ANEXA

LA DISPOZIŢIA NR.

156/21 MAI 2021

Aprobat,

Primar,

Ciprian George BARBU

Politica de securitate IT a Primăriei oraşului Azuga

I. Introducere

Politica de securitate a sistemului IT este responsabilitatea conducerii Primăriei oraşului Azuga şi este elaborată împreună cu Inspectorul de specialitate din Compartimentul de Informatică. Securitatea sistemului IT este în responsabilitatea Compartimentului Informatică al Primăriei oraşului Azuga, împreună cu toţi utilizatorii de resurse IT ale instituţiei.

În vederea stabilirii şi menţinerii politicii de securitate este esenţială implicarea tuturor structurilor de conducere din instituţie alături de tot personalul implicat in folosirea Resurselor IT (RIT) pentru adoptarea deciziilor privind securitatea sistemului informatic.

Accesul la echipamentele de prelucrare a informaţiilor primăriei de către terţe părţi trebuie să se facă sub supraveghere. Pentru accesul terţilor, o evaluare a riscului ar trebui să fie efectuată pentru a stabili implicaţiile de securitate şi cerinţele de control. Măsurile de protecţie trebuie să fie puse de acord şi incluse într-un contract cu terţele părţi. De asemenea în acordurile/contractele de externalizare ar trebui să se abordeze riscurile, controalele şi procedurile de securitate pentru sistemele informatice, reţelele şi/sau echipamentele de birou.

II. Scop

Securitatea informatică asigură cunoaşterea, prevenirea şi contracararea unui atac împotriva spaţiului cibernetic, inclusiv managementul consecinţelor.

- **Cunoaşterea** trebuie să asigure informaţiile necesare în elaborarea măsurilor pentru prevenirea efectelor unor incidente informatice.
- **Prevenirea** este principalul mijloc de asigurare a securităţii informatice. Acţiunile preventive reprezintă cea mai eficientă modalitate atât de a reduce extinderea mijloacelor specifice ale unui atac cibernetic, cât şi de a limita efectele utilizării acestora.

- **Contracararea** trebuie să asigure o reacţie eficientă la atacuri cibernetice, prin identificarea şi blocarea acţiunilor ostile în spaţiul cibernetic, menţinerea sau restabilirea disponibilităţii infrastructurilor cibernetice vizate şi identificarea şi sancţionarea potrivit legii, a autorilor.

Politica de securitate IT are ca **scop** asigurarea confidenţialităţii, integrităţii şi disponibilităţii informaţiei.

- **Confidenţialitatea** se referă la protecţia datelor împotriva accesului neautorizat. Fişierele electronice create, trimise, primite sau stocate folosind sistemul RIT proprii, administrate sau în custodia şi sub controlul Primăriei oraşului Azuga sunt confidenţiale şi pot fi accesate de către functionarii publici sau angajaţii autorizaţi din cadrul Primăriei oraşului Azuga numai în condiţiile prevăzute de lege.

- **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 RIT.

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

III. Definiţii

- **Resurse IT (RIT)**: toate dispozitivele de tipărire, 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: servere, calculatoare personale (PC) (desktop, laptop), tablete, medii de reţea si echipamente de acces la Internet. La acestea se adaugă procedurile, echipamentul, facilităţile, programele şi datele care sunt proiectate, construite, puse în funcţiune (operaţionale) şi menţinute pentru a crea, colecta, înregistra, procesa, stoca, primi, afişa şi transmite informaţia.
- **Administratorul de reţea este şi Administratorul Resurselor IT (ARIT)**: Responsabilul la nivelul instituţiei cu administrarea RIT ale Primariei oraşului Azuga.
- **Utilizator**: o persoană, o aplicaţie automatizată sau proces utilizator autorizate de către Primaria oraşului Azuga, în conformitate cu procedurile şi regulamentele în vigoare, să folosească RIT.
- **Abuz de privilegii**: orice acţiune întreprinsă în mod voit de un utilizator, care vine în contradicţie cu regulamentele Primăriei oraşului Azuga 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 sau servicii Primăriei oraşului Azuga în baza unui contract comercial sau de colaborare.

IV. Clasificarea Informaţiilor

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

Pentru a asigura securitatea şi integritatea informaţiilor, acestea se împart în trei categorii principale:

- Publice
- Secrete
- Strict Secrete

Conducătorii Serviciilor/Birourilor/Compartimentelor din Primaria oraşului Azuga răspund de evaluarea periodică a schemei de clasificare a informaţiilor. Toate informaţiile din instituţie trebuie să se regăsească în una din următoarele categorii:

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

Exemple: informaţiile de pe aviziere, pagina proprie de internet, informările publice ale Primăriei, ale Consiliului Judetean sau Prefecturii.

2. Secrete: În această categorie se includ informaţiile care datorită valorii economice nu trebuie făcute publice. Se includ aici şi informaţiile pe care Primaria oraşului Azuga trebuie să le protejeze conform legislaţiei în vigoare. Datorită valorii economice asociate, aceste date trebuie distruse dacă au fost făcute publice. Aceste date vor fi copiate şi distribuite în cadrul Primăriei oraşului Azuga doar utilizatorilor autorizaţi.

Distribuirea acestor informaţii de către utilizatorii autorizaţi trebuie să se facă pe baza unei clauze de confidenţialitate.

Exemple: clauze contractuale in relaţia cu agenţii economici, conturi si parole de utilizator folosite de agenţii economici sau alte instituţii pe serverele care contin date din instituţie (Datele de personal, Impozitele si Taxele, Datele contabile, Registrul Agricol, ș.a).

3. Strict Secrete sau Confidenţiale: În această categorie se includ toate informaţiile care nu trebuie făcute publice. Divulgarea, utilizarea sau distrugerea acestor date poate intra sub incidenţa Codului Civil, Penal sau legislaţiei fiscale. Accesul la aceste informaţii va fi restricţionat. Datele strict secrete nu pot fi copiate, distribuite sau şterse fără acordul scris al conducerii primăriei.

Exemple: cheile criptografice, conturi administrative de pe serverele de reţea din institutie sau alte servere de aplicaţii din reţeaua internet (REGISTA, ANFP, ANAF, SEAP, FOREXEBUG,

ESOP, etc), datele personale de pe serverele Serviciului Public Comunitar Local de Evidenţa Persoanelor, s.a.

V. Politica de securitate IT interzice:

- scoaterea informaţiei sau echipamentelor din instituţie fara autorizaţie;
- utilizarea neautorizată a informaţiei, infrastructurii sau echipamentelor;
- copierea neautorizată a informaţiei;
- compromiterea parolelor;
- descarcarea unor materiale ilegale;
- utilizarea informaţiilor si sistemelor de calcul pentru scopuri care nu au legatură cu activitatea desfaşurată.

VI. Atribuţii şi Responsabilităţi

Atribuţiile administratorilor includ:

- Administratorii de reţea/sistem/baze de date trebuie să asigure activarea tuturor mecanismelor de securitate;
- Administratorii de reţea/sistem/baze de date elaborează şi propun modificări ale politicii de securitate IT;
- Administratorii de reţea/sistem/baze de date tratează incidentele de securitate în scopul minimizării efectului distructiv al acestora asupra RIT.

Atribuţii ale utilizatorilor:

- Să cunoască şi să respecte prevederile Politicii de securitate IT a instituţiei;
- Să inchidă aplicaţiile sau documentaţia importantă când nu sunt utilizate;
- Să iasă din sistem atunci când un calculator urmează să fie lăsat nesupravegheat, fie şi pentru o scurtă pauză;
- Să cunoască şi să respecte prevederile tuturor regulamentelor şi/sau procedurilor privind securitatea IT;
- Să răspundă direct de securitatea şi conţinutul informaţiilor şi de RIT încredinţate direct sau indirect.

Alte atribuţii:

- Toţi partenerii Primăriei oraşului Azuga (furnizori, agenţi, colaboratori, etc.) trebuie să accepte şi să respecte prezentul regulament.

VII. Măsuri Disciplinare

Încălcarea Politicii de securitate IT se sancţionează prin măsuri disciplinare care pot include:

- În cazul funcţionarilor publici/angajaţilor, se va proceda la suspendarea accesului la resurse, respectiv la alte măsuri disciplinare conform legislaţiei in vigoare;
- Încetarea relaţiilor contractuale în cazul furnizorilor, consultanţilor sau colaboratorilor;
- Suspendarea accesului la resurse în cazul altor utilizatori;
- Interzicerea accesului la RIT.

Toate acţiunile care contravin legilor vor fi raportate organelor competente.

VIII. Alte Dispoziţii

1. Întreg personalul este responsabil privind modul de utilizare a RIT; fiecare utilizator este direct responsabil pentru acţiunile care pot afecta securitatea IT.

2. Utilizatorii sunt responsabili nediscriminatoriu privind raportarea oricărei suspiciuni sau confirmări de încălcare a acestui regulament.

3. Nu există nici o asigurare a confidenţialităţii datelor personale sau a accesului la informaţii folosind protocoale de genul, dar nu numai, mesagerie electronică, navigare Web şi alte instrumente de conversaţie electronică. Utilizarea acestor instrumente de comunicaţie electronică poate fi monitorizată în scopul unor investigaţii sau al rezolvării unor plângeri în condiţiile legilor în vigoare.

4. Serviciile/Birourile/Compartimentele sunt responsabile de autorizarea utilizatorilor pentru folosirea adecvată a RIT.

5. Orice informaţie folosită în sistemul RIT trebuie să fie păstrată confidenţială şi în siguranţă de către utilizator. Faptul că informaţiile pot fi stocate electronic nu schimbă cu nimic obligativitatea de a le păstra confidenţiale şi în siguranţă, tipul informaţiei sau chiar informaţia în sine stau la baza determinării gradului de siguranţă necesar.

6. Toate programele de calculator, aplicaţiile, codul sursă, codul obiect, documentaţia şi datele trebuie protejate.

7. Serviciile/Birourile/Compartimentele trebuie să ofere facilităţi corespunzătoare de control al accesului în scopul monitorizării RIT, protejării datelor şi programelor împotriva întrebuinţării greşite, în concordanţă cu necesităţile stabilite de acestea. Accesul trebuie să fie documentat, autorizat şi controlat în mod corespunzător.

8. Orice program comercial utilizat în cadrul RIT trebuie să fie însoţit de Licenţă care să specifice clar drepturile de utilizare şi restricţiile produsului. Personalul trebuie să respecte prevederile Licenţelor si nu este permisă copierea ilegală a programelor comerciale. Compartimentul Informatică, îşi rezervă dreptul de a şterge orice produs fără Licenţă de pe orice sistem din cadrul RIT.

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

10. RIT ale Primăriei oraşului Azuga se folosesc doar in interes de serviciu, nu trebuie folosite in mod abuziv pentru beneficiul personal. Angajaţii nu trebuie să permită membrilor familiei sau altor persoane din afara instituţiei accesul la RIT ale Primariei oraşului Azuga.

IX. Dispoziţii Finale

1. Politica de securitate IT a Primăriei oraşului Azuga impune dezvoltarea, gestionarea şi punerea în practică de proceduri şi/sau regulamente specifice.

2. Compartimentul Informatică are obligaţia de a revizui periodic prezenta Politică de securitate IT a instituţiei.

3. În fişele posturilor utilizatorilor şi în contractele cu terţi care implică accesul la RIT ale primăriei, se vor introduce obligatoriu referiri la Politica de securitate IT.

4. Pentru a ne asigura că utilizatorii sunt conştienţi de ameninţările de securitate a informaţiilor şi sunt pregătiţi pentru a sprijini Politica de securitate IT a primăriei în cursul activităţii lor la locul de muncă, îşi vor însuşi noţiunile cu privire la securitatea şi utilizarea corectă a sistemelor de prelucrare a informaţiilor.