie să fie securizate pentru evitarea accesului neautorizat;
- echipamentele care necesită o protecţie specială trebuie izolate pentru a se reduce nivelul general de protecţie necesar;
- trebuie adoptate măsuri de securitate pentru minimizarea riscului potenţialelor ameninţări fizice, cum ar fi: furt, foc, explozivi, fum, apă (sau defectări ale instalaţiilor), praf, vibraţii, substanţe chimice, perturbaţii în alimentarea cu energie sau ale sistemului de comunicaţii, radiaţii electromagnetice şi vandalism;
- trebuie stabilite reguli privind mâncatul, băutul şi fumatul în apropierea sistemelor de prelucrare a informaţiilor;
- trebuie monitorizate condiţiile de mediu care pot afecta negativ funcţionarea sistemelor de prelucrare a informaţiei, cum ar fi temperatura şi umiditatea.

Securizarea birourilor, încăperilor şi a sistemelor informaţionale

În vederea securizării birourilor, încăperilor şi sistemelor:

- trebuie să se ţină seama de reglementările şi standardele de sănătate şi siguranţă din domeniu;
- utilităţile puse la dispoziţia publicului trebuie amplasate în aşa fel încât să se evite accesul publicului în zona birourilor sau a încăperilor unde sunt prelucrate date;
- documentaţia care indică amplasamentul sistemelor de prelucrare a informaţiei sensibile nu trebuie să fie la îndemâna publicului.

Protejarea împotriva ameninţărilor externe şi de mediu

Pentru evitarea pagubelor de pe urma incendiilor, inundaţiilor, cutremurelor, exploziilor, revoltelor publice şi a altor forme de dezastre naturale sau produse de om trebuie avute în vedere următoarele:

- materialele periculoase sau inflamabile trebuie depozitate la o distanţă sigură faţă de zona securizată. Produse uşor inflamabile precum hârtia, nu trebuie depozitate în interiorul zonei de securitate;
- echipamentele de backup trebuie amplasate la o distanţă sigură pentru evitarea pagubelor pe care le-ar putea provoca un dezastru la amplasamentul principal;
- trebuie asigurate şi plasate corespunzător echipamente adecvate de stingere a incendiilor.

Desfăşurarea activităţilor în zone de securitate

Trebuie avute în vedere următoarele:

- zonele securizate neocupate trebuie să fie încuiate şi verificate periodic;
- echipamentele foto, video, audio sau alte echipamente de înregistrare, cum ar fi aparatele de fotografiat din dispozitivele mobile, nu trebuie permise decât dacă sunt autorizate.

ANEXA 2 – CONTROLUL ACCESULUI LOGIC

Controlul accesului la sistemele și aplicațiile IT este esențial pentru a menține integritatea tehnologiei și a datelor SPJU DEVA și pentru a împiedica accesul neautorizat la aceste resurse. Accesul la sistemele SPJU DEVA trebuie să se limiteze doar la utilizatorii sau procesele autorizate, pe baza specificațiilor prevăzute în fișa postului de lucru.

Accesul la sistemele informatice și serviciile de rețea ale SPJU DEVA este controlat printr-un proces oficial de înregistrare a utilizatorilor, începând cu o notificare oficială din partea Responsabilului Resurse Umane către Responsabilul IT. Notificarea va fi trimisă prin e-mail și trebuie să menționeze:

- numele și prenumele utilizatorului;
- funcția noului venit;
- data de începere a activității;
- serviciile necesare conform cerințelor postului;
- drepturile de acces speciale pentru noul utilizator (acestea pot fi cerute și ulterior începerii activității).

Schimbarea funcției sau responsabilităților unui utilizator pot implica o modificare a aplicațiilor și serviciilor utilizate. Solicitarea se va face prin e-mail trimis de către Responsabilului Resurse Umane către Responsabilul IT. Modificările se vor face de către Responsabilul IT cu ajutorul, atunci când este necesar, al Administratorului de sistem/aplicație.

În cazul în care un utilizator și-a uitat parola, Responsabilul IT este autorizat să emită o parolă înlocuitoare. La primirea unei astfel de solicitări, Responsabilul IT va emite o parolă temporară, de unică folosință, și va solicita utilizatorului să o modifice la prima logare.

De îndată ce o persoană și-a încheiat relațiile de muncă cu SPJU DEVA, contul de utilizator al acestuia va fi dezactivat sau suspendat. Ca parte a procesului de terminare a contractului, Responsabilul Resurse Umane va informa organizația despre identitatea persoanei, locul de muncă și data de plecare precum și decizia cu privire la dezactivarea sau suspendarea contului de acces la rețea.

ANEXA 3 – 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 catre spital. 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.

Dispozitivele care nu aparțin SPJU DEVA și care se conectează la rețeaua spitalului trebuie să se conformeze regulamentului de utilizare a echipamentelor personale. 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 sau pentru care nu există licenţă 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.

ANEXA 4 - MANAGEMENTUL PAROLELOR

Toate parolele trebuie să îndeplinească următoarele condiţii:

- Să fie schimbate de utilizator în mod regulat, cel puţin o dată la 60 de zile;
- Să aibă o lungime minimă de 8 caractere;
- Să fie parole complexe care să conţină cifre, litere mari si litere mici şi semne de punctuaţie;
- Reutilizarea parolelor este interzisă;
- Parolele stocate trebuie criptate;
- Parolele de utilizator nu trebuiesc divulgate nimănui, nici măcar angajaţilor care răspund de securitatea sistemelor informatice.

Dacă se suspectează că o parolă a putut fi divulgată aceasta trebuie schimbată imediat. Dispozitivele de calcul nu trebuiesc lăsate nesupravegheate fără a activa un sistem de blocare a accesului la acestea; deblocarea trebuie să se facă folosind parolă.

ANEXA 5 - DETECTAREA VIRUŞILOR

Toate staţiile de lucru de sine stătătoare sau conectate la reţeaua de comunicaţii a SPJU DEVA, trebuie să utilizeze programe antivirus aprobate de către Responsabilul IT. Programele antivirus nu trebuie dezactivate. Orice virus care nu a putut fi înlăturat automat de către programul antivirus constituie un incident de securitate şi trebuie raportat imediat Responsabilului IT.

ANEXA 6 - UTILIZAREA REŢELEI INTERNET ŞI INTRANET

Programele pentru acces la reţeaua internet sunt destinate utilizatorilor autorizaţi pentru a fi folosite în scopul desfaşurării activităţii specificate în fişa postului.

Toate programele utilizate pentru acces la reţeaua 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 dispoziţie de către producător.

Nu este permisă utilizarea sistemului informatic al SPJU DEVA în scop personal sau pentru solicitări personale ce nu au legătură cu organizaţia.

Cumpărăturile pe Internet care nu au legătură cu atribuţiile de serviciu sunt interzise.

Orice material confidenţial al SPJU DEVA transmis prin reţeaua internet trebuie criptat.

ANEXA 7 - MUTAREA ARHIVELOR

Trebuie avute în vedere următoarele:

- echipamentele, informaţiile sau produsele software nu trebuie scoase în afara incintei fără o autorizaţie prealabilă;
- trebuie clar identificaţi angajaţii, contractorii şi utilizatorii terţi care dispun de autoritatea necesară pentru a permite mutarea resurselor în afara incintei;
- trebuie stabilite limite de timp pentru mutarea echipamentelor şi trebuie verificată conformitatea returnărilor;
- când este necesar şi potrivit, echipamentele trebuie înregistrate atunci când sunt mutate în afara incintei şi înregistrate din nou când sunt returnate.

Se pot efectua verificări prin sondaj pentru depistarea mutărilor neautorizate de active, a dispozitivelor neautorizate de înregistrare, a armelor etc. şi împiedicarea pătrunderii acestora în interiorul incintei. Aceste verificări prin sondaj trebuie efectuate în conformitate cu legislaţia şi reglementările în domeniu.

ANEXA 8 – SECURITATEA ECHIPAMENTELOR SCOASE ÎN AFARA LOCAȚIEI

Trebuie luate în considerare următoarele măsuri de securitate pentru protecţia echipamentelor scoase din locaţie:

- echipamentele şi mediile de stocare scoase din locaţie nu vor fi lăsate nesupravegheate în locuri publice. Calculatoarele portabile trebuie transportate ca bagaje de mână şi camuflate, pe cât posibil, în timpul călătoriilor;
- instrucţiunile producătorilor pentru protejarea echipamentelor trebuie respectate în permanenţă, ca de exemplu protejarea împotriva expunerii la câmpuri magnetice puternice;
- măsurile de securitate pentru lucrul la domiciliu trebuie stabilite printr-o determinare a riscului şi trebuie aplicate măsurile de siguranţă adecvate, cum ar fi dulapuri de tip fişier sau care se pot încuia, politica biroului curat, controlul accesului la calculatoare şi comunicare securizată cu sediul central.

Riscurile de securitate, cum ar fi deteriorarea, furtul şi interceptarea, pot varia considerabil în funcţie de locaţie şi trebuie luate în considerare pentru determinarea celor mai potrivite măsuri de securitate.

Scoaterea din uz sau reutilizarea în condiţii de siguranţă

Toate părţile din echipament care conţin medii de stocare trebuie verificate pentru a se asigura că orice date importante sau produse software licenţiate au fost înlăturate sau suprascrise într-un mod sigur înainte de distrugere.

Dispozitivele care conţin informaţii sensibile trebuie distruse fizic sau respectivele informaţii trebuie distruse, şterse sau suprascrise prin tehnici care să facă imposibilă recuperarea informaţiei iniţiale, şi nu prin utilizarea funcţiunilor standard de ştergere sau formatare.

Dispozitivele deteriorate care conţin date sensibile ar putea necesita o determinare a riscului pentru a se stabili dacă trebuie distruse fizic şi nu reparate sau casate.

ANEXA 9 - 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 niciunei 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 un incident de securitate.

De asemenea sunt interzise:

- încercarea utilizatorilor de a vizualiza și deduce parolele altora în timpul introducerii acestora;
- transmiterea de parole în clar prin intermediul sistemelor de comunicații (e-mail, mesagerie instant, SMS, etc.);
- Utilizatorii vor asigura stațiile de lucru împotriva accesului neautorizat, atunci când le lasă nesupravegheate, prin blocarea calculatorului, log off sau cu un screen saver protejat cu parolă, cu funcția de activare automată setată la 5 minute sau mai puțin.
- Utilizatorii vor opri stațiile de lucru la sfârșitul programului de lucru;
- Parolele nu vor fi afișate pe sau sub computer sau în orice altă locație accesibilă;
- În cazul în care informațiile confidențiale sau datele cu caracter personal sunt vizibile pentru o persoană neautorizată aflată în imediata apropiere a ecranului computerului, aceasta va fi rugată să se mute la o distanță suficientă pentru a proteja confidențialitatea acestor informații.

ANEXA 10 - Utilizarea echipamentelor proprietate personală

Angajații care folosesc echipamentelor proprietate personală pentru îndeplinirea sarcinilor de serviciu trebuie să fie autorizați în mod explicit să facă acest lucru. Autorizarea va fi dată de Responsabilul IT la cererea șefului direct ca răspuns la o solicitare în care este explicat motivul solicitării. Pentru autorizare, Responsabilul IT va putea cere informații despre echipamentul proprietate personală care va fi utilizat.

Utilizatorii trebuie să asigure aceleași măsuri de protecție a informațiilor ca și cele aplicate pentru echipamentele SPJU DEVA și nu trebuie să introducă riscuri inacceptabile (cum ar fi malware) în rețeaua organizatiei prin utilizarea de echipamente nesigure.

SPJU DEVA își 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 organizației.

Pentru a preveni accesul neautorizat, în funcție de tipul dispozitivului, utilizatorii trebuie să folosească mijloace de autentificare sigură cum ar fi o combinație nume utilizator-parolă sau un dispozitiv de autentificare.

Echipamentele proprietate personală trebuie să aibă funcția de blocare a ecranului activată, timpul maxim de inactivitate pentru blocarea ecranului să fie de maxim 5 minute iar deblocarea să se facă printr-o metodă relativ sigură cum ar fi parolă sau PIN.

Pe orice echipament proprietate personală trebuie să fie instalat și să ruleze un software antivirus corespunzător. La fiecare conectare a echipamentului proprietate personală la calculatorul de serviciu trebuie să fie scanat conținutul memoriei interne.

Este strict interzis accesul la resursele informatice ale SPJU DEVA cu echipamente proprietate personală modificate sau utilizate într-un mod care nu a fost proiectat sau intenționat de producător, de exemplu dispozitivele „rooted" (Android) sau „jailbroken" (iOS).

Utilizatorii trebuie să realizeze copii de siguranță pentru datele organizației create sau modificate pe echipamente proprietate personală, de preferință prin conectarea la rețeaua organizatiei și sincronizarea datelor între echipamentele proprietate personală și o unitate de rețea sau pe un suport amovibil păstrat în condiții de siguranță.

Orice echipament proprietate personală folosit pentru a accesa, stoca sau procesa informații sensibile trebuie să cripteze datele transferate prin rețea (de exemplu, folosind SSL sau VPN), precum și pe cele stocate pe dispozitiv sau pe medii de stocare separate (de exemplu, folosind VeraCrypt sau mecanismele proprii de criptare ale sistemului de operare), indiferent de tehnologia folosită la stocare (de exemplu, hard disk, disc solid-state, CD/DVD, stick USB/memorie flash, dischetă, etc.).

Datele organizației stocate pe echipamentul proprietate personală vor fi șterse:

- dacă dispozitivul este pierdut și are posibilitatea de a fi șters de la distanță;
- la terminarea contractului de muncă, sau
- în cazul retragerii autorizării din cauza încălcării regulamentului de securitate.

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 echipamentele proprietate personală 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.

ANEXA 11 - Accesul la reţeaua de comunicaţii

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

Accesul de la distanţă la reţeaua Spitalului SPJU DEVA se va realiza numai prin echipamente aprobate, folosind protocoale aprobate de către Responsabilul IT şi managementul Spitalului SPJU DEVA.

Utilizatorii din interiorul reţelei de comunicaţie a Spitalului SPJU DEVA 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 SPJU DEVA care necesită conectare la reţea trebuie să se conformeze cu standardele reţelei interne ale SPJU DEVA.

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 SPJU DEVA nu au dreptul să ruleze programe de spargere a parolei, sustragere de pachete, scanare a porturilor, în timp ce sunt conectaţi la reţeaua SPJU DEVA.

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

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

ANEXA 12 - Sistemul de mesagerie electronică

Următoarele acțiuni sunt strict interzise utilizatorilor:

- utilizarea necorespunzătoare a mijloacelor de comunicare, inclusiv, dar fără a se limita la: sprijinirea activităților ilegale, procurarea și distribuirea de materiale sau mesaje cu caracter ofensator, rasist, obscen, discriminator sau în scop de hărțuire, defăimare sau amenințare;
- procurarea și distribuirea neautorizată de materiale protejate de drepturile de autor (imagini, muzică, filme, mărci și logo-uri ale altor companii preluate din reviste, ziare, cărți sau de pe Internet);
- utilizarea mijloacelor de comunicare pentru publicitate neautorizată, relații de afaceri care nu implică sau sunt contrare intereselor SPJU DEVA, campanii politice, utilizarea în scop distractiv sau orice alte scopuri care nu au legătură cu activitatea organizației;
- 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 regulamentele 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 sau informație trimisă prin intermediul rețelelor publice pot fi identificate și atribuite SPJU DEVA. Din acest motiv, postarea pe forumuri sau alte site-uri de informații care implică numele sau adrese de e-mail ale SPJU DEVA 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 SPJU DEVA*".

ANEXA 13 - Utilizarea resurselor informatice în scop personal

Mijloacele de procesare a informației puse la dispoziție de SPJU Deva sunt destinate în primul rând pentru îndeplinirea 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 regulamentul de securitate ale organizației.

SPJU Deva nu își asumă nicio responsabilitate cu privire la securitatea acestor informații, întreaga responsabilitate (inclusiv realizarea copiilor de siguranță) revenind utilizatorului.

Stocarea și transmiterea de informații

Toate datele trimise prin e-mail (ca atașament sau într-un text de e-mail) ar trebui considerate sensibile și protejate ca atare. Nu trimiteți niciodată documente sau informații de lucru unei persoane din afara SJU Deva decât dacă aceasta a fost autorizată de șeful direct. Aceasta include trimiterea e-mail-urilor organizației către propriul dumneavoastră cont de e-mail personal.

Informațiile prelucrate în cadrul SPJU Deva și trimise prin e-mail cu consimțământul persoanelor vizate, trebuie să fie criptate, iar cheia de criptare trimisă printr-un alt mijloc de comunicație (SMS sau altă adresă de e-mail).

Pentru criptarea informațiilor trimise prin e-mail se va utiliza aplicația 7-zip. Pași de urmat:

- Selectăm fișierul pe care dorim să-l arhivăm > click dreapta > selectăm 7-zip > Adaugă într-o arhivă…;
- Se introduce o parolă în secțiunea Criptare;
- Se modifică Metoda de criptare din ZipCrypto în AES-256;
- Se atașează e-mail-ului fișierul arhivat.

Nu toți utilizatorii SPJU Deva au acces la aceleași informații. Înainte de a trimite date sau fișiere unui coleg într-un e-mail, contactați șeful direct pentru a vă asigura că destinatarului i se permite să aibă acces la acesta.

ANEXA 14 - Stocarea în cloud și servicii de tip cloud

Uneori este posibil ca angajații să aibă nevoie de acces la muncă din afara biroului, de la domiciliu, folosind dispozitive sau echipamentele mobile puse la dispoziție de organizație sau echipamente proprietate personală. Cu toate acestea, informațiile despre locul de muncă nu ar trebui să fie stocate sau partajate în conturi sau aplicații cloud personale (exemplu: iCloud, Google Drive, Dropbox, Microsoft OneDrive șamd).

De asemenea, este posibil ca angajații să trebuiască să folosească servicii de mesagerie sau de e-mail bazate pe cloud (exemplu: Whatsapp, Hangouts, Gmail, ș.a.m.d.).

Utilizarea serviciilor de cloud în scopuri de serviciu trebuie să fie autorizată în mod oficial de către șeful direct și responsabilul IT.

Dispozitive de stocare fizică

Stocarea datelor de lucru pe dispozitive fizice, incluzând, dar fără a se limita la acestea, unitățile USB, cardurile de memorie, CD-urile sau hard-urile externe trebuie să fie pre-aprobate de Responsabilul IT. Angajații SPJU Deva trebuie să utilizeze numai dispozitivele furnizate de organizație, cu excepția cazului în care există o permisiune diferită.

Nu utilizați niciodată și nu conectați la computer fără o verificare anterioară, o unitate USB pe care ați găsit-o, ați primit-o cadou sau a fost dată ca element promoțional. Aceste dispozitive pot conține programe malware sau viruși ascunși.

În cazul pierderii sau furtului unui dispozitiv, se va anunța șeful direct imediat, pentru a preveni scurgerea datelor.

Social media

Datele de lucru sau informațiile nu trebuie să fie distribuite niciodată prin intermediul conturilor de social media cum ar fi Facebook, LinkedIn, Google Plus etc.

Criptarea

În timp ce criptarea datelor nu poate împiedica o pierdere a datelor, aceasta poate contribui la asigurarea că, dacă informațiile intră în mâinile greșite, acestea nu pot fi citite sau utilizate. Dacă informațiile trebuie să fie criptate, acestea trebuie să fie protejate de o parolă puternică și nu ar trebui niciodată copiate sau partajate într-un mod care să le facă disponibile procesului de decriptare.

Obligațiile angajaților

Ca parte a obligațiilor contractuale, angajații trebuie să semneze un acord de confidențialitate sau de păstrare a secretului, înainte de a li se acorda acces la sistemele de procesare a informațiilor. Dacă angajatul, subcontractantul sau utilizatorul terț achiziționează echipamentul SPJU Deva sau folosește propriul echipament, trebuie urmate proceduri care să asigure transferarea către SPJU Deva a tuturor informațiilor relevante și ștergerea lor din memoria echipamentelor.

La încetarea activităţii, drepturile de acces ale unei persoane la resursele asociate sistemelor de informaţii şi serviciilor trebuie reanalizate. Acest lucru va stabili dacă este necesară retragerea drepturilor de acces. Modificarea relaţiilor de muncă trebuie să se reflecte în retragerea tuturor drepturilor de acces care nu au fost aprobate în mod specific pentru noul angajament. Drepturile de acces care trebuie retrase sau adaptate includ accesul fizic şi logic, cheile, cardurile de identificare, sistemele de procesare a informaţiei, abonamentele şi eliminarea de pe orice documentaţie care îi identifică pe aceştia ca membri curenţi ai SPJU Deva.

Dacă angajatul care pleacă din SPJU Deva cunoaşte parole pentru conturi rămase active, acestea trebuie schimbate la încetarea sau modificarea relaţiilor de muncă, contractului sau acordului.

ANEXA 15 - Raportarea incidentelor de securitate și de protecția datelor

Toți angajații SPJU Deva trebuie să cunoască procedurile de raportare a diverselor tipuri de evenimente legate de incidente care pot avea impact asupra securității resurselor SPJU Deva sau de încălcare a securității datelor cu caracter personal, și, în cazul identificării unui eveniment, să 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 anunțarea autorității naționale de supraveghere sau a persoanelor vizate, în cazul în care este necesar.

***Incident privind securitatea informației**: un eveniment sau o serie de evenimente de securitate a informației care au o probabilitate semnificativă de a compromite activitățile SPJU Deva și de a aduce amenințări la securitatea informației.*

Conform Regulamentului UE 679/2016–GDPR, un eveniment de încălcare a securității datelor cu caracter personal este un eveniment care poate conduce la prejudicii fizice, materiale sau morale aduse persoanelor fizice, cum ar fi pierderea controlului asupra datelor cu caracter personal sau limitarea drepturilor lor, discriminare, furt sau fraudă de identitate, pierdere financiară, inversarea neautorizată a pseudonimizării, compromiterea reputației, pierderea confidențialității datelor cu caracter personal protejate prin secret profesional sau orice alt dezavantaj semnificativ de natură economică sau socială adus persoanei fizice în cauză.

Impactul nerespectării regulamentului

Toți angajații SPJU Deva sunt obligați să respecte aceast regulamant de securitate. Orice membru al personalului care a încălcat termenii acestui regulament poate face obiectul unor măsuri disciplinare.

ANEXA 16 - Raportarea și transmiterea de informații

Toate datele trimise online sau prin e-mail (ca atașament sau într-un text de e-mail) ar trebui considerate sensibile și protejate ca atare. Nu trimiteți niciodată documente sau informații de lucru unei persoane din afara SPJU DEVA decât dacă este angajatul instituțiilor cu care colaborați direct.

Informațiile prelucrate în SPJU DEVA și trimise online sau prin e-mail cu consimțământul persoanelor vizate, trebuie să fie criptate, iar cheia de criptare trimisă printr-un alt mijloc de comunicație (SMS sau altă adresă de e-mail). Datele transmise online se face folosind semnătura electronică agreată de ambele părți.

Criptarea datelor nu poate împiedica o pierdere a datelor, aceasta poate contribui la asigurarea că, dacă informațiile intră în mâinile greșite, acestea nu pot fi citite sau utilizate. Informațiile criptate trebuie să fie protejate de o parolă puternică și nu ar trebui niciodată copiate sau partajate într-un mod care să le facă disponibile procesului de decriptare.