**Colegiul Tehnic "Apulum" Alba Iulia**

**Aprobat**
**Director**
**Prof. Ursu Carmen Iuliana**

Nr. înreg. 3246 / 31.10.2017

# Planul de securitate a sistemului Resurselor Informatice şi de Comunicaţii
**Versiunea 1.1**
**Revizuit la data de 31.10.2017**

## Introducere

Regulamentele de utilizare a Resurselor Informatice şi de Comunicaţii (RIC) sunt elaborate pentru a stabili un cadru corect, legal şi eficient de utilizare a tehnologiei informaţiei şi comunicaţiilor la Colegiul Tehnic "Apulum" Alba Iulia.

Acestea au ca scop principal protejarea utilizatorilor, colaboratorilor împotriva atacurilor de orice tip (cu sau fără intenţie). De asemenea au ca scop protejarea imaginii unităţii şcolare şi a investiţiilor acesteia pentru dezvoltarea sistemul informatic şi de comunicaţii.

## Scop

În acord cu legislaţia în vigoare din România, Regulamentul de ordine interioară (ROI) al Colegiul Tehnic "Apulum" Alba Iulia, Resursele Informatice şi de Comunicaţii sunt valori ale unităţii şcolare care trebuie exploatate şi administrate ca resurse publice în proprietatea statului român. Scopul acestor regulamente este acela de a asigura:

- stabilirea unor reguli corecte, echitabile şi eficiente pentru folosirea resurselor informatice şi de comunicaţii în vederea sprijinirii procesului educaţional;
- protejarea imaginii unităţii şcolare;
- protejarea investiţiilor unităţii şcolare pentru dezvoltarea sistemului informatic şi de comunicaţii propriu;
- protejarea proprietăţii intelectuale şi a tuturor informaţiilor stocate şi transportate folosind Resursele Informatice şi de Comunicaţii ale utilizatorilor autorizaţi cadre didactice, personal didactic auxiliar, personal administrativ, elevi, colaboratori etc.;
- educarea utilizatorilor resurselor informatice şi de comunicaţii în ceea ce priveşte responsabilităţile asociate cu utilizarea acestora;
- compatibilitatea cu regulamentele, statutul şi atribuţiile stabilite pentru administrarea resurselor informatice şi de comunicaţii.

## Audienţă

Regulamentele de utilizare a Resurselor Informatice şi de Comunicaţii ale Colegiul Tehnic "Apulum" Alba Iulia se aplică nediscriminatoriu tuturor persoanelor cărora li s-a permis accesul la acestea.

**Proceduri de elaborare, modificare şi aprobare a regulamentelor**

• Regulamentele de utilizare a Resurselor Informatice şi de Comunicaţii ale unităţii şcolare se elaborează pentru fiecare activitate specifică domeniului şi trebuie concepute în aşa fel încât fiecare regulament să poată fi folosit cvasi-independent de celelalte.

• Regulamentele vor fi elaborate de către responsabilul IT şi vor fi propuse pentru aprobare conducerii Colegiul Tehnic "Apulum" Alba Iulia.

• Prevederile politicii de securitate aprobate vor fi incluse în contractul de muncă pentru angajaţi şi toate contractele cu terţi (dacă activitatea acestora are legătură cu sistemul informatic şi de comunicaţii al unităţii şcolare).

• Fiecare regulament va conţine informaţii de identificare proprii şi se va specifica data la care acesta a fost aprobat şi data de la care acesta este aplicabil.

• Regulamentele de utilizare a sistemului Resurselor Informatice şi de Comunicaţii vor fi disponibile în format electronic pe site-ul unităţii şcolare la adresa www.aicta.ro.

• Modificarea prevederilor unui regulament se face cu aprobarea conducerii unităţii şcolare. Fiecare modificare va include modificarea versiunii documentului şi a informaţiilor de identificare. Versiunea anterioară rămâne valabilă până în momentul în care noua versiune este aplicabilă.

Prezentul document va conţine o listă a tuturor regulamentelor aplicabile în sistemul Resurselor Informatice şi de Comunicaţii.

**Proceduri şi regulamente specifice:**

1. **Regulament privind utilizarea permanentă a resurselor informatice şi de comunicaţii**

• Utilizatorii trebuie să anunţe responsabilul IT în cazul în care se observă orice problemă/breşă în sistemul de securitate a RIC din cadrul unităţii şcolare cât şi orice posibilă întrebuinţare greşită sau încălcare a regulamentelor în vigoare.

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

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

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

• Utilizatorii nu trebuie să se angajeze într-o activitate care ar putea hărţui sau ameninţa alte persoane; să degradeze performanţele RIC; să împiedice accesul unui utilizator autorizat la RIC; să obţină alte resurse în afara celor alocate; să nu ia în considerare măsurile de securitate impuse prin regulamente.

• Utilizatorii nu trebuie să descarce, instaleze şi să ruleze programe de securitate sau utilitare care expun sau exploatează vulnerabilităţi ale securităţii RIC. De exemplu, utilizatorii nu trebuie să ruleze programe de decriptare a parolelor, de captură de trafic, de scanări ale reţelei sau orice alt program nepermis de regulamente.

• RIC ale unităţii şcolare nu trebuie folosite pentru beneficiul personal.

• Utilizatorii nu trebuie să acceseze, să creeze, să stocheze sau să transmită materiale pe care unitatea şcolară le poate considera ofensatoare, indecente sau obscene (altele decât cele în curs de cercetare educaţională unde acest aspect al cercetării are aprobarea explicită a conducerii unităţii şcolare).
• Accesul la reţeaua Internet prin intermediul RIC se supune aceloraşi regulamente care se aplică utilizării din interiorul instituţiei şi Regulamentului pentru utilizare Internet şi intranet. Angajaţii nu trebuie să permită membrilor familiei sau altor persoane accesul la RIC ale unităţii şcolare.
• Utilizatorii care au acces la sistemul RIC al unităţii şcolare au obligaţia de a purta acte şi sau legitimaţii care să ateste calitatea de utilizator autorizat în spaţiile respective.
• Utilizatorii nu trebuie să se angajeze în acţiuni împotriva scopurilor unităţii şcolare folosind RIC.

## 2. Regulament privind utilizarea ocazională

• În anumite situaţii este permisă utilizarea ocazională a RIC. În aceste situaţii se aplică următoarele restricţii:
• Utilizarea personală ocazională a serviciilor de poştă electronică, acces Internet, telefoane, fax-uri, imprimante, copiatoare etc. este restricţionată la utilizatorii autorizaţi şi nu poate fi extinsă la membrii familiilor sau alte persoane.
• Utilizarea ocazională a RIC nu trebuie să aibă drept rezultate costuri directe pentru unitatea şcolară.
• Utilizarea ocazională a RIC nu trebuie să afecteze activitatea normală a angajaţilor.
• Nu este permisă trimiterea sau recepţionarea documentelor sau fişierelor care pot cauza acţiuni legale împotriva unităţii şcolare sau prejudicierea, indiferent de formă, a intereselor acesteia.

## 3. Regulament privind confidenţialitatea serviciilor informatice şi de comunicaţii

• Utilizatorii trebuie să raporteze orice slăbiciune în sistemul de securitate al calculatoarelor din cadrul unităţii şcolare, orice incident de posibilă întrebuinţare greşită sau încălcare a acestui regulament (prin contactarea responsabilului IT).
• Un mare număr de utilizatori (inclusiv elevi), pot accesa informaţii din exteriorul sistemului de comunicaţii al unităţii şcolare. În aceste condiţii este obligatorie păstrarea confidenţialităţii informaţiilor transmise din exteriorul RIC şi a informaţiilor obţinute din interior.
• Utilizatorii nu trebuie să încerce să acceseze informaţii sau programe de pe sistemele unităţii şcolare pentru care nu au autorizaţie sau consimţământ explicit.
• Nici un utilizator al sistemului RIC al unităţii şcolare nu poate divulga informaţiile la care are acces sau la care a avut acces ca urmare a unei vulnerabilităţi a sistemului RIC. Această regulă se extinde şi după ce utilizatorul a încheiat relaţiile cu unitatea şcolară.
• Confidenţialitatea informaţiilor transmise prin intermediul resurselor de comunicaţii ale terţilor nu poate fi asigurată. Pentru aceste situaţii, confidenţialitatea

şi integritatea informaţiilor se poate asigura folosind tehnici de criptare. Utilizatorii sunt obligaţi să se asigure că toate informaţiile confidenţiale ale unităţii şcolare se transmit în aşa fel încât să se asigure confidenţialitatea şi integritatea acestora.

## 4. Regulament de acces administrativ

• Utilizatorii trebuie să cunoască şi să accepte toate regulamentele privind securitatea RIC înainte de a li se permite accesul la un cont.
• Utilizatorii care au conturi de acces administrativ trebuie sa aibă instrucţiuni de administrare, documentare, instruire şi autorizare a conturilor.
• Utilizatorii cu drepturi administrative sau speciale de acces nu trebuie să folosească în mod abuziv aceste drepturi şi trebuie să facă investigaţii numai sub îndrumarea responsabilului IT.
• Cei care utilizează conturi de acces cu drepturi administrative sau speciale trebuie să folosească tipul de privilegiu cel mai potrivit activităţii pe care o desfăşoară.
• Accesul administrativ trebuie să se conformeze Regulamentului de utilizare a parolelor.
• Parola pentru un cont cu acces privilegiat nu va fi utilizată de mai multe persoane decât cu acordul scris al responsabilului IT şi trebuie să fie schimbată atunci când persoana care utilizează acest cont îşi schimbă locul de muncă, sau în cazul unei modificări a listei de personal ale terţilor (furnizor desemnat) în contractele cu unitatea şcolară.
• Unele conturi sunt necesare pentru audit (verificare, control) intern sau extern, pentru dezvoltare sau instalare de software sau alte operaţiuni definite. Acestea trebuie să îndeplinească următoarele condiţii:
    - trebuie să fie autorizate;
    - trebuie create cu dată de expirare specifică;
    - contul va fi şters atunci când nu mai este necesar.

## 5. Regulament privind accesul fizic la RIC

• Accesul fizic la toate încăperile în care sunt instalate RIC trebuie să fie documentat şi monitorizat.
• Toate încăperile în care sunt instalate RIC trebuie să fie protejate fizic, în funcţie de importanţa acestora şi tipul datelor vehiculate sau stocate.
• Pentru fiecare încăpere în care sunt instalate echipamente ale sistemului RIC se aprobă accesul doar pentru personalul care răspunde de buna funcţionare a echipamentelor din încăperea respectivă şi, dacă este cazul, părţilor contractante, ale căror obligaţii contractuale implică acces fizic.
• Personalul care are drepturi de acces trebuie să deţină legitimaţie de serviciu şi acte de identitate care să-i ateste calitatea.
• Acordarea drepturilor de acces (folosind card-uri, chei, parole etc.) se face în scris de către responsabilul IT.
• Nu este permis transferul dreptului de acces indiferent de motiv.
• Cardurile şi/sau cheile de acces care nu mai sunt folosite trebuie predate responsabilului IT.

• Pierderea sau furtul cardurilor şi/sau cheilor de acces trebuie raportate imediat responsabilului IT.
• Cardurile şi/sau cheile nu trebuie să aibă informaţii de identificare, altele decât informaţia de contact necesară pentru returnare.
• Accesul vizitatorilor în spaţiile protejate trebuie documentat pentru fiecare începere şi în cazul în care este permis, se va delega un însoţitor. Vizitatorii trebuie să fie însoţiţi în zonele cu acces restricţionat.
• Responsabilul IT trebuie să verifice periodic drepturile de acces pe bază de card şi/sau cheie şi să anuleze aceste drepturi pentru persoanele care pierd dreptul de acces.
• Accesul restricţionat trebuie marcat.

## 6. Regulament de acces la reţeaua de comunicaţii

• Utilizatorilor le este permis să utilizeze numai parametrii pentru conectare la reţea specificaţi de către responsabilul IT.
• Conectarea sistemelor de calcul/dispozitivelor mobile de orice fel (laptop, stick, hard-disk extern, smartphone, tabletă etc.) care nu sunt proprietatea unităţii şcolare se face numai cu aprobarea verbală/în scris a responsabilului IT la recomandarea conducerii unităţii şcolare.
• Accesul de la distanţă la reţeaua unităţii şcolare se va realiza numai prin echipamente aprobate, sau prin intermediul unui furnizor de servicii internet (Internet Service Provider - ISP) agreat de către unitate şi folosind protocoale aprobate de către responsabilul IT.
• Utilizatorii RIC din interiorul unităţii şcolare nu se pot conecta la altă reţea.
• Utilizatorii nu trebuie să extindă sau să retransmită serviciile de reţea în nici un fel (pe nici o cale). Nu este permisă instalarea de conexiuni de reţea neautorizate indiferent de motiv. Autorizarea tuturor conexiunilor se face la propunerea conducerii unităţii şcolare de către responsabilul IT.
• Utilizatorii nu trebuie să instaleze echipamente hardware sau programe care furnizează servicii de reţea fără aprobarea responsabilul IT.
• Utilizatorii nu au dreptul să descarce, să instaleze sau să ruleze programe de securitate care pot dezvălui slăbiciuni în securitatea unui sistem. De exemplu, utilizatorii unităţii şcolare nu au dreptul să ruleze programe de spargere a parolei, sustragere de pachete, scanare a porturilor, în timp ce sunt conectaţi la reţeaua unităţii.
• Utilizatorii nu au dreptul să modifice, reconfigureze, instaleze, dezinstaleze echipamente de reţea, cabluri, prize de conexiuni.
• Serviciul de nume şi administrarea adreselor IP sunt deservite exclusiv de către responsabilul IT.
• Nu este permisă instalarea şi sau modificarea echipamentelor utilizate pentru conectare la reţea (inclusiv plăci de reţea) fără aprobarea responsabilului IT. Tipul şi modelul plăcilor de reţea şi tuturor echipamentelor care se pot conecta în reţea trebuie să fie aprobate de către responsabilului IT.

## 7. Regulament privind configurarea sistemelor informatice pentru acces la reţeaua de comunicaţii

• Infrastructura de comunicaţii, reţeaua de comunicaţii digitale a unităţii şcolare este administrată de către responsabilul IT, care este responsabil cu întreţinerea şi dezvoltarea acesteia.
• Pentru a furniza o infrastructură de comunicaţii unitară cu posibilităţi de modernizare toate componentele acesteia sunt instalate de către responsabilul IT sau de către un furnizor avizat explicit de către acesta.
• Toate echipamentele, fără excepţie, conectate la reţeaua de comunicaţii trebuie configurate conform specificaţiilor responsabilul IT.
• Orice dispozitiv hardware, inclusiv plăcile de reţea, care se va conecta la reţeaua unităţii şcolare, trebuie să fie însoţit de o aprobare de tip (producător, model etc.) din partea responsabilul IT.
• Modificarea configuraţiei oricărui dispozitiv activ conectat la reţeaua de comunicaţii se face numai cu aprobarea responsabilul IT.
• Infrastructura de comunicaţii de date a unităţii şcolare suportă un set definit de protocoale de reţea (TCP/IP). Orice utilizare a altui set de protocoale trebuie să fie aprobată în scris de către responsabilul IT.
• Adresele de reţea sunt alocate dinamic pentru echipamentele conectate prin routere sau static pentru staţiile de lucru numai de către responsabilul IT.
• Toate conectările dintre reţeaua de comunicaţii a unităţii şcolare şi alte reţele de comunicaţii, publice sau private, sunt responsabilitatea exclusivă a responsabilul IT.
• Echipamentele de protecţie a reţelei de comunicaţie a unităţii şcolare (ex. firewall) se vor instala de către responsabilul IT.
• Utilizatorii nu au dreptul să extindă sau să retransmită în nici un fel serviciile reţelei (este interzisă instalarea unui telefon, fax, modem, router, switch, hub sau punct de acces la reţeaua unităţii şcolare) fără aprobare din partea responsabilul IT.
• Utilizatorilor li se interzice instalarea de dispozitive hardware de reţea sau programe care furnizează servicii de reţea fără aprobarea responsabilul IT.
• Utilizatorilor nu le este permis accesul la dispozitivele hardware ale reţelei.

## 8. Regulament de tratare a incidentelor de securitate

• Ori de câte ori un incident de securitate este suspectat sau confirmat, precum un virus, vierme, descoperirea unor activităţi suspecte, informaţii modificate etc. trebuie urmate procedurile standard specifice pentru micşorarea riscurilor.
• Responsabilul IT realizează înştiinţarea şi coordonarea pentru tratarea incidentului.
• Responsabilul IT execută strângerea dovezilor fizice şi electronice ce vor face parte din documentaţia pentru tratarea incidentului.
• Responsabilul IT va stabili conţinutul comunicatelor pentru utilizatori privind incidentele şi va determina nivelul şi modul de distribuire a acestei informaţii.
• Responsabilul IT trebuie să comunice proprietarului sau producătorului resursei afectate de un incident informaţiile utile pentru eliminarea sau diminuarea vulnerabilităţilor care au cauzat incidentul.
• Responsabilul IT realizează documentarea anchetei privind incidentul.

• Responsabilul IT răspunde de coordonarea activităţilor de comunicare cu terţi pentru rezolvarea incidentului.
• În cazul în care incidentul nu implică acţiuni contrare legilor în vigoare responsabilul IT va recomanda sancţiuni disciplinare.
• În cazul în care incidentul implică aplicarea legilor civile sau penale responsabilul IT va recomanda sesizarea organelor în drept ale statului şi va acţiona ca persoană de legătură cu acestea.

## 9. Regulament de monitorizare a RIC

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

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

• Fişierele jurnal vor fi examinate regulat în vederea detectării eventualelor atacuri informatice şi abateri de la regulamentele de securitate ale unităţii şcolare. În această categorie intră următoarele (fără a se limita doar la acestea):

- jurnale ale sistemelor de detectarea automată a intruşilor;
- jurnale firewall;
- jurnale ale activităţii conturilor utilizator;
- jurnale ale scanărilor reţea;
- jurnale ale aplicaţiilor;
- jurnale ale solicitărilor de suport tehnic;
- jurnale ale erorilor din sisteme şi servere.

• În mod regulat (cel puţin o dată la şase luni) se vor efectua verificări, de către responsabilul IT pentru detectarea:

- parolelor utilizator care nu respectă regulamentele;
- echipamentelor de reţea conectate neautorizat;
- serviciilor de reţea neautorizate;
- serverelor de pagini web neautorizate;
- echipamentelor ce utilizează resurse comune nesecurizate;
- utilizării de modemuri neautorizate;
- licenţelor pentru sistemele de operare şi programele instalate.

• Orice neregulă privind respectarea regulamentelor de securitate va fi raportată către responsabilul IT în scopul efectuării de investigaţii.

## 10.Regulament de securizare a serverelor

• Un server nu trebuie conectat la reţeaua unităţii şcolare până când nu se află într-o stare sigură acreditată de către responsabilul IT.
• Procedura de securizare a serverelor trebuie să includă obligatoriu următoarele:
- instalarea sistemului de operare dintr-o sursă aprobată;
- aplicarea patch-urilor furnizate de producător;
- înlăturarea programelor, a serviciilor sistem şi a driverelor care nu sunt necesare;
- setarea/activarea parametrilor de securitate, a protecţiilor pentru fişiere şi activarea jurnalelor de monitorizare;
- dezactivarea sau schimbarea parolelor conturilor predefinite;
- securizarea accesului fizic la aceste echipamente.

• Responsabilul IT va monitoriza obligatoriu pentru servere procesul de instalare şi aplicare regulată a patch-urilor de securitate.

## 11.Regulament privind crearea şi utilizarea copiilor de siguranţă (backup)

• Frecvenţa, dimensiunea şi conţinutul copiilor de siguranţă trebuie să fie în concordanţă cu importanţa informaţiei şi cu riscul acceptat de proprietarul datelor.
• Procedura de creare a copiilor de siguranţă şi de recuperare pentru fiecare sistem din cadrul RIC trebuie să fie documentată şi periodic revizuită.

## 12.Regulament pentru detectarea accesului neautorizat

• Procesele de înregistrare şi verificare a activităţii sistemelor de operare, conturilor utilizator şi programelor trebuie să fie funcţionale pe toate sistemele active (host, server, echipamente de reţea).
• Trebuie activate funcţiile de anunţare a persoanelor responsabile oferite de firewall-uri şi sistemele de control al accesului la reţea.
• Trebuie activate funcţiile de înregistrare a evenimentelor pe dispozitivele firewall şi pe toate sistemele de control al accesului.
• Verificările privind integritatea fiecărui sistem trebuie să se facă periodic. Această activitate este obligatorie şi pentru dispozitivele de tip firewall sau dispozitive de control al accesului.
• Se vor verifica periodic programele utilitare pentru detectarea tentativelor de acces neautorizat.
• Toate rapoartele privind incidentele trebuie revizuite în vederea detectării de indicii ce ar putea implica o activitate de acces neautorizat.
• Toate indiciile suspecte sau confirmate de accesări sau încercări de accesare neautorizate trebuie raportate imediat către responsabilul IT.
• Utilizatorii sunt obligaţi să raporteze orice anomalii în performanţa sistemelor utilizate cât şi orice semne ale unor posibile infracţiuni responsabilului IT.

## 13. Regulament privind securitatea informaţiilor în cazul utilizării sistemelor de calcul/dispozitivelor portabile

• Informați responsabilului IT de faptul că aveți un dispozitiv personal pe care doriți să îl folosiți la serviciu. Responsabilului IT vă va introduce dispozitivul în rețeaua unităţii şcolare și vă va informa asupra regulilor de utilizare în interiorul instituției.
• Conectarea sistemelor de calcul/dispozitivelor portabile (laptop, stick, hard-disk extern, smartphone, tabletă etc.) care nu sunt proprietatea unităţii şcolare se face numai cu aprobarea verbală/în scris a responsabilului IT la recomandarea conducerii unităţii şcolare.
• Nu uitați că un smartphone este un dispozitiv de stocare portabil. Scanați conținutul memoriei interne și externe a telefonului la fiecare introducere în calculatorul de serviciu cât și în cel de acasă. In acest fel, nu veți transfera viruși de la serviciu, acasă și viceversa.
• Din același motiv, nu introduceți nici un dispozitiv de stocare găsit (de exemplu, USB stick, CD/DVD-ROM, card SD etc.) în calculatoarele unităţii şcolare. Majoritatea atacurilor asupra rețelei încep cu un astfel de dispozitiv "uitat" de atacator.
• Calculatoarele portabile trebuie să fie protejate prin parole.
• Se va evita stocarea datelor care privesc unitatea şcolară pe dispozitivele portabile.

## 14. Regulament pentru modificări şi modernizări ale RIC

• Orice modificare asupra unei componente a RIC din cadrul unităţii şcolare, cum ar fi: sisteme de operare, componente hardware, echipamente şi componente de reţea, aplicaţii, este supusă prezentului regulament şi trebuie să urmeze procedurile în vigoare.
• Toate propunerile de modernizare şi extindere a elementelor de infrastructură a sistemului RIC vor fi documentate şi aprobate de către responsabilul IT. Nu este permisă modificarea de către utilizatori a elementelor de infrastructură a RIC.
• Modificările şi modernizările sistemelor de calcul vor fi documentate de către responsabilul IT şi aprobate de către conducerea unităţii şcolare.

## 15. Regulament de utilizare a reţelei Internet şi intranet

• Programele pentru acces la reţeaua Internet sunt destinate utilizatorilor autorizaţi pentru a fi folosite în scopuri educaţionale.
• Toate programele utilizate pentru acces la reţeaua Internet trebuie să facă parte din pachetul de programe aprobat de către responsabilul IT. Aceste programe trebuie să includă toate patch-urile de securitate puse la dispoziţie de către producător.
• Toate fişierele care provin din reţeaua Internet trebuie să fie scanate cu un program antivirus care să fie actualizat cel puţin o dată la 24 ore.
• Toate programele pentru acces Internet/intranet trebuie să permită folosirea sistemelor proxy şi/sau firewall.
• Toate informaţiile accesate în reţeaua Internet trebuie să se conformeze Regulamentului de utilizare acceptabilă a RIC.

• Orice activitate a utilizatorilor folosind RIC poate fi înregistrată şi ulterior examinată.
• Nu se vor publica pe site-ul web ale unităţii şcolare materiale publicitare comerciale sau personale.
• Nu este permisă utilizarea RIC ale unităţii şcolare în scop personal sau pentru solicitări personale ce nu au legătură cu unitatea.
• Cumpărăturile pe Internet care nu au legătură cu atribuţiile de serviciu sunt interzise.
• Orice material confidenţial al unităţii şcolare transmis prin reţeaua Internet trebuie criptat.
• Fişierele electronice se supun aceloraşi reguli de păstrare care se aplică şi altor documente şi trebuie păstrate în conformitate cu regulile stabilite prin prezentele regulamente.

## 16.Regulament de administrare a conturilor

• Toate conturile create trebuie să aibă asociată o cerere şi o aprobare corespunzătoare.
• Prin contractul de muncă, contractul de şcolarizare şi/sau alte documente toţi utilizatorii acceptă prevederile regulamentelor privind securitatea sistemului RIC.
• Toţi utilizatorii sunt obligaţi să păstreze confidenţialitatea informaţiilor privind contul de acces.
• Toate conturile trebuie să se poată identifica în mod unic, utilizând numele de cont asociat.
• Toate parolele pentru conturi trebuie să fie create şi folosite în conformitate cu Regulamentul privind parolele de acces.
• Toate conturile utilizator care nu au fost accesate timp de 90 de zile vor fi dezactivate. După încă 90 zile conturile vor fi şterse dacă nu s-a solicitat accesul la acestea.
• Responsabilul IT trebuie să furnizeze o listă cu toţi utilizatorii (listă de conturi) pentru sistemele pe care le administrează, la cererea conducerii unităţii şcolare.

## 17.Regulament pentru parolele de acces

• Toate parolele trebuie să îndeplinească următoarele condiţii:
- să fie schimbate de către responsabilul IT în mod regulat, cel puţin o dată la 90 de zile;
- să aibă o lungime minimă de 8 caractere;
- să fie parole complexe;
- reutilizarea parolelor este interzisă;
- parolele stocate trebuie criptate;
- parolele de cont utilizator sunt responsabilitatea utilizatorilor.

• Responsabilul IT nu trebuie să permită schimbarea parolelor utilizatorilor folosind contul administrativ.
• Utilizatorii nu pot folosi programe de stocare a parolelor. Se pot face excepţii pentru anumite aplicaţii (precum backup automat) cu aprobarea responsabilului IT.

Pentru ca o excepţie să fie aprobată, trebuie să existe o procedură pentru schimbarea parolelor.
• Dispozitivele de calcul nu trebuie lăsate nesupravegheate fără a activa un sistem de blocare a accesului la acestea; deblocarea trebuie să se facă folosind parola.
• Procedurile de schimbare a parolei asistate de responsabilul IT trebuie să respecte următoarea procedură:
- utilizatorul se va legitima, responsabilul IT va verifica drepturile de acces a persoanei la contul utilizator;
- se va genera o nouă parolă care va fi comunicată utilizatorului;
- utilizatorul va schimba parola temporară, comunicată anterior, în maxim 24 ore.

## 18.Regulament privind sistemul de mesagerie electronică

• Următoarele activităţi sunt interzise de regulament:
- trimiterea de mesaje cu caracter de intimidare sau hărţuire;
- folosirea sistemului de mesagerie electronică în scopuri personale;
- folosirea sistemului de mesagerie electronică în scopuri politice sau pentru campanii politice;
- încălcarea drepturilor de autor prin distribuirea neautorizată a materialelor protejate;
- folosirea altei identităţi decât cea reală atunci când se trimite email, exceptând cazurile când persoana este autorizată în scop de suport administrativ.

• Următoarele activităţi sunt interzise deoarece împiedică buna funcţionare a comunicaţiilor în reţea şi eficienţa sistemelor de mesagerie electronică:
- trimiterea mesajelor nesolicitate către grupuri de persoane, exceptând cazurile în care aceste mesaje deservesc instituţia;
- trimiterea mesajelor de dimensiuni foarte mari;
- trimiterea sau retrimiterea mesajelor ce pot conţine viruşi.

• Toate informaţiile şi datele confidenţiale ale unităţii şcolare, transmise către alte reţele externe, trebuie să fie criptate.
• Toate activităţile utilizatorilor ce implică accesul şi/sau folosirea RIC ale unităţii şcolare pot fi oricând înregistrate şi analizate.
• Utilizatorii serviciilor de mesagerie electronică nu trebuie să dea impresia că reprezintă, că îşi spun opinia sau dau declaraţii în numele unităţii şcolare cu excepţia situaţiilor în care aceştia sunt autorizaţi în mod corespunzător (implicit sau explicit) să facă acest lucru. Atunci când este cazul, se va include o declaraţie explicită prin care utilizatorul specifică faptul că nu reprezintă unitatea şcolară. Un exemplu de declaraţie simplă este: “părerile exprimate sunt personale, şi nu ale Colegiului … ”.

## 19.Regulament de detectare a viruşilor

• Toate staţiile de lucru de sine stătătoare sau conectate la reţeaua de comunicaţii a unităţii şcolare, trebuie să utilizeze programe antivirus aprobate de către responsabilul IT.
• Programele antivirus nu trebuie dezactivate.

• Configuraţia programului antivirus trebuie să nu fie modificată într-un mod care să reducă eficacitatea programului.
• Frecvenţa actualizărilor automate a programului antivirus trebuie asigurată de către responsabilul IT.
• Orice server de fişiere conectat la reţeaua unităţii şcolare trebuie să utilizeze un program antivirus aprobat în scopul detectării şi curăţirii viruşilor care pot infecta fişierele puse la dispoziţie.
• Orice server sau gateway pentru e-mail trebuie să folosească un program antivirus pentru e-mail aprobat şi trebuie să respecte regulile de instalare şi utilizare a acestui program.
• Orice virus care nu a putut fi înlăturat automat de către programul antivirus constituie un incident de securitate şi trebuie raportat imediat responsabilului IT.

## 20. Regulament de relaţii cu terţi

• Orice activitate desfăşurată de furnizor care implică acces la RIC trebuie să se conformeze cu regulamentele în vigoare ale unităţii şcolare, cu procedurile standard şi convenţiile care cuprind, dar nu se limitează la următoarele:
- Regulament de securitate a accesului fizic;
- Regulament de confidenţialitate;
- Regulament de securitate a accesului la RIC;
- Regulament de modificare şi modernizare;
- Regulament de utilizare acceptabilă.

• În toate convenţiile şi contractele încheiate cu furnizorii trebuie specificate următoarele:
- informaţiile din cadrul unităţii şcolare, la care furnizorul are drept de acces;
- modul în care informaţiile la care furnizorul are drept de acces urmează a fi protejate de către acesta precum şi măsuri ce vor fi luate în cazul nerespectării clauzelor;
- metodele de predare, distrugere sau de transfer al drepturilor informaţiilor unităţii şcolare aflate în posesia furnizorului, la încheierea contractului.

• Furnizorul trebuie să folosească sistemul RIC din cadrul unităţii şcolare numai în scopul stipulat în contract.
• Orice altă informaţie din sistemul RIC al unităţii şcolare obţinută de furnizor pe durata contractului nu poate fi folosită în interes propriu de către furnizor sau divulgată altora.
• 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 ale unităţii şcolare şi Regulamentul de acces administrativ.
• În cazul terminării/rezilierii contractului sau la cererea unităţii şcolare, furnizorul va preda sau distruge toate informaţiile ce aparţin unităţii şi va oferi certificare în scris privind predarea sau distrugerea informaţiilor în decurs de 24 de ore de la producerea evenimentului.

• Toate programele folosite de furnizor în scopul furnizării serviciilor stipulate în contract către unitatea şcolară trebuie să fie inventariate corespunzător şi să posede drepturi de utilizare atestate prin licenţe.

Întocmit
Analist programator
Berindeie Avram-Teodor