



ROMÂNIA
JUDEȚUL CLUJ
MUNICIPIUL CÂMPIA TURZII

DISPOZIȚIA NR. 274 din 25.04.2019

privind aprobarea Politicii și Regulamentului de Securitate privind Sistemul Resurselor Informatice și de Comunicații din Primăria Câmpia Turzii actualizat

Primarul municipiului Câmpia Turzii:

Văzând:

- referatul nr. 12938/22.04.2019, al Serviciului Resurse Umane Salarizare, cu privire la aprobarea Politicii și Regulamentului de Securitate privind Sistemul Resurselor Informatice și de Comunicații din Primăria Câmpia Turzii actualizat;

În conformitate cu prevederile:

- noului Regulament UE 2016/679 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date;

În temeiul art. 68 din Legea nr. 215/2001, republicată, privind administrația publică locală,

DISPUN:

Art. 1. Se aprobă Politica și Regulamentul de Securitate privind Sistemul Resurselor Informatice și de Comunicații din Primăria Câmpia Turzii actualizat, conform Anexei nr.1, care face parte integrantă din prezenta dispoziție.

Art.2. Cu ducerea la îndeplinire a prezentei dispoziții se încredințează tot personalul instituției

Art.3. Publicitatea Politicii și Regulamentului de Securitate privind Sistemul Resurselor Informatice și de Comunicații din Primăria Câmpia Turzii actualizat, prin postarea pe pagina web www.campiaturzii.ro și se comunică întregului personal prin intermediul șefilor de servicii/compartimente.

Art.4. Prezenta dispoziție se comunică șefilor de servicii/compartimente prin grija Serviciului Juridic.

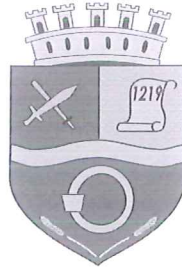
PRIMAR,
Dorin Nicolae LOJIGAN

AVIZAT,
SECRETAR
Nicolae ȘTEFAN

Camelia Mădălina Marinca - șef serviciu SRUS

Redactat: Adrian-Sandu NICOARĂ consilier SRUS

4 ex



ROMÂNIA
JUDEȚUL CLUJ
MUNICIPIUL CÂMPIA TURZII

Nesecret. ex.

Politica și Regulamentul de Securitate privind

SISTEMUL RESURSELOR INFORMATICE ȘI DE COMUNICAȚII

din

PRIMĂRIA CÂMPIA TURZII

Cap. I

Politica de Securitate privind Sistemul Resurselor Informatice și de Comunicații

1.1 Introducere

În acord cu prevederile din prezentul document, Resursele Informatice și de Comunicații (RIC) sunt bunuri strategice ale Primăriei Câmpia Turzii care trebuie administrate ca resurse ale statului român.

Compromiterea securității sistemului RIC poate afecta capacitatea Primăriei Câmpia Turzii de a oferi serviciile specifice, poate conduce la fraude, sau distrugerea datelor, violarea clauzelor contractuale, divulgarea secretelor, afectarea credibilității Primăriei Câmpia Turzii în fața partenerilor săi.

Această politică este stabilită astfel încât:

- Să fie în conformitate cu statutul, regulamentele, legile și alte documente oficiale în vigoare privind administrarea resurselor informatice publice;
- Să stabilească practici prudente și acceptabile privind utilizarea RIC ale Primăriei Câmpia Turzii;
- Să instruiască utilizatorii care au dreptul de folosire a sistemului RIC privind responsabilitățile asociate unei astfel de utilizări;

Politica de securitate a sistemului RIC al Primăriei Câmpia Turzii se aplică nediscriminatoriu tuturor persoanelor cărora li s-a permis accesul la orice resursă informatică și de comunicații a Primăriei Câmpia Turzii .

Următoarele entități și utilizatori sunt vizați în mod distinct de prevederile Politicii:

- Angajații cu contract de muncă pe perioadă determinată sau nedeterminată care au acces la sistemul informațional și de comunicații;
- Colaboratorii Primăriei Câmpia Turzii care au acces la sistemul RIC;
- Furnizorii Primăriei Câmpia Turzii care au acces la sistemul RIC;
- Studenții/elevii care fac practică la Primăria Câmpia Turzii ;
- Alte persoane, entități sau organizații care au acces la sistemul RIC.

1.2 Scopul politicii de securitate

Având în vedere că majoritatea personalului instituției a beneficiat de cursul ECDL, precum și faptul că angajații au trecut de o probă practică de utilizare a calculatorului se presupune că aceștia sunt familiarizați cu termenii tehnici și de asemenea cunosc sistemul de operare Windows și pachetul de programe Microsoft Office.

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

Confidențialitatea se referă la protecția datelor împotriva accesului neautorizat. Fișierele electronice create, trimise, primite sau stocate pe sistemele de calcul aflate în proprietatea, administrarea sau în custodia și sub controlul Primăriei Câmpia Turzii, sunt proprietatea instituției în condițiile legilor în vigoare. Utilizatorul răspunde personal de confidențialitatea datelor încredințate prin procedurile de acces la sistemul RIC.

Integritatea se referă la măsurile și procedurile utilizate pentru protecția datelor împotriva modificărilor sau distrugerii neautorizate.

Disponibilitatea se asigură prin funcționarea continuă a tuturor componentelor sistemului RIC. Diverse aplicații au nevoie de nivele diferite de disponibilitate în funcție de impactul sau daunele produse ca urmare a nefuncționării corespunzătoare a sistemului RIC.

Politica de securitate are ca scop, de asemenea, stabilirea cadrului necesar pentru elaborarea regulamentelor și procedurilor de securitate. Acestea sunt obligatorii pentru toți utilizatorii sistemului RIC.

1.3 Definiții folosite în politica de securitate și regulamentul de utilizare

Resurse Informatice și de Comunicații (RIC): toate dispozitivele de tipărire/imprimare, dispozitive de afișare, unități de stocare, și toate activitățile asociate calculatorului care implică utilizarea oricărui dispozitiv capabil să recepționeze 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), sisteme de procesare distribuită, echipament de laborator și medical conectat la rețea și controlat prin calculator (tehnologie încapsulată), resurse de telecomunicații, medii de rețea, telefoane, faxuri, imprimante și alte accesorii. La acestea se adaugă procedurile, echipamentul, facilitățile, programele și datele care sunt proiectate, construite, puse în funcțiune (operaționale) și menținute pentru a crea, colecta, înregistra, procesa, stoca, primi, afișa și transmite informația.

Administratorul Resurselor Informatice și de Comunicații (ARIC): Responsabil la nivelul Primăriei Câmpia Turzii cu administrarea și finanțarea RIC. Desemnarea ARIC are ca scop stabilirea în mod clar a responsabilității privind crearea, modificarea și aprobarea regulamentelor privind activitățile de finanțare, administrare și utilizare a RIC. Titlul este atribuit în mod automat ordonatorului de credite, adică primarului.

Ofițer responsabil cu Securitatea RIC (OSRIC): Răspunde direct doar în fața ARIC privind administrarea funcțiilor de securitate a informației în cadrul Primăriei Câmpia Turzii. Este persoana de contact intern și extern a Primăriei Câmpia Turzii pentru orice problemă în legătură cu securitatea RIC. Funcția OSRIC este atribuită administratorului de rețea (specialistul IT din cadrul instituției).

Responsabil cu protecția datelor cu caracter personal (DPO): DPO răspunde în fața celui mai înalt nivel al conducerii operatorului. Rolul DPO este de a informa și consilia operatorul referitor la protecția datelor, de a monitoriza respectarea Regulamentului UE 679/2016, de a coopera cu autoritatea de supraveghere

Ofițer responsabil cu securitatea RIC la nivel Departamental (OSRICD): Persoana responsabilă de monitorizarea și implementarea controalelor de securitate și a procedurilor pentru sistemul RIC la nivelul unui Departament. Funcția OSRICD este atribuită șefului de serviciu, birou, departament.

Utilizator: O persoană, o aplicație automatizată sau proces utilizator autorizat de către Primăria Câmpia Turzii, în conformitate cu procedurile și regulamentele în vigoare, să folosească RIC.

Abuz de privilegii: Orice acțiune întreprinsă în mod voit de un utilizator, care vine în contradicție cu regulamentele Primăriei Câmpia Turzii și/sau legile în vigoare, inclusiv cazul în care, din punct de vedere tehnic, nu se poate preveni înfăptuirea de către utilizator a acțiunii respective.

Furnizor: Persoană fizică/juridică care oferă bunuri și/sau servicii Primăriei Câmpia Turzii în baza unui contract comercial sau de colaborare.

Internet: Sistem global care interconectează calculatoare și rețele de calculatoare. Acestea sunt deținute de mai multe organizații, agenții guvernamentale, societăți, instituții academice.

Intranet: Rețea privată destinată comunicațiilor și partajării informațiilor, care, ca și rețeaua Internet, folosește suita de protocoale TCP/IP, însă este accesibilă doar utilizatorilor autorizați din cadrul unei organizații (instituții). În mod obișnuit, rețeaua Intranet a unei organizații este protejată printr-un sistem de protecție (firewall).

Echipe de Răspuns la Incidentele de Securitate a RIC (ERIS): persoanele responsabile de acțiunile desfășurate în scopul micșorării sau eliminării impactului negativ al unui incident de securitate. ERIS este formată din ARIC, OSRIC, DPO, OSRICD.

Virus: Un program care se auto-atașează la un fișier executabil sau la o aplicație vulnerabilă și care generează efecte de la cele deranjante până la cele distructive. Un virus se execută în momentul în care este accesat un fișier 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 același calculator sau pot fi trimise către alte calculatoare prin intermediul rețelei. Prima utilizare a termenului descria un program care s-a multiplicat într-o rețea de calculatoare, folosind resursele sau calculatoarele neutilizate din rețea pentru a distribui aceste copii. Unii dintre acești viermi reprezintă o amenințare la adresa securității datorită faptului că folosesc rețeaua pentru a se împrăști, împotriva voinței proprietarilor de sisteme de calcul, cauzând astfel nefuncționarea sau funcționarea defectuoasă a rețelei. Un vierme este asemănător unui virus prin faptul că se auto-copiază, diferența constând în faptul că un vierme nu are nevoie să se atașeze la anumite fișiere 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 fișier 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 integrității și/sau confidențialității informației 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 informațiilor, modificarea informațiilor sistemului referitoare la caracteristicile componentelor hardware, firmware sau software cu sau fără știința sau intenția utilizatorului.

Rețea locală (LAN): O rețea de comunicații de date ce este distribuită pe o zonă restrânsă (de regulă la nivelul unui grup de lucru). Rețeaua locală oferă comunicații între calculatoare și periferice la o viteză de transfer mare și cu puține erori.

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

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

Copii de Siguranță (backup): Copii ale fișierelor și aplicațiilor făcute pentru a evita pierderea datelor și pentru a permite recuperarea în cazul unor evenimente care pot conduce la pierderi de date.

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

Atac informațional: O încercare de a trece peste măsurile și controalele de securitate fizice sau informatice care protejează un sistem din cadrul sistemului de RIC. Atacatorul poate altera informațiile, poate acorda sau refuza accesul la ele. Succesul unui eventual atac depinde de gradul de vulnerabilitate al sistemului în particular și de eficacitatea contramăsurilor aplicate.

Protecție informațională: Acțiuni întreprinse în vederea afectării informațiilor și sistemelor informatice ostile, în timp ce protejează informațiile și sistemele informatice proprii.

Procedura - reprezintă modalitatea specifică de desfășurare a unei activități sau a unui proces.

1.4 Clasificarea Informațiilor

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

Pentru a asigura securitatea și integritatea informațiilor, acestea se împart în trei categorii principale:

- Publice
- Secrete
- Strict Secrete

ARIC, OSRIC, OSRICD, conducerea instituției răspund de evaluarea periodică a schemei de clasificare a informațiilor. Toate informațiile din Primăria Câmpia Turzii trebuie să se regăsească în una din următoarele categorii:

1. **Publice.** Acestea sunt informațiile accesibile oricărui utilizator din interiorul sau exteriorul Primăriei Câmpia Turzii. Divulgarea, utilizarea neautorizată sau distrugerea acestora nu produce efecte asupra Primăriei Câmpia Turzii sau aceste efecte sunt ne semnificative. Utilizatorii care furnizează aceste informații sunt responsabili de asigurarea integrității și disponibilității acestora în raport cu cerințele Primăriei Câmpia Turzii.

2. **Secrete.** În această categorie se includ informațiile pe care Primăria Câmpia Turzii trebuie să le protejeze conform legislației în vigoare. Aceste date trebuie distruse dacă au fost făcute publice. Aceste date vor fi copiate și distribuite în cadrul Primăriei Câmpia Turzii doar utilizatorilor autorizați. Distribuirea acestor informații de către utilizatorii autorizați trebuie să se facă pe baza unei clauze de confidențialitate.

3. **Strict Secrete sau Confidențiale.** În această categorie se includ toate informațiile care datorită valorii naturii lor nu trebuie făcute publice. Divulgarea, utilizarea sau distrugerea acestor date poate intra sub incidența Codului Civil, Penal sau legislației în vigoare. Accesul la aceste informații va fi restricționat. Datele strict secrete nu pot fi copiate, distribuite sau șterse fără acordul scris al conducerii Primăriei Câmpia Turzii.

1.5 Confidențialitate

1. Fișierele electronice create, trimise, primite sau stocate folosind sistemul RIC propriu, administrate sau în custodia și sub controlul Primăriei Câmpia Turzii nu au caracter personal și pot fi accesate oricând de către angajații autorizați (specialistul IT/administrator rețea) fără înștiințarea utilizatorului.
2. În scopul administrării RIC și pentru asigurarea securității RIC personalul autorizat poate revizui sau utiliza orice informație stocată pe sau transportată prin sistemele RIC în conformitate cu legile în vigoare. În aceleași scopuri, este posibilă monitorizarea activității utilizatorilor.
3. Utilizatorii trebuie să raporteze orice slăbiciune în sistemul de securitate al calculatoarelor din cadrul Primăriei Câmpia Turzii, orice incident de posibilă întrebuițare greșită sau încălcare a acestui regulament (prin contactarea OSRIC sau OSRICD).
4. Un mare număr de utilizatori, pot accesa diverse informații din sistemul de comunicații al Primăriei Câmpia Turzii. În aceste condiții este obligatorie păstrarea confidențialității acestor informațiilor transmise din exteriorul RIC și a informațiilor obținute din interior.
5. Utilizatorii nu trebuie să încerce să acceseze informații sau programe de pe sistemele Primăriei Câmpia Turzii pentru care nu au autorizație sau consimțământ explicit.
6. Nici un utilizator al sistemului RIC ale Primăriei Câmpia Turzii nu poate divulga informațiile la care are acces sau la care a avut acces ca urmare a unei vulnerabilități a sistemului RIC. Această regulă se extinde și după ce utilizatorul a încheiat relațiile cu Primăria Câmpia Turzii, conform angajamentelor personale sau contractelor de munca semnate, existente în cadrul Serviciului Resurse Umane.
7. Confidențialitatea informațiilor transmise prin intermediul resurselor de comunicații ale terților nu poate fi asigurată. Pentru aceste situații, confidențialitatea și integritatea informațiilor se poate asigura folosind tehnici de criptare. Utilizatorii sunt obligați să se asigure că toate informațiile confidențiale ale Primăriei Câmpia Turzii se transmit în așa fel încât să se asigure confidențialitatea și integritatea acestora.
8. În vederea asigurării unui grad mai sporit de securitate și confidențialitate a informațiilor transmise prin sistemul de comunicații al Primăriei Câmpia Turzii nu vor fi utilizate adresele de e-mail și parolele personale, ci doar adresele de e-mail autorizate.
9. Utilizarea sistemului BYOD se poate face doar cu acordul OSRIC și ARIC.

Cap. II Regulamentele de Utilizare a Resurselor Informatice și de Comunicații (RIC)

Introducere

Regulamentele de Utilizare a Resurselor Informatice și de Comunicații sunt elaborate pentru a stabili un cadru corect, legal și eficient de utilizare a tehnologiei informației și comunicațiilor în Primăria Câmpia Turzii. Acestea au ca scop principal protejarea utilizatorilor, colaboratorilor împotriva atacurilor de orice tip (cu sau fără intenție). De asemenea acestea au ca scop protejarea imaginii instituției și a investițiilor acesteia pentru dezvoltarea sistemului informatic și de comunicații.

În acord cu legislația în vigoare în România, Regulamentele de ordine interioară ale Primăriei Câmpia Turzii, Resursele Informatice și de Comunicații sunt valori ale Primăriei Câmpia Turzii care trebuie exploatate și administrate ca resurse publice în proprietatea statului român.

Scopul acestor regulamente este acela de a asigura:

- Stabilirea unor reguli corecte, echitabile și eficiente pentru folosirea resurselor informatice și de comunicații în vederea sprijinirii procesului educațional și a cercetării științifice;

- Protejarea imaginii Primăriei Câmpia Turzii;
- Protejarea investițiilor Primăriei Câmpia Turzii pentru dezvoltarea sistemului informatic și de comunicații propriu;
- Protejarea proprietății intelectuale și a tuturor informațiilor stocate și transportate folosind Resursele Informatică și de Comunicații ale utilizatorilor autorizați: membrii conducerii (primar, viceprimar, secretar), funcționari publici, personal contractual, studenți/elevi aflați în practică, voluntari, colaboratori etc.
- Educarea utilizatorilor resurselor informatice și de comunicații în ceea ce privește responsabilitățile asociate cu utilizarea acestora;
- Compatibilitate cu regulamentele, statutul și atribuțiile stabilite pentru administrarea resurselor informatice și de comunicații

Regulamentele de utilizare a resurselor informatice și de comunicații ale Primăriei Câmpia Turzii se aplică nediscriminatoriu tuturor persoanelor cărora li s-a permis accesul la acesta.

Regulamentele și procedurile de lucru sunt elaborate de responsabilul IT din cadrul instituției și supuse spre aprobare conducerii.

Prevederile Politicii de Securitate aprobate vor fi aplicate tuturor entităților și utilizatorilor după cum urmează:

- Angajații cu contract de muncă pe perioadă determinată sau nedeterminată care au acces la sistemul informațional și de comunicații;
- Colaboratorii Primăria Câmpia Turzii care au acces la sistemul RIC;
- Furnizorii Primăriei Câmpia Turzii care au acces la sistemul RIC;
- Voluntarii sau studenții/elevii care fac practică la Primăria Câmpia Turzii ;
- Alte persoane, entități sau organizații care au acces la sistemul RIC.

Modificarea regulamentului și/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.

2.1 Regulament de utilizare a RIC

1. Utilizarea sistemului RIC se face numai în interes de serviciu.
2. Utilizatorii trebuie să anunțe OSRIC sau OSRICD în cazul în care se observă orice problemă/breșă în sistemul de securitate a RIC din cadrul Primăriei Câmpia Turzii, cât și orice posibilă întrebuintare greșită sau încălcare a regulamentelor în vigoare.
3. Utilizatorii, prin acțiunile lor, nu trebuie să încerce să compromită protecția sistemelor informatice și de comunicații și nu trebuie să desfășoare, deliberat sau accidental, acțiuni care pot afecta confidențialitatea, integritatea și disponibilitatea informațiilor de orice tip în cadrul sistemului RIC al Primăriei Câmpia Turzii.
4. Utilizatorii nu trebuie să încerce să obțină acces la date sau programe din RIC pentru care nu au autorizație sau consimțământ explicit.
5. 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 și/sau informații similare utilizate în scopuri de autorizare și identificare.
6. Utilizatorii nu trebuie să facă copii neautorizate sau să distribuie materiale protejate prin legile privind proprietatea intelectuală (copyright).
7. Utilizatorii nu trebuie să utilizeze programe de tip shareware sau freeware, fără aprobarea OSRIC, cu excepția cazului în care acestea se găsesc pe lista programelor standard folosite în cadrul Primăriei Câmpia Turzii. Această listă va fi întocmită de către OSRIC împreună cu OSRICD în funcție de necesitățile departamentelor.
8. Utilizatorii nu trebuie:
 - să se angajeze într-o activitate care ar putea hărțui sau amenința alte persoane;
 - să degradeze performanțele RIC;
 - să împiedice accesul unui utilizator autorizat la RIC;

- să obțină alte resurse în afara celor alocate;
 - să nu ia în considerare măsurile de securitate impuse prin regulamente;
 - să exploateze defectuos componentele RIC;
 - să utilizeze dischete, cd-uri, sau orice alt suport magnetic de stocare a informației din exteriorul instituției fără acordul explicit al OSIRC;
9. Utilizatorii nu trebuie să descarce, instaleze și să ruleze programe de securitate sau utilitare care expun sau exploatează vulnerabilități ale securității RIC. De exemplu, utilizatorii din Primăriei Câmpia Turzii nu trebuie să ruleze programe de decriptare a parolelor, de captură de trafic, de scanări ale rețelei sau orice alt program nepermis de regulamente.
10. RIC ale Primăriei Câmpia Turzii nu trebuiesc folosite pentru beneficiul personal.
11. Utilizatorii nu trebuie să acceseze, să creeze, să stocheze sau să transmită materiale pe care Primăria Câmpia Turzii le poate considera ofensive, indecente sau obscene (altele decât cele pentru care aprobarea explicită a conducerii instituției).
12. Accesul la rețeaua Internet prin intermediul RIC se supune aceluiași regulamente care se aplică utilizării din interiorul instituției și **Regulamentului pentru Utilizare Internet și Intranet(cap.II subcap.14)**.
13. Angajații nu trebuie să permită membrilor familiei sau altor persoane străine neautorizate, care nu au aprobare explicită din partea ARIC, OSRIC, sau a conducerii instituției accesul la RIC ale Primăriei Câmpia Turzii.
14. Utilizatorii care au acces la sistemul RIC al Primăriei Câmpia Turzii au obligația de a purta acte și/sau legitimații/ecusoane care să ateste calitatea de utilizator autorizat în spațiile Primăriei Câmpia Turzii.
15. Utilizatorii nu trebuie să se angajeze în acțiuni împotriva scopurilor Primăriei Câmpia Turzii folosind RIC.
16. În cazul demisiei/plecării definitive din instituție a unui utilizator acest lucru va fi comunicat OSRIC de către OSRICD și/sau Serviciul Resurse Umane din Cadrul instituției. OSRIC va recurge la stergerea conturilor și parolelor utilizatorului respectiv, iar accesul utilizatorului la RIC va fi interzis.
17. Este interzisă utilizarea RIC de către persoane neautorizate.

2.2. Utilizarea ocazională a RIC în scopuri personale

În aceste situații se aplică următoarele restricții:

- 1.Utilizarea personală ocazională a serviciilor de poștă electronică, acces internet, telefoane, fax-uri, imprimante, copiatoare, etc. este restricționată la utilizatorii autorizați și nu poate fi extinsă la membrii familiilor sau alte persoane.
- 2.Utilizarea ocazională a RIC nu trebuie să aibă drept rezultate costuri directe pentru Primăria Câmpia Turzii.
- 3.Utilizarea ocazională a RIC nu trebuie să afecteze activitatea normală a angajaților.
- 4.Nu este permisă trimiterea sau recepționarea documentelor sau fișierelor care pot cauza acțiuni legale împotriva Primăriei Câmpia Turzii sau prejudicierea, indiferent de formă, a intereselor Instituției.
- 5.Stocarea mesajelor de email, a mesajelor de voce, a documentelor și fișierelor personale din cadrul RIC trebuie să fie nominală.
- 6.Toate mesajele, fișierele și documentele – incluzând mesajele personale, fișierele și documentele – localizate în cadrul RIC sunt proprietatea Instituției și pot fi subiectul unor cereri de verificare/inspectare/accesare de către ARIC, OSRIC sau OSRICD conform regulamentelor.

2.3. Accesul Administrativ

- 1.Utilizatorii trebuie să cunoască și să accepte toate regulamentele privind securitatea RIC înainte de a li se permite accesul la un cont.
- 2.Utilizatorii care au conturi de acces administrativ trebuie sa aibă instrucțiuni de administrare, documentare, instruire și autorizare a conturilor. Aceste instrucțiuni se vor elabora de către fiecare Departament și vor fi incluse în fișa postului.
- 3.Utilizatorii cu drepturi administrative sau speciale de acces nu trebuie să folosească în mod abuziv aceste drepturi și trebuie să facă investigații numai sub îndrumarea OSRIC sau OSRICD.
- 4.Cei care utilizează conturi de acces cu drepturi administrative sau speciale trebuie să folosească tipul de privilegiu cel mai potrivit activității pe care o desfășoară.
- 5.Accesul administrativ trebuie să se conformeze **Regulamentului privind Parolele (cap.II, subcap.2.16)** .
- 6.Parola pentru un cont cu acces privilegiat nu va fi utilizată de mai multe persoane decât cu acordul scris al OSRIC și trebuie să fie schimbată atunci când o persoană care utilizează acest cont își schimbă locul de muncă din cadrul Departamentului sau a Instituției, sau în cazul unei modificări a listei de personal ale terților (furnizor desemnat) în contractele cu Primaria Câmpia Turzii .
- 7.Trebuie să existe o procedură prin care o altă persoană, în afară de administrator, să poată avea acces la contul administratorului în caz de forța majoră. Această procedură va fi elaborată de către OSRIC și comunicată OSRICD aflat în cauză.
- 8.Unele conturi sunt necesare pentru audit (verificare, control) intern sau extern, pentru dezvoltare sau instalare de software sau alte operațiuni definite. Acestea trebuie să îndeplinească următoarele condiții:
 - trebuie să fie autorizate;
 - trebuie create cu dată de expirare specifică;
 - contul va fi șters atunci când nu mai este necesar.

2.4. Accesul Fizic

1. Accesul fizic la toate încăperile în care sunt instalate RIC trebuie să fie documentat și monitorizat.
2. Toate încăperile în care sunt instalate RIC trebuie să fie protejate fizic, în funcție de importanța acestora și tipul datelor vehiculate sau stocate.
3. Pentru fiecare încăpere în care sunt instalate echipamente ale sistemului RIC se aprobă accesul doar pentru personalul care răspunde de buna funcționare a echipamentelor din încăperea respectivă și, dacă este cazul, părților contractante, ale căror obligații contractuale implică acces fizic.
4. Personalul care are drepturi de acces trebuie să dețină legitimație de serviciu și acte de identitate care să-i ateste calitatea.
5. Nu este permis transferul dreptului de acces indiferent de motiv.
6. Accesul publicului, vizitatorilor, sau a persoanelor străine în cadrul instituției se va face doar pe baza actului de identitate. Vizitatorii/persoanele străine trebuie să fie însoțiți în zonele cu acces restricționat.
7. Pentru fiecare spațiu în care sunt instalate RIC se va păstra o evidență a accesului pentru verificări de rutină în situații critice.

2.5. Conectarea la Sistemul Resurselor Informatice și de Comunicații

1. Utilizatorilor le este permis să utilizeze numai parametrii pentru conectare la rețea specificați de către administratorul de rețea .

2. Pentru fiecare sistem conectat trebuie să existe o persoană care să răspundă de acesta, numele și datele de identificare ale acesteia se vor comunica către OSRIC.
3. Conectarea sistemelor de calcul care nu sunt proprietatea Primăriei Câmpia Turzii se face numai cu aprobarea în scris din partea conducerii instituției.
4. Accesul de la distanță la rețeaua Primăriei Câmpia Turzii se va realiza numai prin echipamente aprobate, sau prin intermediul unui Furnizor de Servicii Internet (Internet Service Provider (ISP)) agreat de către Primăria Câmpia Turzii și folosind protocoale aprobate de către OSRIC.
5. Utilizatorii RIC din interiorul Primăriei Câmpia Turzii nu se pot conecta la altă rețea.
6. Utilizatorii nu trebuie să extindă sau să retransmită serviciile de rețea în nici un fel (pe nici o cale). Nu este permisă instalarea de conexiuni de rețea neautorizate indiferent de motiv. Autorizarea tuturor conexiunilor se face la propunerea Departamentelor de către responsabilul IT.
7. Utilizatorii nu trebuie să instaleze echipamente hardware sau programe care furnizează servicii de rețea fără aprobarea responsabilului IT.
8. Sistemele computerizate din afara Instituției care necesită conectare la rețea trebuie să se conformeze cu standardele rețelei interne ale Primăriei Câmpia Turzii.
9. 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. De exemplu, utilizatorii Primăriei Câmpia Turzii nu au dreptul să ruleze programe de spargere a parolei, sustragere de pachete, scanare a porturilor, în timp ce sunt conectați la rețeaua Instituției.
10. Utilizatorii nu au dreptul să modifice, reconfigureze, instaleze, dezinstaleze echipamente de rețea, cabluri, prize de conexiuni.
11. Serviciul de nume și administrarea adreselor IP sunt deservite exclusiv de către responsabilul IT.
12. Serviciile de interconectare a rețelei Primăriei Câmpia Turzii cu alte rețele sunt realizate exclusiv de către responsabilul IT.
13. Nu este permisă instalarea și/sau modificarea echipamentelor utilizate pentru conectare la rețea (inclusiv plăci de rețea) fără aprobarea responsabilului IT. Tipul și modelul plăcilor de rețea și tuturor echipamentelor care se pot conecta în rețea trebuie să fie aprobate de către responsabilul IT.

2.6. Configurarea Parametrilor de Acces la Rețea

1. Infrastructura de comunicații, rețeaua de comunicații digitale, a Primăriei Câmpia Turzii este administrată de către Compartimentul de Informatică care este responsabil cu întreținerea și dezvoltarea acesteia.
2. Pentru a furniza o infrastructură de comunicații unitară cu posibilități de modernizare toate componentele acesteia sunt instalate de către responsabilul IT sau de către un furnizor avizat explicit de către responsabilul IT.
3. Toate echipamentele, fără excepție, conectate la rețeaua de comunicații trebuie configurate conform specificațiilor responsabilului IT.
4. Orice dispozitiv hardware, inclusiv plăcile de rețea și modemuri, care se va conecta la rețeaua Primăriei Câmpia Turzii, trebuie să fie însoțit de o aprobare de tip (producător, model etc.) din partea responsabilului IT.
5. Modificarea configurației oricărui dispozitiv activ conectat la rețeaua de comunicații se face numai de către responsabilul IT.
6. Infrastructura de comunicații de date a Primăriei Câmpia Turzii suportă un set definit de protocoale de rețea (TCP/IP, NwLink IPX/ISP). Orice utilizare a altui set de protocoale trebuie să fie aprobată în scris de către responsabilul IT.
7. Adresele de rețea sunt alocate dinamic sau static numai de către responsabilul IT.
8. Toate conectările în rețeaua de comunicații a Primăriei Câmpia Turzii sunt responsabilitatea responsabilului IT, conectarea se va face numai în baza unei cereri standard aprobată de către conducerea Instituției.

9. Toate conectările dintre rețeaua de comunicații a Primăriei Câmpia Turzii și alte rețele de comunicații, publice sau private, sunt responsabilitatea exclusivă a responsabilului IT
10. Echipamentele de protecție a rețelei de comunicație a Primăriei Câmpia Turzii (firewall) se vor instala de către responsabilul IT.
11. Utilizatorii nu au dreptul să extindă sau să retransmită în nici un fel serviciile rețelei (este interzisă instalarea unui telefon, fax, modem, router, switch, hub sau punct de acces la rețeaua Instituției) fără aprobare din partea responsabilului IT. Utilizatorilor li se interzice instalarea de dispozitive hardware de rețea sau programe care furnizează servicii de rețea fără aprobarea responsabilului IT.
12. Utilizatorilor nu le este permis accesul la dispozitivele hardware ale rețelei.

2.7. Tratarea Incidentelor de Securitate și de nerespectare a Politicii și Regulamentului de Securitate

Membrii Echipei de Răspuns la Incidentele de Securitate (Membrii ERIS) ai Primăriei Câmpia Turzii, au funcții și responsabilități pre-definite care pot fi prioritare îndatoririlor obișnuite.

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

OSRIC este responsabil cu înștiințarea și coordonarea echipei ERIS pentru tratarea incidentului.

OSRIC este responsabil cu strângerea dovezilor fizice și electronice ce vor face parte din documentația pentru tratarea incidentului.

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

OSRIC, în colaborare cu ARIC va stabili conținutul comunicatelor pentru utilizatori privind incidentele și va determina nivelul și modul de distribuire a acestei informații.

OSRIC și ERIS trebuie să comunice proprietarului sau producătorului resursei afectate de un incident informațiile utile pentru eliminarea sau diminuarea vulnerabilităților care au cauzat incidentul.

OSRIC este responsabil cu documentarea anchetei privind incidentul cu asistență din partea ERIS.

OSRIC este responsabil de coordonarea activităților de comunicare cu terți pentru rezolvarea incidentului.

Având în vedere stadiul actual al dezvoltării, natura și domeniul de aplicare, contextul și scopurile prelucrării, precum și riscul cu diferite grade de probabilitate și gravitate pentru drepturile și libertățile persoanelor fizice, ERIS implementează măsuri tehnice și organizatorice adecvate în vederea asigurării unui nivel de securitate corespunzător acestui risc, incluzând printre altele, după caz:

- A) Pseudonimizarea și criptarea datelor cu caracter personal;
- B) Capacitatea de a asigura confidențialitatea, integritatea, disponibilitatea și rezistența continuă ale sistemelor și serviciilor de prelucrare;
- C) Capacitatea de a restabili disponibilitatea datelor cu caracter personal și accesul la acestea în timp util în cazul în care are loc un incident de natură fizică sau tehnică;
- D) Un proces pentru testarea, evaluarea și aprecierea periodică a eficacității măsurilor tehnice și organizatorice pentru a garanta securitatea prelucrării.

La evaluarea nivelului adecvat de securitate, se ține seama în special de riscurile prezentate de prelucrare, generate în special, în mod accidental sau ilegal, de distrugerea, pierderea, modificarea, divulgarea neautorizată sau accesul neautorizat la datele cu caracter personal transmise, stocate sau prelucrate în alt mod.

În cazul în care incidentul nu implică acțiuni contrare legilor în vigoare OSRIC va recomanda ARIC sancțiuni disciplinare.

În cazul în care incidentul implică aplicarea legilor civile sau penale OSRIC va recomanda ARIC sesizarea organelor în drept ale statului și va acționa ca ofițer de legătură cu acestea.

2.8. Monitorizarea Resurselor Informatice și de Comunicații

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

- Tipul traficului (ex. structura pe protocoale și servicii) extern și conținutul acestuia în cazurile în care acest lucru se impune sau este ordonat.
- Tipul traficului în rețea, a protocoalelor și a echipamentelor conectate la RIC, conținutul acestuia în cazurile în care acest lucru se impune sau este ordonat.
- Parametrii de securitate pentru sistemele individuale (la nivelul sistemelor de operare).

Fișierele jurnal vor fi examinate regulat în vederea detectării eventualelor atacuri informatice și abateri de la regulamentele de securitate ale Primăriei Câmpia Turzii .

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

- Jurnale ale sistemelor de detectare automată a intrușilor.
- Jurnale Firewall
- Jurnale ale activității conturilor utilizator
- Jurnale ale scanărilor rețea
- Jurnale ale aplicațiilor
- Jurnale ale solicitărilor de suport tehnic
- Jurnale ale erorilor din sisteme și servere.
- Jurnale ale echipamentelor de telefonie
- În mod regulat (cel puțin o dată la șase luni) se vor efectua verificări pentru detectarea :
 - a) Parolelor utilizator care nu respectă regulamentele
 - b) Echipamentelor de rețea conectate neautorizat
 - c) Serviciilor de rețea neautorizate
 - d) Serverelor de pagini de web neautorizate
 - e) Echipamentelor ce utilizează resurse comune nesecurizate
 - f) Utilizării de modemuri neautorizate
 - g) Licențelor pentru sistemele de operare și programele instalate

Orice neregulă privind respectarea regulamentelor de securitate va fi raportată OSRIC sau OSRICD în scopul efectuării de investigații.

2.9. Securitatea Serverelor

Un server nu trebuie conectat la rețeaua Primăriei Câmpia Turzii 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 și a driver-lor care nu sunt necesare
- setarea/activarea parametrilor de securitate, a protecțiilor pentru fișiere și activarea jurnalelor de monitorizare
- dezactivarea sau schimbarea parolelor conturilor predefinite
- securizarea accesului fizic la aceste echipamente

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

2.10 Crearea și Utilizarea Copiilor de Siguranță (Backup)

1. Frecvența, dimensiunea și conținutul copiilor de siguranță trebuie să fie în concordanță cu importanța informației și cu riscul acceptat de proprietarul datelor.
2. Procedura de creare a copiilor de siguranță și de recuperare pentru fiecare sistem din cadrul RIC trebuie să fie documentată și periodic revizuită.
3. Verificarea copiilor de siguranță se va face după o procedură documentată și revizuită periodic.
4. Copiile de siguranță trebuie să fie periodic testate pentru a asigura faptul că informațiile stocate sunt recuperabile.
5. Accesul la mediile de backup ale Primăriei Câmpia Turzii se va face numai de personalul abilitat în acest sens.
6. Acestea trebuie revizuite periodic (anual).
7. Accesul trebuie interzis pentru persoanele autorizate care își schimbă locul de muncă.
8. Benzile sau mediile utilizate pentru stocarea copiilor de siguranță trebuie să aibă un sistem de identificare care să conțină cel puțin următoarele date de identificare a informației stocate:
 - numele sistemului;
 - data creării copiei;
 - tipul de copie (completă, incrementală etc.);
 - clasificarea sensibilității (siguranței/securității);
 - informații de contact.

2.11 Detectarea Tentativelor de Acces Neautorizat

1. Procesele de înregistrare și verificare a activității sistemelor de operare, conturilor utilizator și programelor trebuie să fie funcționale pe toate sistemele active (host, server, echipamente de rețea).
2. Trebuie activate funcțiile de anunțare a persoanelor responsabile oferite de firewall-uri și sistemele de control al accesului la rețea.
3. Trebuie activate funcțiile de înregistrare a evenimentelor pe dispozitivele firewall și pe toate sistemele de control al accesului.
4. Înregistrările de verificare ale dispozitivelor de control al accesului trebuie monitorizate/revizuite (examine) zilnic de către administratorul de sistem.
5. Verificările privind integritatea fiecărui sistem trebuie să se facă periodic. Această activitate este obligatorie și pentru dispozitivele de tip firewall sau dispozitive de control al accesului.
6. Înregistrările de verificare pentru serverele și host-urile din rețeaua internă trebuie revizuite cel puțin săptămânal.
7. Se vor verifica periodic (săptămânal) programele utilitare pentru detectarea tentativelor de acces neautorizat.
8. Toate rapoartele privind incidentele trebuie revizuite în vederea detectării de indicii ce ar putea implica o activitate de acces neautorizat.
9. Toate indiciile suspecte sau confirmate de accesări sau încercări de accesare neautorizate trebuie raportate imediat către OSRIC.
10. Utilizatorii sunt obligați să raporteze orice anomalii în performanța sistemelor utilizate cât și orice semne ale unor posibile infracțiuni la OSRIC sau OSRICD.

2.12 Utilizarea Calculatoarelor Portabile

- 1.OSRIC trebuie să aprobe, în scris, conectarea dispozitivelor portabile la RIC ale Instituției.
- 2.Calculatoarele portabile trebuie să fie protejate prin parole.
- 3.Se va evita stocarea datelor care privesc Primaria Câmpia Turzii pe dispozitivele portabile. În cazul în care nu există o altă alternativă de stocare locală, toate datele care privesc Primaria Câmpia Turzii trebuie criptate.
- 4.Conectarea sistemelor de calcul care nu sunt proprietatea Primăriei Câmpia Turzii se face numai cu aprobarea în scris a responsabilului IT la recomandarea Departamentelor.
- 5.Dispozitivele portabile de calcul neutilizate trebuie securizate fizic. Aceasta presupune încuierea lor într-un birou, într-un dulap.

2.13 Modificări și Modernizări ale Sistemului Resurselor Informatice și de Comunicații

- 1.Orice modificare asupra unei componente a RIC din cadrul Primăriei Câmpia Turzii, cum ar fi: sisteme de operare, componente hardware, echipamente și componente de rețea, aplicații, este supusă prezentului regulament și trebuie să urmeze procedurile în vigoare.
- 2.Responsabilul IT trebuie să fie anunțat de toate modificările care afectează mediul de funcționare a sistemelor componente ale RIC (ex: aparate de aer condiționat, instalații de apă, încălzire, instalații electrice și alarme, etc.).
- 3.Toate propunerile de modernizare și extindere a elementelor de infrastructură a sistemului RIC vor fi documentate și aprobate de către ARIC. Nu este permisă modificarea de către utilizatori a elementelor de infrastructură a RIC.
- 4.Modificările și modernizările sistemelor de calcul vor fi documentate de către utilizator și aprobate de către conducerea instituției.

2.14 Utilizare Internet și Intranet

1. Programele pentru acces la rețeaua Internet sunt destinate utilizatorilor autorizați pentru a fi folosite în scopuri exclusiv de serviciu, cu excepția situației prevăzute în regulamentul **Utilizarea ocazională a RIC în scopuri personale (cap.II subcap.2.2)**.
2. Toate programele utilizate pentru acces la rețeaua Internet trebuie să facă parte din pachetul de programe aprobat de către responsabilul IT. Aceste programe trebuie să includă toate patch-urile de securitate puse la dispoziție de către producător.
3. Toate fișierele care provin din rețeaua Internet trebuie să fie scanate cu un program antivirus care să fie actualizat cel puțin o dată la 24 ore.
4. Toate programele pentru acces Internet/Intranet trebuie să permită folosirea sistemelor proxy și/sau firewall.
5. Toate informațiile accesate în rețeaua Internet trebuie să se conformeze **Regulamentului de Utilizare Acceptabilă a RIC(cap.II subcap.2.1)**.
6. Orice activitate a utilizatorilor folosind RIC poate fi înregistrată și ulterior examinată.
7. Nu se vor publica pe sit-urile web ale Primăriei Câmpia Turzii materiale cu caracter ofensator sau de hărțuire.
8. Nu se vor publica pe site-urile web ale Primăriei Câmpia Turzii, materiale publicitare comerciale sau personale.
9. Nu se vor publica pe site-urile web ale Primăriei Câmpia Turzii date ale Primăriei Câmpia Turzii fără asigurarea că materialele sunt disponibile numai persoanelor sau grupurilor autorizate.
10. Nu este permisă utilizarea RIC ale Primăriei Câmpia Turzii în scop personal sau pentru solicitări personale ce nu au legătură cu Primaria Câmpia Turzii .

11. Cumpărăturile pe internet care nu au legătură cu atribuțiile de serviciu și sunt interzise. Cumpărăturile în interes de serviciu se vor supune regulilor de achiziție ale Primăriei Câmpia Turzii . Orice material confidențial al Primăriei Câmpia Turzii transmis prin rețeaua Internet trebuie criptat.

12. Fișierele electronice se supun acelorași reguli de păstrare ce se aplică și altor documente și trebuie păstrate în conformitate cu regulile stabilite prin prezentele regulamente și regulamentele proprii fiecărui Departament.

13. Este interzisă accesarea site-urilor cu caracter pornografic.

14. Este interzisă folosirea programelor peer-to-peer (exemple: Yahoo messenger, MSN, DC++, etc.)

15. Este interzisă descărcarea/instalarea programelor din rețeaua Internet

2.15. Administrarea Conturilor

Prin acord individual, fișa postului și/sau alte documente toți utilizatorii acceptă prevederile regulamentelor privind securitatea sistemului RIC.

Toți utilizatorii sunt obligați să păstreze confidențialitatea informațiilor privind contul de acces.

Toate parolele pentru conturi trebuie să fie create și folosite în conformitate cu **Regulamentul privind Parolele de Acces (cap.II subcap.2.16)**.

Conturile utilizator ale persoanelor plecate din Instituție 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 șterse dacă nu s-a solicitat accesul la acestea.

Administratorii de sisteme sau alt personal autorizat sunt responsabili de ștergerea conturilor persoanelor (utilizatorilor) care nu mai lucrează în Primăria Câmpia Turzii , sau care nu mai au relații cu Primăria Câmpia Turzii.

2.16 Parole de Acces

1. Toate parolele trebuie să îndeplinească următoarele condiții:

- Să fie schimbate de utilizator în mod regulat, cel puțin 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 angajaților care răspund de securitatea sistemelor informatice.

2. Dacă se suspectează că o parolă a putut fi divulgată aceasta trebuie schimbată imediat.

3. 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 excepții pentru anumite aplicații (precum backup automat) cu aprobarea OSRIC.

Dispozitivele de calcul nu trebuie lăsate nesupravegheate fără a activa un sistem de blocare a accesului la acestea; deblocarea trebuie să se facă folosind parolă.

Procedurile de schimbare a parolei asistate de administratorul de sistem trebuie să respecte următoarea procedură:

- Utilizatorul se va legitima, administratorul va verifica drepturile de acces a persoanei la contul utilizator;
- Se va genera o parolă care va fi comunicată utilizatorului

OSRIC va avea o evidență cu toți utilizatorii sistemului RIC precum și cu parolele pe care le dețin.

2.17 Sistemul de Mesagerie Electronică

Următoarele activități sunt interzise de regulament:

1. Trimiterea de mesaje cu caracter de intimidare sau hărțuire;
2. Folosirea sistemului de mesagerie electronică în scopuri personale;
3. Folosirea sistemului de mesagerie electronică în scopuri politice sau pentru campanii politice;
4. Încălcarea drepturilor de autor prin distribuirea neautorizată a materialelor protejate;
5. Folosirea altei identități decât cea reală atunci când se trimite email, exceptând cazurile când persoana este autorizată în scop de suport administrativ.
6. Folosirea programelor de poștă electronică neautorizate.
7. Următoarele activități sunt interzise deoarece împiedică buna funcționare a comunicațiilor în rețea și eficiența sistemelor de mesagerie electronică:
8. Trimiterea sau retrimiteră email-urilor în lanț;
9. Trimiterea mesajelor nesolicitate către grupuri de persoane, exceptând cazurile în care aceste mesaje deserveșc instituția.
10. Trimiterea mesajelor de dimensiuni foarte mari;
11. Trimiterea sau retrimiteră mesajelor ce pot conține viruși.
12. Toate informațiile și datele confidențiale ale Primăriei Cămpia Turzii, transmise către alte rețele externe, trebuie să fie criptate.
13. Toate activitățile utilizatorilor ce implică accesul și/sau folosirea RIC ale Primăriei Cămpia Turzii pot fi oricând înregistrate și analizate.
14. Utilizatorii serviciilor de mesagerie electronică nu trebuie să dea impresia că reprezintă, că își spun opinia sau dau declarații în numele Primăriei Cămpia Turzii, cu excepția situațiilor în care aceștia sunt autorizați în mod corespunzător (implicit sau explicit) să facă acest lucru. Atunci când este cazul, se va include o declarație explicită prin care utilizatorul specifică faptul că nu reprezintă Primăria Cămpia Turzii. Un exemplu de declarație simplă este: "părerile exprimate sunt personale, și nu ale Primăriei Cămpia Turzii" sau "aceasta este o opinie personală și nu reprezintă în mod necesar poziția oficială a Primăriei Cămpia Turzii".
15. Utilizatorii nu trebuie să trimită, retrimită sau să primească informații confidențiale sau senzitive ce privesc Primăria Cămpia Turzii, folosind conturi utilizator care nu sunt proprietatea Primăriei Cămpia Turzii. Exemple de astfel de conturi, sunt (dar nu sunt limitate numai la acestea: Hotmail, Yahoo mail, AOL mail), precum și adrese de email puse la dispoziție de alți Furnizorii de Servicii Internet.
16. Utilizatorii nu trebuie să trimită, retrimită, primească sau să stocheze informații confidențiale sau nesigure, ce privesc Primăria Cămpia Turzii, folosind dispozitive de comunicații mobile care nu sunt autorizate de Primăria Cămpia Turzii. Exemple de astfel de dispozitive (dar nu sunt limitate numai la acestea) sunt: asistenți digitali personali, tablete, telefoanele mobile.

2.18 Detectarea virușilor

1. Toate stațiile de lucru de sine stătătoare sau conectate la rețeaua de comunicații a Primăriei Cămpia Turzii, trebuie să utilizeze programe antivirus aprobate de către OSRIC.
2. Programele antivirus nu trebuie dezactivate.
3. Configurația programului antivirus trebuie să nu fie modificată într-un mod care să reducă eficacitatea programului.
4. Frecvența actualizărilor automate a programului antivirus trebuie asigurată de către utilizator.
5. Orice server de fișiere conectat la rețeaua Instituției trebuie să utilizeze un program antivirus aprobat în scopul detectării și curățirii virușilor care pot infecta fișierele puse la dispoziție.
6. Orice server sau gateway pentru e-mail trebuie să folosească un program antivirus pentru e-mail aprobat și trebuie să respecte regulile de instalare și utilizare a acestui program.

7. Orice virus care nu a putut fi înlăturat automat de către programul antivirus constituie un incident de securitate și trebuie raportat imediat OSRIC sau OSRICD.

2.19 Licențe de utilizare

1. Primaria Câmpia Turzii furnizează un număr suficient de copii cu Licență pentru toate programele aprobate spre utilizare astfel încât angajații să își poată desfășura munca într-un mod eficient și rapid.

2. Primaria Câmpia Turzii trebuie să se pună de acord în mod adecvat cu furnizorii implicați pentru obținerea de copii adiționale ale licențelor dacă și când acestea sunt necesare în activitatea instituției.

3. Copiile suplimentare ale materialelor protejate prin drepturi de autor nu vor fi stocate pe sistemele sau resursele rețelei Primăriei Câmpia Turzii în situația în care nu există aprobări specifice. Administratorii de sistem vor șterge produsele și toate materialele protejate prin drepturi de autor în situația menționată, cu excepția cazului în care utilizatorii implicați fac dovada autorizației de folosire sau stocare de la producătorii de drept.

4. Programele sau alte bunuri informatice aflate sub incidența drepturilor de autor aflate în posesia Primăriei Câmpia Turzii nu vor fi copiate, cu excepția cazului în care această copiere este în concordanță cu prevederile licenței.

2.20 Relații cu terți

Orice activitate desfășurată de furnizor care implică acces la RIC trebuie să se conformeze cu regulamentele în vigoare ale Primăriei Câmpia Turzii.

În toate convențiile și contractele încheiate cu Furnizori trebuie specificate următoarele:

- Informațiile din cadrul Primăriei Câmpia Turzii, la care Furnizorul are drept de acces;
- Modul în care informațiile la care Furnizorul are drept de acces urmează a fi protejate de către acesta precum și măsuri ce vor fi luate în cazul nerespectării clauzelor;
- Metodele de predare, distrugere sau de transfer al drepturilor informațiilor Instituției aflate în posesia Furnizorului, la încheierea contractului.
- Furnizorul trebuie să folosească sistemul RIC din cadrul Primăriei Câmpia Turzii numai în scopul stipulat în contract.
- Orice altă informație din sistemul RIC al Primăriei Câmpia Turzii obținută de Furnizor pe durata contractului nu poate fi folosită în interes propriu de către Furnizor sau divulgată altora.
- Toate echipamentele de întreținere ale Furnizorului, aflate în rețeaua internă a Primăriei Câmpia Turzii și care se pot conecta în exterior prin intermediul rețelei, a liniilor telefonice sau a liniilor închiriate, precum și toate conturile de utilizator create temporar pentru Furnizor și necesare pentru acces la RIC ale Primăriei Câmpia Turzii, vor fi scoase din uz la încheierea relațiilor 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** (cap.II subcap.2.16) și **Regulamentul de Acces Administrativ** (cap.II subcap.2.3).
- Activitățile principale ale Furnizorului trebuie să fie documentate de acesta și puse la dispoziția conducerii Instituției, 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 și de livrare.
- În cazul retragerii din contract a unui angajat al Furnizorului, indiferent de motiv, Furnizorul se va asigura că toate informațiile sensibile sunt colectate și predate Primăriei Câmpia Turzii sau distruse în cel mult 24 de ore de la producerea evenimentului.

- În cazul terminării/rezilierii contractului sau la cererea Primăriei Câmpia Turzii , Furnizorul va preda sau distruge toate informațiile ce aparțin Instituției și va oferi certificare în scris privind predarea sau distrugerea informațiilor în decurs de 24 de ore de la producerea evenimentului.
- În cazul încheierii contractului sau la cererea Primăriei Câmpia Turzii, Furnizorul trebuie să predea imediat toate legitimațiile, cartelele de acces, echipamentele și stocurile Primăriei Câmpia Turzii . Echipamentele și/sau stocurile care urmează a fi reținute de către Furnizor trebuiesc documentate și autorizate de Conducerea Primăriei Câmpia Turzii.
- Toate programele folosite de Furnizor în scopul furnizării serviciilor stipulate în contract către Primăria Câmpia Turzii trebuie să fie inventariate corespunzător și să posede drepturi de utilizare atestate prin Licențe.

Șef serviciu
Serviciul Resurse Umane Salarizare
Camelia Mădălina Marinca

Redactat
Adrian-Sandu NICOARĂ consilier SRUS