GRĂDINIŢA CU PROGRAM PRELUNGIT „MIHAI EMINESCU"
STR. OLARI, NR. 3, COD 210258, TG-JIU, GORJ
COD FISCAL: 29448992
TEL./FAX: 0353 801417
E-mail: gr_eminescu_gj@yahoo.com

REGULAMENT

PRIVIND POLITICA DE SECURITATE IT AL GRĂDINIŢEI CU PROGRAM PRELUNGIT „MIHAI EMINESCU" TG-JIU

AVIZUL CONSILIULUI DE ADMINISTRAŢIE,
APROBAT ÎN CONSILIUL DE ADMINISTRAŢIE ÎN DATA 31.01.2017

DIRECTOR,
PROF. ANA-MARIA BÎZDOACĂ

AVIZUL CONSILIULUI PROFESORAL,
DEZBĂTUT ŞI AVIZAT ÎN ŞEDINŢA CONSILIULUI PROFESORAL ÎN DATA DE: **27.01.2017**

CAPITOLUL I
DISPOZIŢII GENERALE

Art.1 În acord cu prevederile prezentului regulament, Resursele Informatice şi de Comunicaţii puse la dispozitie şi administrate de către instituţia de învăţământ sunt bunuri strategice ale grădiniţei.
Art.2 Documentele interne de reglementare a utilizării Resurselor Informatice şi de Comunicaţii sunt elaborate pentru a stabili un cadru corect, legal şi eficient de utilizare a tehnologiei informaţiei şi comunicaţiilor în Grădiniţa cu Program Prelungit „Mihai Eminescu" Tg-Jiu.
Art.3 Acestea au ca scop principal protejarea utilizatorilor, colaboratorilor împotriva atacurilor de orice tip (cu sau fără intenţie). De asemenea, acestea vizează protejarea imaginii grădiniţei şi a investiţiilor acesteia pentru dezvoltarea sistemul informatic şi de comunicaţi.
Art.4 Reţeaua informatică a grădiniţei sprijină procesul de învăţământ şi de cercetare prin mijloacele de comunicare şi serviciile specifice oferite de reţelele de calculatoare.
Art.5 Compromiterea securităţii acestor resurse poate afecta capacitatea grădiniţei de a oferi servicii informatice şi de comunicaţii, poate conduce la fraude sau distrugerea datelor, la violarea clauzelor contractuale, divulgarea secretelor, la afectarea credibilităţii instituţiei în faţa partenerilor săi. Prin urmare, prezentul regulament este motivat tehnic de necesitatea menţinerii în funcţiune, în condiţii de securitate, a reţelei, precum şi de necesitatea dezvoltării normale a unei resurse de informare.
Art.5 Scopul urmărit de politica de securitate este acela de asigurare a integrităţii, confidenţialităţii şi disponibilităţii informaţiei, precum şi stabilirea cadrului necesar pentru elaborarea regulilor şi procedurilor de securitate.
(1) *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 grădiniţei sunt proprietatea acesteia în condiţiile legilor în vigoare. Utilizatorul răspunde personal de confidenţialitatea datelor încredinţate prin procedurile de acces la Resursele Informatice şi de Comunicaţii.
(2) *Integritatea* se referă la măsurile şi procedurile utilizate pentru protecţia datelor împotriva modificărilor sau distrugerii neautorizate.
(3) *Disponibilitatea* se asigură prin funcţionarea continuă a tuturor componentelor Resurselor Informatice şi de Comunicaţii. Diverse aplicaţii au nevoie de nivele diferite de disponibilitate în funcţie de impactul sau daunele produse ca urmare a nefuncţionării corespunzătoare a Resurselor Informatice şi de Comunicaţii.
Art.6 Cel puţin o oră de consiliere pe semestru va fi rezervată pentru abordarea subiectului siguranţei în mediul online. Pentru ca părinţii să devină conştienţi de posibilele riscuri şi incidente. De asemenea, planificarea pentru orele de consiliere şi orientare va include şi învăţarea despre comunicarea eficientă şi responsabilă, deoarece aceasta este o competenţă necesară fiecărui copil.
Art.7 Personalul grădiniţei va promova politica de securitate în rândul preşcolarilor şi al părinţilor, prin intermediul unor sesiuni de informare în cadrul cărora vor fi utilizate resurse diverse. Astfel, preşcolarii şi părinţii vor fi ajutaţi să dezvolte o atitudine responsabilă referitoare la siguranţa online, utilizarea sistemului şi conţinutul pe care îl accesează sau îl creează. De asemenea, se ia în considerare furnizarea de informaţii pentru părinţi prin intermediul site-ului grădiniţei.
Art.8 Dispozitivele mobile personale vor fi utilizate în sala de grupă de către cadrele didactice, numai în scopuri educative, astfel încât procesul instructiv-educativ să nu fie perturbat. Utilizarea dispozitivelor în alte scopuri decât cele educative este considerată abatere comportamentală şi se va pedepsi conform prevederilor din Regulamentul de ordine interioară al grădiniţei.
Art.9 Orice imagini sau clipuri video ale copiilor vor fi folosite numai în concordanţă cu politica grădiniţei de utilizarea a imaginii (Acord de folosire a imaginii copilului în/de către grădiniţă) şi se va lua întotdeauna în considerare consimţământul părinţilor.

Art.10 Personalul grădiniţei va respecta drepturile de proprietate intelectuală şi drepturile de autor.
Art.11 Toate incidentele îngrijorătoare cu privire la siguranţa online a copiilor vor fi raportate coordonatorului desemnat pentru protecţia copilului şi/sau administratorului, cât mai curând posibil. De asemenea, se va raporta orice acces accidental, primirea de materiale nepotrivite, breşe de securitate sau site-uri nepotrivite către persoana responsabilă cu filtrarea conţinutului, cât mai curând posibil.
Art.12 Datele cu caracter personal ale preşcolarilor, personalului sau părinţilor/tutorilor sunt păstrate în conformitate cu Legea nr. 677/2001 pentru protecţia persoanelor cu privire la prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date. Aceasta înseamnă că toate datele cu caracter personal vor fi obţinute şi prelucrate în mod corect şi legal şi vor fi păstrate în confidenţialitate şi siguranţă, prin intermediul unor măsuri de securitate adecvate, fie că sunt utilizate la locul de muncă, stocate online (numai în ţări sau pe site-uri cu metode adecvate de control al protecţiei datelor) sau accesate de la distanţă. Orice date preluate de pe site-ul grădiniţei (cum ar fi prin e-mail sau pe memory stick-uri sau CD-uri) vor fi criptate printr-o metodă aprobată de către instituţie.

CAPITOLUL II
DOCUMENTE DE REFERINŢĂ

Art.13 Legislaţie primară
(1) Orice activitate care se desfăşoară prin intermediul reţelei trebuie să respecte legislaţia în vigoare (internă şi internaţională):
a. Legea nr. 8/1996 privind dreptul de autor şi drepturile conexe;
b. H.G. nr. 58/1998 –pentru aprobarea Strategiei naţionale de informatizare şi implementare în ritm accelerat a societăţii informaţionale şi a Programului de acţiuni privind utilizarea pe scară largă şi dezvoltarea sectorului tehnologiilor informaţiei în România;
c. Ordonanţa de Guvern nr. 124/200 pentru completarea cadrului juridic privind dreptul de autor şi drepturile conexe, prin adoptarea de măsuri pentru combaterea pirateriei în domeniile audio şi video, precum şi a programelor pentru calculator;
d. Legea nr. 544/2001 privind liberul acces la informaţiile de interes public;
e. Legea nr. 677/2001 pentru protecţia persoanelor cu privire la prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date;
f. H.G. nr. 1609/2008, privind organizarea şi funcţionarea Agenţiei ARNIEC/RoEduNet;
g. Convenţia privind Criminalitatea Informatică a Consiliului Europei;
h. Declaraţia privind libertatea comunicării pe Internet a Consiliului Europei.
(2) Legislaţia primară va fi actualizată cu modificările şi completările ulterioare, dar şi cu alte acte normative relevante în domeniul securităţii informatice.
Art.14 Reglementări interne
(1) Regulamentele şi procedurile în vigoare în cadrul Grădiniţei cu Program Prelungit „Mihai Eminescu" Tg-Jiu.

CAPITOLUL III
DEFINIŢII

Art.15 *Intranet* = reţeaua internă de calculatoare.
Art.16 *Cont* = o entitate specificată printr-un identificator şi/sau parolă pentru accesul la sistemul de comunicaţie şi/sau la o resursă de calcul.
Art.17 *Resurse IT* = 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: mainframeuri, servere, calculatoare personale, calculatoare-agendă (*notebookuri*, *laptop*-uri), calculatoare de buzunar, asistent digital personal (*Personal Digital Assistant* - PDA), 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 crea, colecta, înregistra, procesa, stoca, primi, afişa şi transmite informaţia.
Art.18 *Administratorul de reţea este şi Administratorul Resurselor Informatice si de Comunicare* = persoana responsabilă la nivelul instituţiei cu administrarea Resurselor IT.
Art.19 *Utilizator* = o persoană, o aplicaţie automatizată sau process utilizator autorizat de către, în conformitate cu procedurile şi regulamentele în vigoare, să folosească Resursele IT.
Art.20 *Abuz de privilegii* = orice acţiune întreprinsă în mod voit de un utilizator, care vine în contradicţie cu regulamentele grădiniţei 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.
Art.21 *Furnizor*: Persoană fizică/juridică care oferă bunuri sau servicii instituţiei în baza unui contract comercial sau de colaborare.
Art.22 (1) *Sistemele de Informaţii şi TIC* includ reţele, date şi stocare de date, tehnologii de comunicare online şi offline şi dispozitive de acces. Exemplele includ telefoane mobile, PDA-uri, camere digitale, e-mail şi site-uri de socializare.
(2) Sistemele de informare deţinute de instituţii de învăţământ trebuie să fie utilizate în mod corespunzător. Sunt considerate infracţiuni care pot să contravină legislaţiei în vigoare: obţinerea accesului neautorizat la date informatice; obţinerea accesului neautorizat la date informatice cu intenţia de a comite sau facilita comiterea altor infracţiuni sau de a modifica datele informatice fără autorizare.

CAPITOLUL IV
POLITICA DE SECURITATE

Art.23 Politica de securitate este alcătuită astfel încât să fie în conformitate cu statutul, regulamentele, legile şi alte documente oficiale în vigoare privind administrarea resurselor informatice publice, să stabilească practici prudente şi acceptabile privind utilizarea Resurselor Informatice şi de Comunicaţii ale grădiniţei şi să instruiască utilizatorii care au dreptul de folosire a Resurselor Informatice şi de Comunicaţii privind responsabilităţile asociate unei astfel de utilizări.
Art.24 Clasificarea informaţiilor din punct de vedere al securităţii şi integrităţii informaţiilor:
(1) Informaţii Publice - acestea sunt informaţii accesibile oricărui utilizator din interiorul sau exteriorul grădiniţei. Exemplu de astfel de date sunt cele de la avizier, pe site-urile Web, sau informaţiile de presă.
(2) Informaţii Secrete - aceste informaţii includ date care dacă sunt făcute publice aduc daune economice sau de imagine grădiniţei. Astfel de date pot fi: clauze contractuale, informaţii obţinute prin participare la licitaţii, conturi sau parole etc. Aceste date trebuie protejate prin clauze de confidenţialitate.
(3) Informaţii Strict Secrete - în acestă categorie intră date ce nu pot fi copiate, distribuite sau şterse fără acordul scris al conducerii gădiniţei şi care ar aduce mari prejudiii în caz de compromitere. Ex: parole la servere importante, date examene de admitere, rezidenţiat, chei de criptare etc.
Art.25 Politica de securitate a resurselor IT în Grădiniţa cu Program Prelungit „Mihai Eminescu" Tg-Jiu se aplică nediscriminatoriu tuturor persoanelor cărora li s-a permis accesul la orice resursă informatică şi de comunicaţii a instituţiei.
Art.26 Următoarele entităţi şi utilizatori sunt vizaţi în mod distinct de prevederile politicii:
(1) Angajaţii cu contract de muncă pe perioadă determinată sau nedeterminată care au acces la sistemul informaţional şi de comunicaţi.
(2) Colaboratorii grădiniţei care au acces la resursele IT.
(3) Furnizorii grădiniţei care au acces la resursele IT.
(4) Alte persoane, entităţi sau organizaţii care au acces la resursele IT.

CAPITOLUL V
ATRIBUŢII SI OBLIGAŢII

Art.27 Administratorii reţelei au următoarele atribuţii cu privire la politicile de securitate:
(1) Elaborează şi propune modificări ale politicii de securitate.
(2) Elaborează şi propune pentru aprobare regulamentele şi procedurile de securitate.
(3) Tratarea incidentelor de securitate.
(4) Elaborează proceduri pentru identificarea utilizatorilor.
Art.28 Atribuţiile utilizatorilor sunt:
(1) Să cunoască şi să respecte prevederile politicii de securitate,
(2) Să cunoască şi să respecte prevederile regulamentelor şi procedurilor de securitate.
(3) Să răspundă direct de securitatea şi conţinutul informaţiilor şi resursele informatice şi de comunicaţii încredinţate direct sau indirect.
Art.29 Toţi partenerii grădiniţei trebuie să accepte şi să respecte aceste politici de securitate.

CAPITOLUL VI
CONFIDENŢIALITATEA INFORMAŢIILOR

Art.30 Fiecare utilizator este responsabil în mod direct de modul de utilizare a resurselor grădiniţei.
Art.31 Nu există nicio asigurare a confidenţialităţii datelor personale sau a accesului la informaţii, mesagerie electronică, navigare Web, conversaţii telefonice, acces la reţelele Wireless, transmisie fax-uri 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.
Art.32 Modul de acces la resursele grădiniţei trebuie reglementat şi monitorizat împotriva întrebuinţării greşite sau rău voite.
Art.33 Orice sistem din proprietatea grădiniţei trebuie sa fie însoţit de fişa sistemului de calcul care coţine licenţele şi aplicaţiile ce pot fi folosite.
Art.34 Toate programele de calculator, aplicaţiile, codul sursă, codul obiect, documentaţia şi datele sunt proprietatea grădiniţei şi trebuie să fie protejate.
Art.35 Administratorii îşi rezervă dreptul de a şterge, de pe orice sistem orice program sau fişier ce nu are legătura cu scopul muncii respective, sau contravine politicilor grădiniţei. De asemena se poate suspenda functionarea oricărui echipament care poate afecta funcţioanarea sistemelor din cadrul grădiniţei.
Art.36 Personalul autorizat poate revizui sau utiliza orice informaţie stocată pe sau transportată prin sistemele grădiniţei în conformitate cu legile în vigoare. În aceleaşi scopuri, este posibilă monitorizarea activităţii utilizatorilor (de exemplu, dar fără a se limita la, numere de telefon formate sau sit-uri web vizitate).
Art.37 Utilizatorii trebuie să raporteze orice slăbiciune în sistemul de securitate al calculatoarelor din cadrul grădiniţei, orice incident de posibilă întrebuinţare greşită sau încălcare a acestui regulament.
Art.38 Utilizatorii nu trebuie să încerce să acceseze informaţii sau programe de pe sistemele grădiniţei pentru care nu au autorizaţie sau consimţământ explicit.
Art.39 Niciun utilizator al sistemelor din grădiniţei nu poate divulga informaţiile la care are acces sau la care a avut acces ca urmare a unei vulnerabilităţi a sistemului. Această regulă se extinde şi după ce utilizatorul a încheiat relaţiile cu grădiniţa.
Art.40 Informaţiile publicate electronic de către grădiniţei pe site-ul propriu şi în subdomeniile acestuia sunt proprietate a grădiniţei. Caracterul public al acestora reflectă faptul că ele sunt puse la dispoziţie de către grădiniţă în beneficiul comunităţii publice, în scop de informare asupra programelor educative şi a activităţii grădiniţei.
Art.41 Orice utilizare a informaţiilor de pe site în domeniul *gradinitamihaieminescu.ro* de către persoane particulare sau organizaţii în alte scopuri decât cele în care au fost oferite, se face pe propria răspundere a acestora. Într-o asemenea eventualitate, grădiniţa îşi rezervă dreptul de a solicita aplicarea prevederilor legale în vigoare.

Art.42 Fişierele electronice create, trimise, primite sau stocate folosind Resursele Informatice şi de Comunicaţii administrate sau în custodia şi sub controlul grădiniţei nu au caracter personal şi pot fi accesate oricând de către angajaţii autorizaţi fără înştiinţarea utilizatorului.

CAPITOLUL VII
PLANUL DE SECURITATE

Art.43 Politica de securitate a grădiniţei impune dezvoltarea, gestionarea şi punerea în practică de proceduri şi/sau reguli specifice care să asigure integritatea, confidenţialitatea şi disponibilitatea informaţiei în utilizarea RIC.
Art.44 Planul de securitate conţine toate regulile şi procedurile aplicabile în sistemul Resurselor Informatice şi de Comunicaţii ale grădiniţei.
Art.45 Planul de securitate are ca scop principal protejarea utilizatorilor şi colaboratorilor împotriva atacurilor de orice tip (cu sau fără intenţie). De asemenea, acesta are ca scop protejarea imaginii grădiniţei şi a investiţiilor acesteia pentru dezvoltarea sistemului informatic şi de comunicaţii, protejarea proprietăţii intelectuale şi a tuturor informaţiilor stocate şi transportate cu ajutorul Resurselor Informatice şi de Comunicaţii ale utilizatorilor autorizaţi: cadre didactice, personal administrativ, preşcolari, colaboratori etc.
Art.46 Regulile au fost elaborate pentru fiecare activitate specifică domeniului şi au fost concepute în aşa fel încât fiecare să poată fi folosită cvasi independent de celelalte.
Art.47 Regulile şi procedurile din planul de securitate au rolul:
(1) de a fi corecte, echitabile şi eficiente pentru folosirea resurselor informatice şi de comunicaţie în vederea sprijinirii procesului didactic şi al cercetării ştiinţifice;
(2) de a educa utilizatorii resurselor informatice şi de comunicaţie în ceea ce priveşte responsabilităţile asociate cu utilizarea acestora;
(3) de a fi compatibile cu regulamentele, statutul şi atribuţiile stabilite pentru administrarea resurselor informatice şi de comunicaţii.
Art.48 Regulile de utilizare a Resurselor Informatice şi de Comunicaţii ale grădiniţei se aplică nediscriminatoriu tuturor persoanelor cărora li s-a permis accesul la aceste resurse;

CAPITOLUL VIII
PROCEDEE ŞI REGLEMENTĂRI

Art.49 Regulamentul privind accesul la reţeaua intranet/internet şi utilizarea aplicaţiilor software parte integrantă din Regulamentul de organizare şi funcţionare (ROF) a grădiniţei, prevede următoarele reguli privind accesul la email:
(1) Orice parolă trebuie să fie complexă. Pentru parole se respectă regulile privind parolele de acces. Administratorul pe serverul de email, creează contul de email cu o parola iniţială, care va fi schimbată de utilizator la prima accesare a contului.
(2) Toţi utilizatorii sunt obligaţi să păstreze confidenţialitatea informaţiilor privind contul de acces şi datele din acestea.
(3) Utilizatorii nu trebuie să trimită, retrimită sau să primească informaţii confidenţiale sau senzitive ce privesc grădiniţa, folosind conturi utilizator care nu sunt proprietatea grădiniţei. Exemple de astfel de conturi, sunt (dar nu sunt limitate numai la acestea: Hotmail, Yahoo mail, etc.), precum şi adrese de email puse la dispoziţie de alţi Furnizori de Servicii Internet.
Art.50 De asemenea accesul la reţeaua intranet/internet şi utilizarea aplicaţiilor software, referitor la accesul la email, este interzis:
(1) Trimiterea de mesaje cu caracter de intimidare sau hărţuire.
(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 identităţi decât cea reală atunci când se trimite email, exceptând cazurile când persoana este autorizată în scop de suport administrativ.

(6) Trimiterea mesajelor nesolicitate către grupuri de persoane, exceptând cazurile în care aceste mesaje deservesc instituţia.
Art.51 Administratorii de reţea asigură confidenţialitatea datelor personale sau a accesului la informaţii folosind poşta electronică sau alte instrumente de conversaţie electronică în limitele competenţelor, a posibilităţilor tehnice existente şi a limitelor impuse de prevederile legale în vigoare.

CAPITOLUL IX
REGLEMENTĂRI PRIVIND SECURITATEA DATELOR

Art.52 Securizarea serverelor se realizează prin următoarele reguli:
(1) Serverele trebuie să fie într-o locaţie cu acces securizat; accesul este restricţionat doar la personalul tehnic autorizat.
(2) Instalarea sistemului de operare dintr-o sursă aprobată.
(3) Setarea/activarea parametrilor de securitate, a protecţiilor pentru fişiere şi activarea jurnalelor de monitorizare.
(4) Dezactivarea sau schimbarea parolelor conturilor predefinite.
(5) Crearea şi utilizarea copiilor de siguranţă (backup).
Art.53 Regulile privind parolele de acces sunt următoarele:
(1) Orice parolă ar trebui să fie complexă şi să aibă o lungime minimă de 8 caractere. O parolă complexă este un şir de caractere compus din litere minuscule, majuscule, cifre.
(2) Nu folosiţi aceeaşi parolă pentru mai multe conturi.
(3) Dacă aveţi multe parole le puteţi scrie într-un fişier, însă criptaţi acel fişier şi asiguraţi-vă că nu-l veţi pierde. Evitaţi denumirea acelui fişier cu una explicită (ex. parolelemele.rar).
(4) Evitaţi să păstraţi parole în agende electronice, telefoane mobile.
(5) Parolele trebuie să fie schimbate de utilizator în mod regulat.
(6) Aveţi grijă la facilitatea browser-elor de reţinere a parolelor (AutoFill, Remember password) cu atât mai mult atunci când calculatorul pe care lucraţi e folosit de mai multe personae.
(7) Parolele de cont utilizator nu trebuie divulgate nimănui, nici măcar angajaţilor care răspund de securitatea sistemelor informatice.
(8) Dacă se suspectează că o parolă a putut fi divulgată aceasta trebuie schimbată imediat.
(9) Administratorii de sistem nu trebuie să permită schimbarea parolelor utilizatorilor folosind contul administrativ.
(10) 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.
(11) Schimbarea parolei asistate de administratorul de sistem trebuie să respecte următoarea procedură:
a. utilizatorul se va legitima;
b. administratorul va verifica drepturile de acces ale persoanei la contul utilizator;
c. utilizatorul va introduce o nouă parolă.
Art.54 Alte reglementări privind securitatea sunt cele care urmează, acestea se referă la activităţi interzise precum:
(1) Activităţi comerciale neautorizate;
(2) Trafic masiv de informaţii sau trafic de informaţii cu caracter frivol, obscen şi pornografic;
(3) Folosirea unor drepturi de acces la resurse pentru care nu sunt autorizaţi;
(4) Ştergerea sau alterarea datelor altor utilizatori;
(5) Tentativele de descoperire şi de folosire a parolelor altor utilizatori;
(6) Crearea sau folosirea de instrumente soft destinate spargerii sistemelor de securitate ale calculatoarelor;
(7) Provocarea deliberată de defectiuni hardware şi software;
(8) Perturbarea traficului reţelei grădiniţei;
(9) Generarea de trafic needucativ;
(10) Transferuri de materiale care contravin legilor drepturilor de autor (software pirat, filme, muzică, cărţi, etc.);
(11) Generarea de spam;
(12) Răspândirea de aplicaţii de tip virus, troieni, viermi, spyware sau altele;

(14) Folosirea de aplicaţii de tip key-logere;
(15) Modificarea adresei MAC a plăcii de reţea;
(16) Setările pentru IP şi DNS, altfel decât cu "Obtain an IP/DNS address automatically", fără autorizaţie din partea administratorului;
(17) Utilizarea de programe pentru scanarea reţelei, exploit-uri;
(18) Transmiterea de mesaje cu caracter comercial;
(19) Publicitatea cu caracter comercial;
(20) Folosirea de software fără licenţă pe calculatoarele din grădiniţă sau conectate la reţeaua acesteia.

CAPITOLUL X
REGLEMENTĂRI/PROCEDEE ADMINISTRARE INFORMAŢII

Art.55 Regulile specifice privind administrarea informaţiilor şi activităţi de mentenanţă sunt conţinute în proceduri specifice elaborate de administratori.
Art.56 Reguli de administrare a conturilor de email:
(1) Fiecare cont de email creat pe domeniul gradinitamihaieminescu.ro trebuie să aibă asociate o cerere şi o aprobare corespunzătoare.
(2) Toţi utilizatorii sunt obligaţi să păstreze confidenţialitatea informaţiilor privind contul de acces.
(3) Toate conturile trebuie să se poată identifica în mod unic, utilizând numele de cont asociat.
(4) Toate parolele pentru conturi trebuie să fie create şi folosite în conformitate cu regulile privind parolele de acces.
(5) Numărul de mesaje din Inbox nu este limitat.
(6) Pentru păstrarea tuturor mesajelor primite este necesară instalarea unui client local de email (ex: Mozilla Thunderbird, Outlook express etc.) pe calculatorul individual al fiecărui utilizator.
(7) La cererea conducerii, administratorul trebuie să furnizeze o listă cu toţi utilizatorii (listă de conturi) pentru sistemele pe care le administrează.

CAPITOLUL XI
MĂSURI DISCIPLINARE

Art.57 Administratorul reţelei are dreptul să ia măsuri de restricţionare (blocare parţială sau totală), fără notificare, a accesului la Resursele Informatice şi de Comunicaţii în cazul utilizatorilor care încalcă prevederile politicii de securitate şi regulile aplicabile în sistemul de RIC (din planul de securitate) sau legislaţia în vigoare şi care, astfel, pun în pericol funcţionarea şi/sau securitatea reţelei.
Art.58 În situaţii cu totul deosebite, când eventuale acţiuni ale unor utilizatori care, pe proprie răspundere, atentează grav la securitatea reţelei, se pot lua următoarele măsuri:
(1) rezilierea contractului de muncă în cazul angajaţilor;
(2) încetarea relaţiilor contractuale (de colaborare) în cazul contractanţilor, furnizorilor sau consultanţilor.
Art.59 Toate acţiunile care contravin legilor vor fi raportate organelor competente.

CAPITOLUL XII
DISPOZIŢII FINALE

Art.60 Aprobarea Regulamentului privind politicile de securitate IT se face de către Consiliul de Administraţie al Grădiniţei cu Program Prelungit ,,Mihai Eminescu" Tg-Jiu.
Art.61 Prezentul Regulament intră în vigoare la data de 31.01.2017, odată cu aprobarea acestuia de către Consiliul de Administratie al Grădiniţei cu Program Prelungit ,,Mihai Eminescu" Tg-Jiu.