Anexa nr.3 la Proiectul de hotărâre nr.13/2021

Regulamentul de Securitate privind Sistemul Resurselor Informatice şi de Comunicaţii privind Protecția Datelor cu Caracter Personal din cadrul Primărie comunei Capleni, județul Satu Mare

Cuprins

Capitolul I

Introducere

În acord cu prevederile din prezentul document, Resursele Informatice şi de Comunicaţii sunt bunuri strategice ale Primărie comunei Capleni, județul Satu Mare care trebuiesc administrate ca resurse ale Primărie comunei Capleni, județul Satu Mare numită în continuare Operator.

Compromiterea securităţii sistemului RSRITC poate afecta capacitatea Operatorului de a oferi serviciile specifice, poate conduce la fraude sau distrugerea datelor, violarea clauzelor contractuale, divulgarea secretelor, afectarea credibilităţii Operatorului în faţa partenerilor săi.

RSRITC este stabilit astfel încât:

- ✓ Să fie în conformitate cu statutul, regulamentele, legile şi alte documente oficiale în vigoare privind administrarea resurselor informatice;
- ✓ Să stabilească practici prudente şi acceptabile privind utilizarea RSRITC ale Operatorului;
- ✓ Să instruiască utilizatorii care au dreptul de folosire a sistemului RSRITC privind responsabilităţile asociate unei astfel de utilizări;

Regulamentul de securitate a sistemului Operatorului se aplică nediscriminatoriu tuturor persoanelor cărora li s-a permis accesul la orice resursă informatică şi de comunicaţii al Operatorului.

Următorii utilizatori sunt vizaţi în mod distinct de prevederile RSRITC:

- ✓ Angajaţii cu contract de muncă pe perioadă determinată sau nedeterminată care au acces la sistemul informaţional şi de comunicaţii;
- ✓ Colaboratorii Operator care au acces la sistemul RSRITC;

Scopul politicii de securitate

Politica de securitate a sistemului RSRITC are ca scop asigurarea integrităţii, confidenţialităţii şi disponibilităţii informaţiei.

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 Operatorului, sunt proprietatea instituţiei în condiţiile legilor în vigoare. Utilizatorul răspunde personal de confidenţialitatea datelor încredinţate prin procedurile de acces la sistemul RSRITC.

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 RSRITC. Diverse aplicaţii au nevoie de nivele diferite de disponibilitate în funcţie de impactul sau daunele produse ca urmare a nefuncţionării corespunzătoare a sistemului RSRITC.

Politica de securitate are ca scop, de asemenea, stabilirea cadrului necesar pentru elaborarea regulamentelor şi procedurilor de securitate. Acestea sunt obligatorii pentru toţi utilizatorii sistemului RSRITC.

Definiţii folosite în politica de securitate şi regulamentul de utilizare

Resurse Informatice şi de Comunicaţii : toate dispozitivele de tipărire/imprimare, dispozitive de afişare, unităţi de stocare, şi toate activităţile asociate calculatorului care implică utilizarea oricărui dispozitiv capabil să recepţioneze email, să navigheze pe site-uri de Web, cu alte cuvinte, capabil să transmită, stocheze, administreze date electronice, incluzând, dar nu limitat la: mainframe-uri, servere, calculatoare personale, calculatoare-agendă (notebook-uri), calculatoare de buzunar, asistent digital personal (Personal Digital Assistant - PDA), pagere, 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, echipamentul, facilităţile, programele şi datele care sunt proiectate, construite, puse în funcţiune (operaţionale) şi menţinute pentru a creea, colecta, înregistra, procesa, stoca, primi, afişa şi transmite informaţia.

Administratorul Resurselor Informatice şi de Comunicaţii (ARIC): Desemnarea ARSRITC are ca scop stabilirea în mod clar a responsabilităţii privind crearea, modificarea şi aprobarea regulamentelor privind activităţile de finanţare, administrare şi utilizare a RIC. Titlul este atribuit în mod automat şefului de departament IT, iar acolo unde nu există, se aplică ordonatorului de credit.

Ofiţer responsabil cu Securitatea IT (OSRIC): Răspunde direct doar în faţa ARSRITC privind administrarea funcţiilor de securitate al informaţiei în cadrul Operatorului. Este persoana de contact pentru orice problemă în legătură cu securitatea IT (specialistul IT din cadrul instituţiei).

Responsabilul cu protecţia datelor personale (RPD): Persoana responsabilă de monitorizarea şi implementarea controalelor de securitate, precum şi a procedurilor pentru sistemul RSRITC la nivelul Operatorului. Este persoana de contact al Operatorului pentru orice problemă în legătură cu protecţia datelor personale.

ANSPDCP: Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal, în calitate de autoritate publică centrală autonomă cu competență generală la prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date.

Utilizator: O persoană, o aplicaţie automatizată sau proces utilizator autorizat de către Operator, în conformitate cu procedurile şi regulamentele în vigoare, să folosească RSRITC.

Abuz de privilegii: Orice acţiune întreprinsă în mod voit de un utilizator, care vine în contradicţie cu regulamentele Operatorului şi/sau legile în vigoare, inclusiv cazul în care, din punct de vedere tehnic, nu se poate preveni înfăptuirea de către utilizator a acţiunii respective.

Furnizor: Persoană fizică/juridică care oferă bunuri şi/sau servicii Operatorului în baza unui contract comercial sau de colaborare.

Internet: Sistem global care interconectează calculatoare şi reţele de calculatoare. Acestea sunt deţinute de mai multe organizaţii, agenţii guvernamentale, societăţi, instituţii academice.

Intranet: Reţea privată destinată comunicaţiilor şi partajării informaţiilor, care, ca şi reţeaua Internet, foloseşte suita de protocoale TCP/IP, însă este accesibilă doar utilizatorilor autorizaţi din cadrul unei organizaţii (instituţii). În mod obişnuit, reţeaua Intranet a unei organizaţii este protejată printr-un sistem de protecţie (firewall).

Echipa de Răspuns la Incidentele de Securitate a RSRITC(ERIS): persoanele responsabile de acţiunile desfăşurate în scopul micşorării sau eliminării impactului negativ al unui incident de securitate. ERIS este formata din ARIC, OSRIC, RPD.

Virus: Un program care se auto-ataşează la un fişier executabil sau la o aplicaţie vulnerabilă şi care generează efecte de la cele deranjante până la cele distructive. Un virus se execută în momentul în care este accesat un fişier infectat. Un virus de macro infectează codul executabil încapsulat în pachetul de programe Microsoft Office (Word, Excel, PowerPoint) sau alte programe care permit utilizatorului să genereze macro-uri.

Vierme: Un program care se auto-copiază în oricare altă parte a unui sistem informatic. Aceste copii pot fi create pe acelaşi calculator sau pot fi trimise către alte calculatoare prin intermediul reţelei. Prima utilizare a termenului descria un program care s-a multiplicat într-o reţea de calculatoare, folosind resursele sau calculatoarele neutilizate din reţea pentru a distribui aceste copii. Unii dintre aceşti viermi reprezintă o ameninţare la adresa securităţii datorită faptului că folosesc reţeaua pentru a se împrăştia, împotriva voinţei proprietarilor de sisteme de calcul, cauzând astfel nefuncţionarea sau funcţionarea defectuoasă a reţelei. Un vierme este asemănător unui virus prin faptul că se auto-copiază, diferenţa constând în faptul că un vierme nu are nevoie să se ataşeze la anumite fişiere pentru a se multiplica.

Cal troian: de obicei un virus sau un vierme – care este ascuns sub forma unui program atractiv sau inofensiv, cum ar fi un joc, sau program de grafică (o felicitare în format electronic, un program tip screen-saver). Victimele pot primi un astfel de cal troian prin email sau pe o dischetă, adeseori de la o altă victimă necunoscută sau pot fi încurajate să descarce un fişier de pe o pagină Web sau un forum.

Incident de Securitate: În termeni informatici este definit ca un eveniment prin care se încearcă sau se realizează accesul la un sistem informatic, un atac asupra integrităţii şi/sau confidenţialităţii informaţiei de pe un sistem informatic automatizat. Aceasta include examinarea sau navigarea neautorizată, întreruperea sau anularea unui serviciu, date alterate sau distruse, prelucrarea (procesarea), stocarea sau extragerea informaţiilor, modificarea informaţiilor sistemului referitoare la caracteristicile componentelor hardware, firmware sau software cu sau fără ştiinţa sau intenţia utilizatorului.

Reţea locală (LAN): O reţea de comunicaţii de date ce este distribuită pe o zonă restrânsă (de regulă la nivelul unui grup de lucru). Reţeaua locală oferă comunicaţii între calculatoare şi periferice la o viteză de transfer mare şi cu puţine erori.

Server: Un program de calculator care oferă servicii altor programe aflate pe acelaşi calculator sau pe calculatoare diferite. Un calculator care rulează un program tip server este denumit în mod frecvent server, cu toate că pe acelaşi calculator mai pot rula şi alte programe de tip client sau server.

Gazdă (Host): Un sistem care oferă servicii pentru un anumit număr de utilizatori.

Copii de Siguranţă (backup): Copii ale fişierelor şi aplicaţiilor făcute pentru a evita pierderea datelor şi pentru a permite recuperarea în cazul unor evenimente care pot conduce la pierderi de date.

Firewall: Un mecanism de control al accesului care acţionează ca o barieră între două sau mai multe segmente ale unei reţele de calculatoare sau ale unei arhitecturi de tip client/server, folosit pentru a proteja reţelele interne sau segmente ale acestora împotriva utilizatorilor sau proceselor neautorizate.

Atac informaţional: O încercare de a trece peste măsurile şi controalele de securitate fizice sau informatice care protejează un sistem din cadrul sistemului de

RSRITC. Atacatorul poate altera informaţiile, poate acorda sau refuza accesul la ele. Succesul unui eventual atac depinde de gradul de vulnerabilitate al sistemului în particular şi de eficacitatea contramăsurilor aplicate.

Protecţie informaţională: Acţiuni întreprinse în vederea afectării informaţiilor şi sistemelor informatice ostile, în timp ce protejează informaţiile şi sistemele informatice proprii.

Procedura - reprezintă modalitatea specifică de desfăşurare a unei activităţi sau a unui proces.

Confidenţialitate

Fişierele electronice create, trimise, primite sau stocate folosind sistemul RSRITC propriu, administrate sau în custodia şi sub controlul Operatorului nu au caracter personal şi pot fi accesate oricând de către angajaţii autorizaţi (specialistul IT/administrator reţea) fără înştiinţarea utilizatorului.

În scopul administrării RSRITC şi pentru asigurarea securităţii RSRITC personalul autorizat poate revizui sau utiliza orice informaţie stocată pe sau transportată prin sistemele RSRITC în conformitate cu legile în vigoare. În aceleaşi scopuri, este posibilă monitorizarea activităţii utilizatorilor.

Utilizatorii trebuie să raporteze orice slăbiciune în sistemul de securitate al calculatoarelor din cadrul Operator, orice incident de posibilă întrebuinţare greşită sau încălcare a acestui regulament (prin contactarea OSRSRITC- RPD).

Un mare număr de utilizatori, pot accesa diverse informaţii din sistemul de comunicaţii al Operatorului. În aceste condiţii este obligatorie păstrarea confidenţialităţii acestor informaţiilor transmise din exteriorul RSRITC şi a informaţiilor obţinute din interior.

Utilizatorii nu trebuie să încerce să acceseze informaţii sau programe de pe sistemele Operatorului pentru care nu au autorizaţie sau consimţământ explicit.

Nici un utilizator al sistemului RSRITC ale Operatorului nu poate divulga informaţiile la care are acces sau la care a avut acces ca urmare a unei vulnerabilităţi a sistemului RSRITC. Această regulă se extinde şi după ce utilizatorul a încheiat relaţiile cu Operatorul, conform angajamentelor personale sau contractelor de munca semnate, existente in cadrul Serviciului Resurse Umane.

Confidenţialitatea informaţiilor transmise prin intermediul resurselor de comunicaţii ale terţilor nu poate fi asigurată. Pentru aceste situaţii, confidenţialitatea şi integritatea informaţiilor se poate asigura folosind tehnici de criptare. Utilizatorii sunt obligaţi să se asigure că toate informaţiile confidenţiale ale Operatorului se transmit în aşa fel încât să se asigure confidenţialitatea şi integritatea acestora.

CAPITOLUL II

Introducere

Regulamentele de Utilizare a Resurselor Informatice şi de Comunicaţii sunt elaborate pentru a stabili un cadru corect, legal şi eficient de utilizare a tehnologiei informaţiei şi comunicaţiilor pentru Operator. Acestea au ca scop principal protejarea utilizatorilor, colaboratorilor împotriva atacurilor de orice tip (cu sau fără intenţie). De asemenea acestea au ca scop protejarea imaginii instituţiei şi a investiţiilor acesteia pentru dezvoltarea sistemul informatic şi de comunicaţii.

În acord cu legislaţia în vigoare în România, Resursele Informatice şi de Comunicaţii sunt valori ale Operatorului care trebuie exploatate şi administrate ca resurse private în proprietatea Operatorului.

Scopul acestor regulamente este acela de a asigura:

- ✓ Stabilirea unor reguli corecte, echitabile şi eficiente pentru folosirea resurselor informatice şi de comunicaţii în vederea sprijinirii procesului educaţional şi a cercetării ştiinţifice;
- ✓ Protejarea imaginii Operatorului;
- ✓ Protejarea investiţiilor Operatorului pentru dezvoltarea sistemului informatic şi de comunicaţii propriu;
- ✓ Protejarea proprietăţii intelectuale şi a tuturor informaţiilor stocate şi transportate folosind Resursele Informatice şi de Comunicaţii ale utilizatorilor autorizaţi: membrii conducerii, personalul propriu, colaboratori etc.
- ✓ Educarea utilizatorilor resurselor informatice şi de comunicaţii în ceea ce priveşte responsabilităţile asociate cu utilizarea acestora;
- ✓ Compatibilitate cu regulamentele, statutul şi atribuţiile stabilite pentru administrarea resurselor informatice şi de comunicaţii.

Regulamentele de utilizare a resurselor informatice şi de comunicaţii ale Operatorului se aplică nediscriminatoriu tuturor persoanelor cărora li s-a permis accesul la acesta.

Regulamentele şi procedurile de lucru sunt elaborate de Compartimentul Informatică din cadrul instituţiei şi supuse spre aprobare conducerii.

Prevederile Politicii de Securitate şi Procedurile de Lucru aprobate vor fi aplicate tuturor entităţilor şi utilizatorilor după cum urmează:

- ✓ Angajaţii cu contract de muncă pe perioadă determinată sau nedeterminată care au acces la sistemul informaţional şi de comunicaţii;
- ✓ Colaboratorii Operatorului care au acces la sistemul RSRITC;

Modificarea regulamentului şi/sau a procedurilor generale de lucru se va face ori de câte ori este nevoie, iar aprobarea modificărilor se va face de către conducere la propunerea OSRIC.

Regulament de utilizare a RSRITC

Utilizarea sistemului RSRITC se face numai în interes de serviciu.

Utilizatorii trebuie să anunţe OSRIC- RPD în cazul în care se observă orice problemă/breşă în sistemul de securitate a RSRITC al Operatorului cât şi orice posibilă întrebuinţare greşită sau încălcare a regulamentelor în vigoare.

Utilizatorii, prin acţiunile lor, nu trebuie să încerce să compromită protecţia sistemelor informatice şi de comunicaţii şi nu trebuie să desfăşoare, deliberat sau accidental, acţiuni care pot afecta confidenţialitatea, integritatea şi disponibilitatea informaţiilor de orice tip în cadrul sistemului Operatorului.

Utilizatorii nu trebuie să încerce să obţină acces la date sau programe din RSRITC pentru care nu au autorizaţie sau consimţământ explicit.

Utilizatorii nu trebuie să divulge nimănui numerele de acces Dialup sau Dialback prin modem.

Utilizatorii nu trebuie să divulge sau să înstrăineze nume de cont-uri, parole, Numere de Identificare Personală (PIN-uri), dispozitive pentru autentificare (ex.: Smartcard) sau orice dispozitive şi/sau informaţii similare utilizate în scopuri de autorizare şi identificare.

Utilizatorii nu trebuie să facă copii neautorizate sau să distribuie materiale protejate prin legile privind proprietatea intelectuală (copyright).

Utilizatorii nu trebuie să utilizeze programe de tip shareware sau freeware, fără aprobarea OSRIC, cu excepţia cazului în care acestea se găsesc pe lista programelor standard folosite de către Operator. Această listă va fi întocmită de către OSRSRITC împreună cu RPD în funcţie de necesităţile departamentelor.

Utilizatorii nu trebuie să se angajeze într-o activitate care ar putea hărţui sau ameninţa alte persoane.

Utilizatorii nu trebuie să degradeze performanţele RSRITC.

Utilizatorii nu trebuie să împiedice accesul unui utilizator autorizat la RSRITC.

Utilizatorii nu trebuie să obţină alte resurse în afara celor alocate.

Utilizatorii nu trebuie să ignore măsurile de securitate impuse prin regulamente.

Utilizatorii nu trebuie să exploateze defectuos componentele RSRITC.

Utilizatorii nu trebuie să utilizeze dischete, cd-uri, sau orice alt suport magnetic de stocare a informaţiei din exteriorul instituţiei fără acordul explicit al OSIRC - RPD;

Utilizatorii nu trebuie să descarce, instaleze şi să ruleze programe de securitate sau utilitare care expun sau exploatează vulnerabilităţi ale securităţii RSRITC, care au capacitatea de a decripta parole sau informații stocate în mod criptat, care pot captura traficul în rețeaua internă sau care pot scana structura rețele interne sau orice alt program nepermis în mod explicit prin regulamente.

RSRITC ale Operatorului nu trebuiesc folosite pentru beneficiul personal.

Utilizatorii nu trebuie să acceseze, să creeze, să stocheze sau să transmită materiale pe care Operatorul le poate considera ofensive, indecente sau obscene.

Accesul la reţeaua Internet prin intermediul RSRITC se supune aceloraşi regulamente care se aplică utilizării din interiorul instituţiei şi Regulamentului pentru Utilizare Internet şi Intranet (cap.II subcap.14).

Angajaţii nu trebuie să permită membrilor familiei sau altor persoane străine neautorizate, care nu au aprobare explicită din partea ARIC, OSRIC, RPD sau a conducerii instituţiei accesul la RSRITC ale Operatorului. Utilizatorii care au acces la sistemul RSRITC al Operatorului au obligaţia de a purta acte şi/sau legitimaţii/ecusoane care să ateste calitatea de utilizator autorizat în spaţiile Operatorului. Utilizatorii nu trebuie să se angajeze în acţiuni împotriva scopurilor Operatorului folosind RSRITC.

În cazul demisiei/plecării definitive din companie a unui utilizator acest lucru va fi comunicat OSRIC- RPD de către Serviciul Resurse Umane din Cadrul instituţiei. OSRSRITC va recurge la stergerea conturilor şi parolelor utilizatorului respectiv, iar accesul utilizatorului la RSRITC va fi interzis.

Este interzisă utilizarea RSRITC de către persoane neautorizate.

Utilizarea ocazională a RSRITC în scopuri personale

În aceste situaţii se aplică următoarele restricţii:

✓ Utilizarea personală ocazională a serviciilor de poştă electronică, acces internet, telefoane, fax-uri, imprimante, copiatoare, etc. este restricţionată la utilizatorii autorizaţi şi nu poate fi extinsă la membrii familiilor sau alte persoane.

✓ Utilizarea ocazională a RSRITC nu trebuie să aibă drept rezultate costuri directe pentru Operator. Utilizarea ocazională a RSRITC nu trebuie să afecteze activitatea normală a angajaţilor.

✓ Nu este permisă trimiterea sau recepţionarea documentelor sau fişierelor care pot cauza acţiuni legale împotriva Operatorului sau prejudicierea, indiferent de formă, a intereselor acestuia.

✓ Stocarea mesajelor de email, a mesajelor de voce, a documentelor şi fişierelor personale din cadrul RSRITC trebuie să fie nominală.

✓ Toate mesajele, fişierele şi documentele – incluzând mesajele personale, fişierele şi documentele – localizate în cadrul RSRITC sunt proprietatea Companiei şi pot fi subiectul unor cereri de verificare/inspectare/accesare de către ARIC, OSRIC, RPD conform regulamentelor.

Accesul Administrativ

✓ Utilizatorii trebuie să cunoască şi să accepte toate regulamentele privind securitatea RSRITC înainte de a li se permite accesul la un cont.

✓ Utilizatorii care au conturi de acces administrativ trebuie sa aibă instrucţiuni de administrare, documentare, instruire şi autorizare a conturilor. Aceste instrucţiuni se vor elabora de către fiecare Departament şi vor fi incluse în fişa postului.

✓ Utilizatorii cu drepturi administrative sau speciale de acces nu trebuie să folosească în mod abuziv aceste drepturi şi trebuie să facă investigaţii numai sub îndrumarea OSRSRITC sau RPD.

✓ Cei care utilizează conturi de acces cu drepturi administrative sau speciale trebuie să folosească tipul de privilegiu cel mai potrivit activităţii pe care o desfăşoară.

✓ Accesul administrativ trebuie să se conformeze Regulamentului privind Parolelor.

✓ Parola pentru un cont cu acces privilegiat nu va fi utilizată de mai multe persoane decât cu acordul scris al OSRIC-RPD şi trebuie să fie schimbată atunci când o persoana care utilizează acest cont îşi schimbă locul de muncă din cadrul Departamentului sau a Instituţiei, sau în cazul unei modificări a listei de personal ale terţilor (furnizor desemnat) în contractele cu Operatorul.

✓ Trebuie să existe o procedură prin care o altă persoană, în afară de administrator, să poată avea acces la contul administratorului în caz de forţa majoră. Această procedură va fi elaborată de către OSRSRITC şi comunicată ARSRITC-RPD.

✓ 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.

Accesul Fizic

✓ Accesul fizic la toate încăperile în care sunt instalate RSRITC trebuie să fie documentat şi monitorizat.

✓ Toate încăperile în care sunt instalate RSRITC trebuie să fie protejate fizic, în funcţie de importanţa acestora şi tipul datelor vehiculate sau stocate.

✓ Pentru fiecare încăpere în care sunt instalate echipamente ale sistemului RSRITC se aprobă accesul doar pentru personalul care răspunde de buna funcţionare a echipamentelor din încăperea respectivă şi, dacă este cazul, părţilor contractante, ale căror obligaţii contractuale implică acces fizic.

✓ Personalul care are drepturi de acces trebuie să deţină legitimaţie de serviciu şi acte de identitate care să-i ateste calitatea.

✓ Nu este permis transferul dreptului de acces indiferent de motiv.

✓ Accesul publicului, vizitatorilor, sau a persoanelor străine în cadrul instituţiei se va face doar pe baza actului de identitate. Vizitatorii/persoanele străine trebuie să fie însoţiţi în zonele cu acces restricţionat.

✓ Pentru fiecare spaţiu în care sunt instalate RSRITC se va păstra o evidenţă a accesului pentru verificări de rutină în situaţii critice.

Conectarea la Sistemul Resurselor Informatice şi de Comunicaţii

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

✓ 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 OSRIC.

✓ Conectarea sistemelor de calcul care nu sunt proprietatea Operatorului se face numai cu aprobarea în scris din partea conducerii instituţiei pentru rețeaua de producție sau oricând consideră de cuvință utilizatorul în cazul rețelei pentru vizitatori.

✓ Accesul de la distanţă la reţeaua Operatorului se va realiza numai prin echipamente aprobate, sau prin intermediul unui Furnizor de Servicii Internet (Internet Service Provider (ISP)) agreat de către Operator şi folosind protocoale aprobate de către OSRIC.

✓ Utilizatorii RSRITC din interiorul rețelei Operatorului 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. Autorizarea tuturor conexiunilor se face la propunerea Departamentelor de către Compartimentul de Informatică.

✓ Utilizatorii nu trebuie să instaleze echipamente hardware sau programe care furnizează servicii de reţea fără aprobarea Compartimentului de Informatică.

✓ Sistemele computerizate din afara Instituţiei care necesită conectare la reţea trebuie să se conformeze cu standardele reţelei interne a Operatorului.

✓ Utilizatorii nu au dreptul să descarce din Internet, să instaleze sau să ruleze programe de securitate sau de altă natură care pot dezvălui slăbiciuni în securitatea unui sistem.

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

✓ Serviciul de nume şi administrarea adreselor IP sunt deservite exclusiv de către Compartimentul de Informatică.

✓ Serviciile de interconectare a reţelei Operatorului cu alte reţele sunt realizate exclusiv de către Compartimentul de Informatică.

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

Configurarea Parametrilor de Acces la Reţea

✓ Infrastructura de comunicaţii, reţeaua de comunicaţii digitale, a Operatorului este administrată de către Compartimentul de Informatică care este responsabil cu întreţinerea şi dezvoltarea acesteia.

✓ Pentru a furniza o infrastructură de comunicaţii unitară cu posibilităţi de modernizare toate componentele acesteia sunt instalate de către Compartimentul de Informatică sau de către un furnizor avizat explicit de către Compartimentul de Informatică

✓ Toate echipamentele, fără excepţie, conectate la reţeaua de comunicaţii trebuie configurate conform specificaţiilor Compartimentul de Informatică

✓ Orice dispozitiv hardware, inclusiv plăcile de reţea şi modemuri, care se va conecta la reţeaua Operatorului, trebuie să fie însoţit de o aprobare de tip (producător, model etc.) din partea Compartimentul de Informatică.

✓ Modificarea configuraţiei oricărui dispozitiv activ conectat la reţeaua de comunicaţii se face numai de către Compartimentul de Informatică.

✓ Toate conectările în reţeaua de comunicaţii a Operator sunt responsabilitatea Compartimentul de Informatică, conectarea se va face numai în baza unei cereri standard aprobată de către conducerea Companiei.

✓ Toate conectările dintre reţeaua de comunicaţii a Operatorului şi alte reţele de comunicaţii, publice sau private, sunt responsabilitatea exclusivă a Compartimentul de Informatică

✓ Echipamentele de protecţie a reţelei de comunicaţie ale Operator (firewall) se vor instala de către Compartimentul de Informatică.

✓ Utilizatorii nu au dreptul să extindă sau să retransmită în nici un fel serviciile reţelei (este interzisă instalarea unui telefon, fax, modem, router, switch, hub sau punct de acces la reţeaua Instituţiei) fără aprobare din partea Compartimentul de Informatică. Utilizatorilor li se interzice instalarea de dispozitive hardware de reţea sau programe care furnizează servicii de reţea fără aprobarea Compartimentul de Informatică.

- ✓ Utilizatorilor nu le este permis accesul la dispozitivele hardware ale reţelei.

Tratarea Incidentelor de Securitate şi de nerespectare a Politicii şi Regulamentului de Securitate

Membrii Echipei de Răspuns la Incidentele de Securitate (Membrii ERIS) ai Operatorului, au funcţii şi responsabilităţi pre-definite care pot fi prioritare îndatoririlor obişnuite.

Ori de câte ori un incident de securitate este suspectat sau confirmat, precum un virus, vierme, descoperirea unor activităţi suspecte, informaţii modificate etc., trebuie urmate procedurile standard specifice pentru micşorarea riscurilor.

OSRSRITC este responsabil cu înştiinţarea şi coordonarea echipei ERIS pentru tratarea incidentului.

OSRSRITC este responsabil cu strângerea dovezilor fizice şi electronice ce vor face parte din documentaţia pentru tratarea incidentului.

Folosind resurse tehnice speciale se va monitoriza nivelul daunelor şi gradul de eliminare sau atenuare a vulnerabilităţilor acolo unde este cazul.

OSRIC, în colaborare cu RPD va stabili conţinutul comunicatelor pentru utilizatori privind incidentele şi va determina nivelul şi modul de distribuire a acestei informaţii.

OSRSRITC şi RPD trebuie să comunice proprietarului sau producătorului resursei afectate de un incident informaţiile utile pentru eliminarea sau diminuarea vulnerabilităţilor care au cauzat incidentul.

OSRSRITC este responsabil cu documentarea anchetei privind incidentul cu asistenţă din partea ERIS.

OSRSRITC este responsabil de coordonarea activităţilor de comunicare cu terţi pentru rezolvarea incidentului.

În cazul în care incidentul nu implică acţiuni contrare legilor în vigoare RPD va recomanda ARSRITC sancţiuni disciplinare.

În cazul în care incidentul implică aplicarea legilor civile sau penale RPD va recomanda ARSRITC sesizarea organelor în drept ale statului şi va acţiona ca ofiţer de legătură cu acestea.

Monitorizarea Resurselor Informatice şi de Comunicaţii

Monitorizarea RSRITC se va face astfel încât să fie posibilă detectarea în timp util a atacurilor informatice şi a situaţiilor de încălcare a regulamentelor de securitate. Echipamentele utilizate pentru monitorizare (dedicate sau nu) vor urmări şi înregistra:

- ✓ Tipul traficului (ex. structura pe protocoale şi servicii) extern şi conţinutul acestuia în cazurile în care acest lucru se impune sau este ordonat;
- ✓ Tipul traficului în reţea, a protocoalelor şi a echipamentelor conectate la RSRITC, conţinutul acestuia în cazurile în care acest lucru se impune sau este ordonat;
- ✓ Parametrii de securitate pentru sistemele individuale (la nivelul sistemelor de operare).

Fişierele jurnal vor fi examinate regulat în vederea detectării eventualelor atacuri informatice şi abateri de la regulamentele de securitate ale Operatorului.

În această categorie intră următoarele (fără a se limita doar la acestea):

- ✓ Jurnale ale sistemelor de detectarea automată a intruşilor;
- ✓ Jurnale Firewall;
- ✓ Jurnale ale activităţii conturilor utilizator;
- ✓ Jurnale ale scanărilor reţea;
- ✓ Jurnale ale aplicaţiilor;
- ✓ Jurnale ale erorilor din sisteme şi servere.

Securitatea Serverelor

Un server nu trebuie conectat la reţeaua Operatorului până când nu se află într-o stare sigură acreditată de către OSRIC.

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 şi a driver-lor care nu sunt necesare;
- ✓ Setarea/activarea parametrilor de securitate, a protecţiilor pentru fişiere şi activarea jurnalelor de monitorizare;
- ✓ Dezactivarea sau schimbarea parolelor conturilor predefinite;
- ✓ Securizarea accesului fizic la aceste echipamente.

Compartimentul de Informatică va monitoriza obligatoriu pentru serverele principale (enterprise) procesul de instalare şi aplicare regulată a patch-urilor de securitate şi, prin sondaj, pentru serverele departamentale sau a grupurilor de lucru.

Crearea şi Utilizarea Copiilor de Siguranţă (Backup)

Frecvenţa, dimensiunea şi conţinutul copiilor de siguranţă trebuie să fie în concordanţă cu importanţa informaţiei şi cu riscul acceptat de proprietarul datelor.

Procedura de creare a copiilor de siguranţă şi de recuperare pentru fiecare sistem din cadrul RSRITC trebuie să fie documentată şi periodic revizuită.

Verificarea copiilor de siguranţă se va face după o procedură documentată şi revizuită periodic.

Copiile de siguranţă trebuie să fie periodic testate pentru a asigura faptul că informaţiile stocate sunt recuperabile.

Accesul la mediile de backup ale Operatorului se va face numai de personalul abilitat în acest sens.

Accesul trebuie interzis pentru persoanele autorizate care îşi schimbă locul de muncă.

Detectarea Tentativelor de Acces Neautorizat

Procesele de înregistrare şi verificare a activităţii sistemelor de operare, conturilor utilizator şi programelor trebuie să fie funcţionale pe toate sistemele active (host, server, echipamente de reţea).

Trebuie activate funcţiile de anunţare a persoanelor responsabile oferite de firewall-uri şi sistemele de control al accesului la reţea.

Trebuie activate funcţiile de înregistrare a evenimentelor pe dispozitivele firewall şi pe toate sistemele de control al accesului.

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

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

Înregistrările de verificare pentru serverele şi host-urile din reţeaua internă trebuie revizuite cel puţin săptămânal.

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

Toate rapoartele privind incidentele trebuie revizuite 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 OSRIC-RPD.

Utilizatorii sunt obligaţi să raporteze orice anomalii în performanţa sistemelor utilizate cât şi orice semne ale unor posibile infracţiuni la OSRSRITC- RPD.

Utilizarea Calculatoarelor Portabile

OSRSRITC–RPD trebuie să aprobe, în scris, conectarea dispozitivelor portabile la RSRITC ale Instituţiei.

Calculatoarele portabile trebuie să fie protejate prin parole.

Se va evita stocarea datelor care privesc Operatorul pe dispozitivele portabile. În cazul în care nu există o altă alternativă de stocare locală, toate datele care privesc Operatorul trebuiesc criptate.

Conectarea sistemelor de calcul care nu sunt proprietatea Operatorului se face numai cu aprobarea în scris a Compartimentul de Informatică la recomandarea Departamentelor.

Dispozitivele portabile de calcul neutilizate trebuie securizate fizic. Aceasta presupune încuierea lor într-un birou, într-un dulap.

Modificări şi Modernizări ale Sistemului Resurselor Informatice şi de Comunicaţii

Orice modificare asupra unei componente a RSRITC din cadrul Operatorului, cum ar fi: sisteme de operare, componente hardware, echipamente şi componente de reţea, aplicaţii, este supusă prezentului regulament şi trebuie să urmeze procedurile în vigoare.

Compartimentul de Informatică trebuie să fie anunţat de toate modificările care afectează mediul de funcţionare a sistemelor componente ale RSRITC.

Toate propunerile de modernizare şi extindere a elementelor de infrastructură a sistemului RSRITC vor fi documentate şi aprobate de către ARIC. Nu este permisă modificarea de către utilizatori a elementelor de infrastructură a RSRITC.

Modificările şi modernizările sistemelor de calcul vor fi documentate de către utilizator şi aprobate de către conducerea instituţiei.

Utilizare Internet şi Intranet

Programele pentru acces la reţeaua Internet sunt destinate utilizatorilor autorizaţi pentru a fi folosite în scopuri exclusiv de servici, cu excepţia situaţiei prevăzute în regulamentul Utilizarea ocazională a RSRITC în scopuri personale.

Toate programele utilizate pentru acces la reţeaua Internet trebuie să facă parte din pachetul de programe aprobat de către Compartimentul de Informatică. Aceste programe trebuie să includă toate patch-urile de securitate puse la dispoziţie 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.

Toate informaţiile accesate în reţeaua Internet trebuie să se conformeze Regulamentului de Utilizare Acceptabilă a RSRITC.

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

Nu se vor publica pe sit-urile web ale Operatorului materiale cu caracter ofensiv sau de hărţuire.

Nu se vor publica pe sit-urile web ale Operatorlui date ale Operatorului fără asigurarea că materialele sunt disponibile numai persoanelor sau grupurilor autorizate.

Nu este permisă utilizarea RSRITC al Operatorului în scop personal sau pentru solicitări personale ce nu au legătură cu Operatorul. Orice material confidenţial al Operatorului transmis prin reţeaua Internet trebuie criptat.

Fişierele electronice se supun aceloraşi reguli de păstrare ce se aplică şi altor documente şi trebuie păstrate în conformitate cu regulile stabilite prin prezentele regulamente şi regulamentele proprii fiecărui Departament.

Este interzisă accesarea site-urilor cu caracter pornografic.

Este interzisă folosirea programelor peer-to-peer.

Este interzisă descărcarea/instalarea programelor din reţeaua Internet.

Administrarea Conturilor

Prin acord individual, fişa postului şi/sau alte documente toţi utilizatorii acceptă prevederile regulamentelor privind securitatea sistemului RSRITC.

Toţi utilizatorii sunt obligaţi să păstreze confidenţialitatea informaţiilor privind contul de acces.

Toate parolele pentru conturi trebuie să fie create şi folosite în conformitate cu Regulamentul privind Parolele de Acces.

Conturile utilizator ale persoanelor plecate din Instituţie pe timp îndelungat (mai mult de 90 de zile) vor fi dezactivate (conturile nu vor mai putea fi accesate).

Toate conturile utilizator care nu au fost accesate timp de 30 de zile vor fi dezactivate. După încă 30 zile conturile vor fi şterse dacă nu s-a solicitat accesul la acestea.

Administratorii de sisteme sau alt personal autorizat sunt responsabili de ştergerea conturilor persoanelor (utilizatorilor) care nu mai lucrează pentru Operator, sau care nu mai au relaţii cu Operatorul.

Parole de Acces

Toate parolele trebuie să îndeplinească următoarele condiţii:

- ✓ Să fie schimbate de utilizator în mod regulat, cel puţin o dată la 90 de zile;
- ✓ Să aibă o lungime minimă de 6 caractere;
- ✓ Să fie parole complexe;
- ✓ Reutilizarea parolelor este interzisă;
- ✓ Parolele stocate trebuie criptate;

Parolele de cont utilizator nu trebuie 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.

Administratorii de sistem nu trebuie să permită schimbarea parolelor utilizatorilor folosind contul administrativ.

Utilizatorii nu pot folosi programe de stocare a parolelor. Se pot face excepţii pentru anumite aplicaţii (precum backup automat) cu aprobarea OSRIC-RPD.

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.

Sistemul de Mesagerie Electronică

Următoarele activităţi sunt interzise de regulament:

- ✓ Trimiterea de mesaje cu caracter de intimidare sau hărţuire;
- ✓ Folosirea sistemului de mesagerie electronică în scopuri personale;
- ✓ Folosirea sistemului de mesagerie electronică în scopuri politice sau pentru campanii politice;
- ✓ Încălcarea drepturilor de autor prin distribuirea neautorizată a materialelor protejate;
- ✓ Folosirea altei identităţi decât cea reală atunci când se trimite email, exceptând cazurile când persoana este autorizată în scop de suport administrativ.
- ✓ Folosirea programelor de poştă electronică neautorizate.
- ✓ Trimiterea sau retrimiterea email-urilor în lanţ;
- ✓ Trimiterea mesajelor nesolicitate către grupuri de persoane, exceptând cazurile în care aceste mesaje deservesc interesele companiei;
- ✓ Trimiterea mesajelor de dimensiuni foarte mari;
- ✓ Trimiterea sau retrimiterea mesajelor ce pot conţine viruşi.

Toate informaţiile şi datele confidenţiale ale Operatorului, transmise către alte reţele externe, trebuie să fie criptate.

Toate activităţile utilizatorilor ce implică accesul şi/sau folosirea RSRITC ale Operatorului pot fi oricând înregistrate şi analizate.

Utilizatorii serviciilor de mesagerie electronică nu trebuie să dea impresia că reprezintă, că îşi spun opinia sau dau declaraţii în numele Operatorului, cu excepţia situaţiilor în care aceştia sunt autorizaţi în mod corespunzător (implicit sau explicit) să facă acest lucru. Atunci când este cazul, se va include o declaraţie explicită prin care utilizatorul specifică faptul că nu reprezintă Operatorul.

Utilizatorii nu trebuie să trimită, retrimită sau să primească informaţii confidenţiale sau senzitive ce privesc Operatorul, folosind conturi utilizator care nu sunt proprietatea Operatorului. Exemple de astfel de conturi, sunt (dar nu sunt limitate numai la acestea: Hotmail, Yahoo mail, AOL mail), precum şi adrese de email puse la dispoziţie de alţi Furnizorii de Servicii Internet.

Utilizatorii nu trebuie să trimită, retrimită, primească sau să stocheze informaţii confidenţiale sau nesigure, ce privesc Operatorul, folosind dispozitive de comunicaţii mobile care nu sunt autorizate de Operator. Exemple de astfel de dispozitive (dar nu sunt limitate numai la acestea) sunt: asistenţi digitali personali, pagere ce permit trimiterea/primirea de informaţii şi telefoanele mobile.

Detectarea viruşilor

Toate staţiile de lucru de sine stătătoare sau conectate la reţeaua de comunicaţii a Operatorului, trebuie să utilizeze programe antivirus aprobate de către OSRIC.

Programele antivirus nu trebuie dezactivate.

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

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

Orice server de fişiere conectat la reţeaua Instituţiei trebuie să utilizeze un program antivirus aprobat în scopul detectării şi curăţirii viruşilor care pot infecta fişierele puse la dispoziţie.

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

Orice virus care nu a putut fi înlăturat automat de către programul antivirus constituie un incident de securitate şi trebuie raportat imediat OSRIC-RPD –ARIC-ANSPDCP.

Licenţe de utilizare

Toate aplicațiile folosite în interesul Operatorului atât sistemele de operare cât și aplicațiile specifice vor fi folosite cu licență.

Operatorul trebuie să se pună de acord în mod adecvat cu furnizorii implicaţi pentru obţinerea de copii adiţionale ale licenţelor dacă şi când acestea sunt necesare în activitatea instituţiei.

Copiile suplimentare ale materialelor protejate prin drepturi de autor nu vor fi stocate pe sistemele sau resursele reţelei Operatorului în situaţia în care nu există aprobări specifice. Administratorii de sistem vor şterge produsele şi toate materialele protejate prin drepturi de autor în situaţia menţionată, cu excepţia cazului în care utilizatorii implicaţi fac dovada autorizaţiei de folosire sau stocare de la producătorii de drept.

Programele sau alte bunuri informatice aflate sub incidenţa drepturilor de autor aflate în posesia Operatorului nu vor fi copiate, cu excepţia cazului în care această copiere este în concordanţă cu prevederile licenţei.

Relaţii cu terţi

Orice activitate desfăşurată de furnizor care implică acces la RSRITC trebuie să se conformeze cu regulamentele în vigoare ale Operatorului.

În toate convenţiile şi contractele încheiate cu Furnizori trebuie specificate următoarele:

Informaţiile din cadrul Operatorului, la care Furnizorul are drept de acces;

Modul în care informaţiile la care Furnizorul are drept de acces urmează a fi protejate de către acesta precum şi măsuri ce vor fi luate în cazul nerespectării clauzelor;

Metodele de predare, distrugere sau de transfer al drepturilor informaţiilor Instituţiei aflate în posesia Furnizorului, la încheierea contractului.

Furnizorul trebuie să folosească sistemul RSRITC din cadrul Operatorului numai în scopul stipulat în contract.

Orice altă informaţie din sistemul RSRITC al Operatorului obţinută de Furnizor pe durata contractului nu poate fi folosită în interes propriu de către Furnizor sau divulgată altora.

Toate echipamentele de întreţinere ale Furnizorului, aflate în reţeaua internă a Operatorului şi care se pot conecta în exterior prin intermediul reţelei, a liniilor telefonice sau a liniilor închiriate, precum şi toate conturile de utilizator create temporar pentru Furnizor şi necesare pentru acces la RSRITC ale Operatorului, vor fi scoase din uz la încheierea relaţiilor contractuale.

Accesul Furnizorului trebuie să fie identificat în mod unic iar administrarea parolelor sau metodele de autentificare trebuie să fie în conformitate cu Regulamentul privind Parolele de Acces şi Regulamentul de Acces Administrativ.

Activităţile principale ale Furnizorului trebuie să fie documentate de acesta şi puse la dispoziţia conducerii Operatorului, la cerere. Acestea trebuie să cuprindă, dar să nu fie limitate la, evenimente precum: schimbări de personal, schimbări de parolă, schimbări majore în derularea proiectului, timpii de sosire, de plecare şi de livrare.

În cazul retragerii din contract a unui angajat al Furnizorului, indiferent de motiv, Furnizorul se va asigura că toate informaţiile sensibile sunt colectate şi predate Operatorului sau distruse în cel mult 24 de ore de la producerea evenimentului.

În cazul terminării/rezilierii contractului sau la cererea Operatorului, Furnizorul va preda sau distruge toate informaţiile ce aparţin Operatorului şi va oferi certificare în scris privind predarea sau distrugerea informaţiilor în decurs de 24 de ore de la producerea evenimentului.

În cazul încheierii contractului sau la cererea Operatorului, Furnizorul trebuie să predea imediat toate legitimaţiile, cartelele de acces, echipamentele şi stocurile Operatorului.

Echipamentele şi/sau stocurile care urmează a fi reţinute de către Furnizor trebuiesc documentate şi autorizate de Conducerea Operatorului.

Toate programele folosite de Furnizor în scopul furnizării serviciilor stipulate în contract către Operator trebuie să fie inventariate corespunzător si să posede drepturi de utilizare atestate prin Licenţe.

Avizat RPD

Aprobat Primar

Iniţiator
Megyeri Tamás-Róbert
Primarul comunei Căpleni

Avizat
Csizmar Erika
Secretar general

……..

…….