REGULAMENT

PRIVIND UTILIZAREA ȘI SECURITATEA RESURSELOR INFORMATICE ȘI DE COMUNICAȚII A REȚELEI DIN CADRUL UNIVERSITĂȚII "AUREL VLAICU" DIN ARAD

R 80

REVIZIA 1

Domeniu de aplicare:

Prezentul regulament este valabil pentru utilizatorii resurselor informatice și de comunicații (R.I.C.) angajați, studenți sau colaboratori ai Universității "AUREL VLAICU" din Arad

Cuprins:

Aprobat: Ramona LILE	Semnătura:	Data intrării în vigoare:
Avizat: Alexandru POPA	Semnătura:	10.09.2018
Elaborat: Florin PEIȚA	Semnătura:	

REGULAMENT
privind utilizarea şi securitatea Resurselor Informatice şi de Comunicaţii a reţelei din cadrul *Universităţii „Aurel Vlaicu "din Arad*

Capitolul 1.
INTRODUCERE

În acord cu prevederile din prezentul regulament, Resursele Informatice şi de Comunicaţii puse la dispoziţie şi administrate de către Compartimentul IT (C.I.R.P.I.) sunt bunuri strategice ale Universităţii *„Aurel Vlaicu"* din Arad care trebuie administrate ca resurse ale statului român.

Compromiterea securităţii acestor resurse poate afecta capacitatea Universităţii *„Aurel Vlaicu" din Arad* 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 *UAV*, precum şi de necesitatea dezvoltării normale a unei resurse de informare.

1.1. Reţeaua *UAV*

Reţeaua de calculatoare a Universităţii *„Aurel Vlaicu "* (numită *UAV* în cele ce urmează) cuprinde totalitatea Resurselor Informatice şi de Comunicaţie ale Universităţii cu sau fără acces la reţeaua Internet/Intranet.

Reţeaua *UAV* are ca scop sprijinirea procesului de învăţământ şi cercetare prin mijloacele de comunicare şi serviciile specifice oferite de reţelele de calculatoare conectate în Internet.

Orice activitate care se desfăşoară prin intermediul reţelei *UAV* trebuie să respecte legislaţia în vigoare (internă şi internaţională): *Legea nr. 64/2004, Legea nr. 285/2004, Legea nr. 451/2004, Legea nr. 496/2004, Legea nr. 506/2004 cu modificarile si completarile ulterioare, Legea nr. 51/2003, Legea nr. 161/2003 abrogată parţial, modificată prin Legea 128/2017, Legea nr. 196/2003 cu modificarile si completarile ulterioare, Legea 365/2002 cu modificarile si completarile ulterioare, Legea republicata nr. 455/2001, Legea 129/2018, Legea nr. 8/1996 cu modificarile si completarile ulterioare, HG nr. 1308/2002, Convenţia privind Criminalitatea Informatică a Consiliului Europei, Declaraţia privind libertatea comunicării pe Internet a Consiliului Europei, etc.), statutul* şi *regulamentul de funcţionare* (aprobat prin OMEN 3704/26.04.2000) ale reţelei naţionale educaţionale RoEduNet la care *UAV* este afiliată, precum şi prezentul *Regulament.*

1.2. Definiţii şi termeni

Internet = reţeaua internaţională de calculatoare. Regulile acestei reţele se regăsesc în prevederile InterNIC, RIPE, etc.

Cont = o entitate specificată printr-un identificator şi/sau parolă pentru accesul la sistemu de comunicaţie şi/sau la o resursă de calcul.

Administrator de reţea = o persoană calificată şi autorizată, responsabilă pentru gestionarea şi operarea unor resurse de calcul şi/sau de comunicaţie pentru uzul altor persoane.

Resurse Informatice şi de Comunicaţii (RIC) = 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), pagere, sisteme de procesare distribuită, echipament de laborator 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.

Utilizator = o persoană, o aplicaţie automatizată sau proces utilizator autorizat de către UAV, în conformitate cu procedurile şi regulamentele în vigoare, să folosească Resursele Informatice şi de Comunicaţii ale UAV (a se vedea).

Abuz de privilegii = orice acţiune întreprinsă în mod voit de un utilizator, care vine în contradicţie cu regulamentele UAV 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 prentru UAV în baza unui contract comercial sau de colaborare.

Capitolul 2.

POLITICA DE SECURITATE

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 Resursele Informatice şi de Comunicaţii ale UAV şi să instruiască utilizatorii care au dreptul de folosire a Resurselor Informatice şi de Comunicaţii privind responsabilităţile asociate unei astfel de utilizări.

2.1. Audienţă

Politica de securitate a Resurselor Informatice şi de Comunicaţii ale UAV se aplică nediscriminatoriu tuturor; persoanelor cărora li s-a permis accesul la orice RIC a instituţiei. Nu există niciun fel conotaţii politice, religioase, rasiale legate de prevederile politicii de securitate. Trebuie privită doar ca un instrument de protecţie a muncii utilizatorilor şi nu ca un element restrictiv.

Prevederile Politicii vizează în mod direct utilizatorii reţelei *UAV,* dar şi furnizorii sau alte persoane, entităţi şi organizaţii care au acces la Resursele Informatice şi de Comunicaţii ale UAV.

2.2. Scop

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 i procedurilor de securitate

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 UAV sunt proprietatea Universităţii în condiţiile legilor în vigoare. Utilizatorul răspunde personal de confidenţialitatea datelor încredinţate prin procedurile de acces la Resursele Informatice şi de Comunicaţii.

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 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.

2.3. 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 şi strict secrete.

Publice: Acestea sunt informaţiile accesibile oricărui utilizator din interiorul sau exteriorul UAV. 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 UAV.

Exemple: Informaţiile de pe aviziere, servere web publice, ştirile de presă, informările Rectorului sau Senatului.

Secrete: În această categorie se includ informaţiile care datorită valorii economice nu trebuie făcute publice. Se includ aici şi informaţiile pe care UAV 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 UAV doar utilizatorilor autorizaţi. Distribuirea acestor informaţii de către utilizatorii autorizaţi trebuie să se facă pe baza unei clauze de confidenţialitate.

Exemple: clauze contractuale, conturi si parole folosite pe serverele de contabilitate sau gestiune a şcolarităţii.

Strict Secrete sau Confidenţiale: În această categorie se includ toate informaţiile care datorită valorii economice 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 Universităţii.

Exemple: cheile criptografice, conturi administrative de pe serverele de gestiune a şcolarităţii sau de contabilitate.

2.4. Atribuţii şi responsabilităţi

2.4.1. Atribuţii manageriale

Orice angajat sau compartiment al UAV trebuie să se asigure că managementul respectă prevederile prezentei Politici şi a regulamentelor sau procedurilor asociate.

Administratorii de reţea/sistem/baze de date trebuie să asigure existenţa jurnalelor şi a traseelor auditării pentru orice tip de acces în sistem conform regulilor sau procedurilor asociate.

Administratorii de reţea/sistem/baze de date trebuie să asigure activarea tuturor mecanismelor de securitate.

Compartimentul de audit intern este responsabil de evaluarea schemei de clasificare a informaţiilor.

2.4.2. Atribuţii şi obligaţii ale administratorilor reţelei *UAV*

Administratorul reţelei *UAV* este Compartimentul IT (C.I.R.P.I.). Desemnarea Compartimentul IT (C.I.R.P.I.) ca administrator are ca scop stabilirea în mod clar a responsabilităţii privind administrarea şi buna funcţionare a Resurselor Informatice şi de Comunicaţii din cadrul reţelei *UAV*, precum şi a responsabilităţii privind crearea, modificarea şi aprobarea regulilor şi politicilor referitoare la activităţile de administrare şi utilizare a Resurselor Informatice şi de Comunicaţii.

Atribuţiile şi obligaţiile *Compartimentul IT (C.I.R.P.I.)* includ:

- Elaborarea şi propunerea de modificări ale politicii de securitate a sistemului RIC ;
- Elaborarea şi propunerea pentru aprobare a planului de securitate (acesta conţine o listă a tuturor regulilor şi procedurilor de securitate aplicabilela sistemul de RIC ;
- Elaborarea procedurilor pentru identificarea utilizatorilor RIC ;
- Tratarea incidentelor de securitate în scopul minimizării efectului distructiv al acestora asupra RIC.

2.4.3. Atribuţii şi obligaţii ale utilizatorilor reţelei *UAV*

Utilizatorii reţelei *UAV* pot fi cadre didactice, cercetători, personal administrativ, studenţi, doctoranzi sau colaboratori ai UAV care solicită calitatea de utilizator.

Utilizatorii standard nu au drept de administrare a reţelei şi pot folosi numai acele RIC pentru care sunt autorizaţi, indiferent dacă sunt resurse locale sau resurse accesibile în Internet.

Atribuţiile şi obligaţiile utilizatorilor sunt următoarele:

- Să cunoască şi să respecte prevederile politicii de securitate a RIC ;
- Să cunoască şi să respecte prevederile tuturor regulilor şi procedurilor privind securitatea RIC
- Să răspundă direct de securitatea şi conţinutul informaţiilor şi resursele informatice şi de comunicaţii încredinţate direct sau indirect.

2.4.4. Alte atribuţii

Toţi partenerii UAV (furnizori, agenţi, colaboratori etc.) trebuie să accepte şi să respecte politica de securitate, precum şi regulile specifice privind utilizarea şi securitatea Resurselor Informatice şi de Comunicaţii ale *UAV*.

2.5. Prevederi pentru asigurarea integrităţii, confidenţialităţii şi disponibilităţii informaţiei în utilizarea Resursele Informatice şi de Comunicaţii ale UAV

Politica de securitate a UAV impune dezvoltarea, gestionarea şi punerea în practică de proceduri şi/sau reguli specifice care să asigure integritatea, confidenţialitatea şi disponibilitatea informaţiei în utilizarea RIC. Toate procedurile şi/sau regulile aplicabile în sistemul Resurselor Informatice şi de Comunicaţii ale *UAV* fac parte din Planul de Securitate *(vezi capitolul 3)* şi sunt obligatorii pentru toţi utilizatorii.

Întreg personalul este responsabil privind modul de utilizare a RIC şi nu trebuie să facă abuz de privilegii; fiecare utilizator este direct responsabil pentru acţiunile care pot afecta securitatea Resurselor Informatice şi de Comunicaţii.

Utilizatorii sunt responsabili nediscriminatoriu privind raportarea oricărei suspiciuni sau confirmări de încălcare a politicii de securitate.

Nu există nicio asigurare a confidenţialităţii datelor personale sau a accesului la informaţii folosind protocoale de genul, dar nu numai, mesagerie electronică, navigare Web, conversaţii telefonice, 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.

Departamentele şi facultăţile sunt responsabile de autorizarea utilizatorilor pentru folosirea adecvată a RIC.

Orice informaţie folosită în sistemul RIC 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.

Toate programele de calculator, aplicaţiile, codul sursă, codul obiect, documentaţia şi datele sunt proprietatea Universităţii şi trebuie să fie protejate.

Departamentele şi Facultăţile trebuie să ofere facilităţi corespunzătoare de control al accesului în scopul monitorizării RIC, 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.

Personalul trebuie să respecte prevederile Licenţelor si nu este permisă copierea ilegală a programelor comerciale. Compartimentul IT (C.I.R.P.I.), direct sau prin intermediul Departamentelor şi Facultăţilor, îşi rezervă dreptul de a şterge orice produs fără licenţă de pe orice sistem din cadrul Resurselor Informatice şi de Comunicaţii.

Compartimentul IT (C.I.R.P.I.), direct sau prin intermediul Departamentelor şi Facultăţilor, îşi rezervă dreptul de a şterge, de pe orice sistem, orice program sau fişier care nu are legătură cu scopul muncii respective.

Domeniul electronic *uav.ro* şi subdomeniile acestuia sunt gestionate de UAV ca domenii proprii, în conformitate cu înregistrarea corespunzătoare a UAV ca proprietar al acestui domeniu la autoritatea românească în materie de nume de domenii (RNC). Drepturile de utilizare ale domeniului *uav.ro* sunt rezervate pentru UAV. Informaţiile publicate electronic de către UAV pe site-ul propriu www.uav.ro şi în subdomeniile acestuia sunt proprietate a UAV. Caracterul public al acestora reflectă faptul că ele sunt puse la dispoziţie de către UAV în beneficiul comunităţii publice, în scop de informare asupra programelor academice şi a activităţii UAV.

Informaţiile depuse pe site-urile publice ale facultăţilor / departamentelor UAV aparţin facultăţilor / departamentelor respective ca şi subunităţi organizatorice ale UAV. Orice utilizare a informaţiilor de pe site-urile publice ale UAV în domeniul *uav.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, UAV îşi rezervă dreptul de a solicita aplicarea prevederilor legale în vigoare.

Fişierele electronice create, trimise, primite sau stocate folosind Resursele Informatice şi de Comunicaţii administrate sau în custodia şi sub controlul UAV nu au caracter personal şi pot fi accesate oricând de către angajaţii autorizaţi din cadrul Compartimentul IT (C.I.R.P.I.), Departamente şi Facultăţi fără înştiinţarea utilizatorului.

În scopul administrării RIC şi pentru asigurarea securităţii acestora, personalul autorizat poate revizui sau utiliza orice informaţie stocată pe sau transportată prin sistemele Resurselor Informatice şi de Comunicaţii în conformitate cu legile în vigoare. În aceleaşi scopuri, este posibilă monitorizarea activităţii utilizatorilor (de exemplu: pagini web vizitate).

Utilizatorii trebuie să raporteze orice slăbiciune în sistemul de securitate al calculatoarelor din cadrul UAV, orice incident de posibilă întrebuinţare greşită sau încălcare a acestui regulament (prin contactarea Compartimentul IT (C.I.R.P.I.).

Un mare număr de utilizatori (inclusiv studenţi), pot accesa informaţii din exteriorul sistemului de comunicaţii al UAV. În aceste condiţii este obligatorie păstrarea confidenţialităţii informaţiilor transmise din exteriorul UAV şi a informaţiilor obţinute din interiorul instituţiei.

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

Niciun utilizator al Resurselor Informatice şi de Comunicaţii UAV nu poate divulga informaţiile la care are acces sau la care a avut acces ca urmare a unei vulnerabilităţi a sistemelor ce compun Resursele Informatice şi de Comunicaţii. Această regulă se extinde şi după ce utilizatorul a încheiat relaţiile cu UAV.

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 UAV se transmit în aşa fel încât să se asigure confidenţialitatea şi integritatea acestora.

Capitolul 3. PLANUL DE SECURITATE

3.1. Introducere

Planul de securitate conţine toate regulile şi procedurile aplicabile în sistemul Resurselor Informatice şi de Comunicaţii a *UAV.*

Acestea sunt elaborate pentru a stabili un cadru corect, legal şi eficient de utilizare a tehnologiei informaţiei şi comunicaţiilor în UAV.

3.2. Scop

În acord cu legislaţia în vigoare în România şi Regulamentele de ordine interioară ale UAV, Resursele Informatice şi de Comunicaţii sunt valori ale Universităţii care trebuie exploatate şi administrate ca resurse publice în proprietatea statului român.

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 Universităţii 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, studenţi, colaboratori etc.

Regulile *(vezi anexele prezentului Regulament)* 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

Regulile şi procedurile din planul de securitate au rolul:

- de a fi corecte, echitabile şi eficiente pentru folosirea RIC în vederea sprijinirii procesului educaţional şi al cercetării ştiinţifice.
- de a educa utilizatorii RIC în ceea ce priveşte responsabilităţile asociate cu utilizarea acestora.
- de a fi compatibile cu regulamentele, statutul şi atribuţiile stabilite pentru administrarea resurselor informatice şi de comunicaţii.

3.3. Audienţă

Regulile de utilizare a Resurselor Informatice şi de Comunicaţii ale UAV se aplică nediscriminatoriu tuturor persoanelor cărora li s-a permis accesul la acestea.

Capitolul 4. MĂSURI DISCIPLINARE

Administratorul reţelei *UAV* 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 *UAV.*

În situaţii cu totul deosebite, când eventuale acţiuni ale unor utilizatori care, pe proprie răspundere, atentează grav la securitatea reţelei *UAV,* se pot lua următoarele măsuri:

- rezilierea contractului de muncă în cazul angajaţilor;
- încetarea relaţiilor contractuale (de colaborare) în cazul contractanţilor, furnizorilor sau consultanţilor;
- suspendarea sau exmatricularea în cazul studenţilor;

Toate acţiunile care contravin legilor vor fi raportate organelor competente.

Capitolul 5. REFERINŢE

- RFC 1244 - Site Security Handbook: www.ietf.org/rfc/rfc1244.txt ;
- *Legea republicată nr.455* din 30 aprilie 2014 din MO 316 privind semnătura electronică;
- *Legea nr. 544* din 12 octombrie 2001 cu modificările și completările ulterioare privind liberul acces la informaţiile de interes public.
- *Hotărârea nr. 1259* din 13 decembrie 2001 modificată prin *Hotărârea nr. 2303* din 30 decembrie 2004 privind aprobarea Normelor tehnice şi metodologice pentru aplicarea *Legii nr. 455* din 2001 cu modificările și completările ulterioare privind semnătura electronică;
- *Hotărârea nr. 781* din 25 iulie 2002 privind protecţia informaţiilor secrete de serviciu;
- *Legea nr. 182* din 12 aprilie 2002 cu modificările și completările ulterioare privind protecţia informaţiilor clasificate;

- *Legea nr. 161* din 19 aprilie 2003 cu modificările și completările ulterioare privind unele măsuri pentru asigurarea transparenţei în exercitarea demnităţilor publice, a funcţiilor publice şi în mediul de afaceri, prevenirea şi sancţionarea corupţiei.

Capitolul 6. DISPOZIŢII FINALE

Regulamentul va fi disponibil în format electronic pe site-ul web al UAV şi la Compartimentul IT (C.I.R.P.I.). Se recomandă ca acest document să fie disponibil sau să se facă trimitere la acesta de pe toate site-urile web din cadrul UAV.

Prezentul document va conţine informaţii de identificare proprii şi se va specifica data la care a fost aprobat şi data de la care intră în vigoare.

Modificarea prevederilor Regulamentului se face numai cu aprobarea conducerii UAV. Fiecare modificare a conţinutului va conduce la modificarea versiunii documentului şi a informaţiilor de identificare. Versiunea anterioară rămâne valabilă până în momentul în care noua versiune intră în vigoare.

Aprobat,
RECTOR
Prof.univ.dr. Ramona LILE

Vizat jurist,
Avocat Gianina IGNUŢA

IGNUŢA D. DACIANA GIANINA
Cabinet de Avocat
C.I.F. 33247199

Anexa 1

REGULI DE UTILIZARE
a Resurselor Informatice şi de Comunicaţii

A. Utilizarea permanentă a Resurselor Informatice şi de Comunicaţii\

- Utilizarea Resurselor Informatice şi de Comunicaţii se face numai în interes de serviciu.
- Utilizatorii trebuie să anunţe compartimentul IT (C.I.R.P.I.) atât despre orice problemă/breşă în sistemul de securitate din cadrul UAV, cât şi despre orice posibilă întrebuinţare greşită sau încălcare a regulamentelor în vigoare.
- Prin acţiunile lor, utilizatorii nu trebuie să încerce să compromită protecţia sistemelor informatice şi de comunicaţii şi nu trebuie să desfăşoare, deliberat sau accidental, acţiuni care pot afecta confidenţialitatea, integritatea şi disponibilitatea informaţiilor de orice tip.
- Utilizatorii nu trebuie să încerce să obţină acces la date sau programe din Resursele Informatice şi de Comunicaţii pentru care nu au autorizaţie sau consimţământ explicit.
- Utilizatorii nu trebuie să´divulge sau să înstrăineze nume de cont-uri, parole, Numere de Identificare Personală (PIN-uri), 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 si a dreptului de autor(copyright).
- Utilizatorii nu trebuie să utilizeze programe de tip shareware sau freeware, fără aprobarea compartimentului IT (C.I.R.P.I.).
- Utilizatorii nu trebuie: să se angajeze într-o activitate care ar putea hărţui sau ameninţa alte persoane; să degradeze performanţele sistemelor ce alcătuiesc Resursele Informatice şi de Comunicaţii; să împiedice accesul unui utilizator autorizat la Resursele Informatice şi de Comunicaţii; 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 sistemelor ce alcatuiesc Resursele Informatice şi de Comunicaţii. De exemplu, utilizatorii Universităţii „Aurel Vlaicu", nu trebuie să ruleze programe de decriptare a parolelor, de captură de trafic, de scanări ale reţelei sau orice alt program nepermis de regulamente.
- Resursele Informatice şi de Comunicaţii din cadrul Universităţii „Aurel Vlaicu", nu trebuie să fie folosite pentru beneficiul personal.
- Utilizatorii nu trebuie să acceseze, să creeze, să stocheze sau să transmită materiale din cadrul Universităţii „Aurel Vlaicu", care se poate considera ofensive, indecente sau obscene (altele decât cele în curs de cercetare academică unde acest aspect al cercetării are aprobarea explicită a conducerii Universităţii).

- Accesul la reţeaua Internet prin intermediul Resursele Informatice şi de Comunicaţii 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 Resursele Informatice şi de Comunicaţii ale Universităţii.
- Utilizatorii nu trebuie să se angajeze în acţiuni împotriva scopurilor Universităţii „Aurel Vlaicu" folosind Resursele Informatice şi de Comunicaţii.
- Nu este permisă trimiterea sau recepţionarea documentelor sau fişierelor care pot cauza acţiuni legale împotriva Universităţii „Aurel Vlaicu" sau prejudicierea, indiferent de formă, a intereselor Universităţii.
- Toate mesajele, fişierele şi documentele localizate în cadrul Resurselor Informatice şi de Comunicaţii sunt proprietatea Universităţii şi pot fi subiectul unor cereri de verificare/inspectare/accesare conform regulamentelor.

B. Utilizarea ocazională a Resurselor Informatice şi de Comunicaţii

În anumite situaţii este permisă utilizarea ocazională a Resurselor Informatice şi de Comunicaţii. 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 utillizatorii 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 Universitate;
- utilizarea ocazională a RIC nu trebuie să afecteze activitatea normală a angajaţilor.

Anexa 2

REGULI
privind Configurarea Sistemelor Informatice pentru Acces la Reţeaua de Comunicaţii

- Infrastructura de comunicaţii, reţeaua de comunicaţii digitale a Universităţii este administrată de către compartimentul IT (C.I.R.P.I.) care este responsabilă cu întreţinerea şi dezvoltarea acesteia.
- Pentru a furniza o infrastructură de comunicaţii unitară cu posibilităţi de modernizare toate componentele acesteia sunt instalate de către compartimentul IT (C.I.R.P.I.) sau de către un furnizor avizat . Toate echipamentele, fără excepţie, conectate la reţeaua de comunicaţii trebuie configurate conform specificaţiilor departamentului IT.
- Modificarea configuraţiei oricărui dispozitiv activ conectat la reţeaua de comunicaţii se face numai cu aprobarea compartimentului IT (C.I.R.P.I.).
- Adresele de reţea sunt alocate dinamic sau static numai de către compartimentul IT
- Toate conectările dintre reţeaua de comunicaţii a Universităţii şi alte reţele de comunicaţii, publice sau private, sunt responsabilitatea exclusivă a compartimentului IT (C.I.R.P.I.).
- Echipamentele de protecţie a reţelei de comunicaţie a Universităţii (firewall) se vor instala de către compartimentul IT (C.I.R.P.I.).
- Utilizarea sistemelor de protecţie (firewall) din Departamente şi Facultăţi nu este permisă fără autorizaţie din partea compartimentului IT (C.I.R.P.I.). Această restricţie se aplică şi în cazul în care se folosesc adrese private de reţea.
- Utilizatorii nu au dreptul să extindă sau să retransmită în niciun fel serviciile reţelei (este interzisă instalarea unui, fax, modem, router, switch, hub sau punct de acces la reţeaua Universităţii) fără aprobare din partea compartimentului IT (C.I.R.P.I.).
- Utilizatorilor li se interzice instalarea de dispozitive hardware de reţea sau programe care furnizează servicii de reţea fără aprobarea compartimentului IT (C.I.R.P.I.).
- Utilizatorilor nu le este permis accesul la dispozitivele hardware ale reţelei.

***Anexa* 3**

REGULI
de tratare a incidentelor de securitate

- În cazul incidentelor de securitate din UAV, membrii compartimentul IT (C.I.R.P.I.) au funcţii şi responsabilităţi predefinite care pot fi prioritare îndatoririlor obişnuite.
- Ori de câte ori un incident de securitate este suspectat sau confirmat (exemple: virus, vierme, descoperirea unor activităţi suspecte, informaţii modificate etc.), trebuie urmate procedurile standard specifice pentru micşorarea riscurilor.
- Compartimentul IT (C.I.R.P.I.) este responsabil cu înştiinţarea şi coordonarea pentru tratarea incidentului.
- Compartimentul IT (C.I.R.P.I.) este responsabil cu strângerea dovezilor fizice şi electronice ce vor face parte din documentaţia pentru tratarea incidentului.
- Folosind resurse tehnice speciale se va monitoriza nivelul daunelor şi gradul de eliminare sau atenuare a vulnerabilităţilor acolo unde este cazul.
- Compartimentul IT (C.I.R.P.I.) va stabili conţinutul comunicatelor pentru utilizatori privind incidentele şi va determina nivelul şi modul de distribuire a acestei informaţii.
- Compartimentul IT (C.I.R.P.I.) trebuie să comunice proprietarului sau producătorului resursei afectate de un incident informaţiile utile pentru eliminarea sau diminuarea vulnerabilităţilor care au cauzat incidentul.
- Compartimentul IT (C.I.R.P.I.) este responsabil cu documentarea anchetei privind incidental.
- Compartimentul IT (C.I.R.P.I.) este responsabil de coordonarea activităţilor de comunicare cu terţi pentru rezolvarea incidentului.
- În cazul în care incidentul nu implică acţiuni contrare legilor în vigoare Compartimentul IT (C.I.R.P.I.) va recomanda sancţiuni disciplinare.
- În cazul în care incidentul implică aplicarea legilor civile sau penale Compartimentul IT (C.I.R.P.I.) va recomanda sesizarea organelor în drept ale statului şi va acţiona ca ofiţer de legătură cu acestea.

***Anexa* 4**

REGULI
de monitorizare a Resurselor Informatice şi de Comunicaţii

Monitorizarea Resurselor Informatice şi de Comunicaţii (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 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 Universităţii. În această categorie
- intră următoarele (fără a se limita doar la acestea):
- Jurnale ale sistemelor de detectare 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.
- Compartimentul IT (C.I.R.P.I.) va efectua, în mod regulat (cel puţin o dată la şase luni),
- verificări pentru detectarea:
- Echipamentelor de reţea conectate neautorizat;
- Serviciilor de reţea neautorizate;
- Serverelor de pagini de web neautorizate;
- Echipamentelor ce utilizează resurse comune nesecurizate;
- Utilizării de modem-uri neautorizate;
- Licenţelor pentru sistemele de operare şi programele instalate.
- Orice neregulă privind respectarea regulamentelor de securitate va fi raportată către
- Compartimentul IT (C.I.R.P.I.) în scopul efectuării de investigaţii.

Anexa 5

REGULI
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.
- Înregistrările de verificare ale dispozitivelor de control al accesului trebuie monitorizate/revizuite (examinate) zilnic de către administratorul de sistem.
- Verificările privind integritatea fiecărui sistem trebuie să se facă periodic. Această activitate este obligatorie şi pentru dispozitivele de tip firewall sau dispozitive de control al accesului.
- Înregistrările de verificare pentru serverele şi host-urile din reţeaua internă trebuie revizuite cel puţin săptămânal.
- Se vor verifica periodic 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 Compartimentul IT (C.I.R.P.I.) .
- Utilizatorii sunt obligaţi să raporteze Compartimentul IT (C.I.R.P.I.) orice anomalii în performanţa sistemelor utilizate sau orice semne ale unor posibile infracţiuni.

***Anexa* 6**

REGULI
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 Resurselor Informatice şi de Comunicaţii trebuie să fie documentată şi periodic revizuită.
- Furnizorul care oferă servicii de stocare a copiilor de siguranţă în alte zone pentru Universitate trebuie să fie acreditat în acest scop de către o autoritate a statului.
- Procedurile stabilite între Universitate şi furnizorii de stocare a copiilor de siguranţă în altă zonă trebuie să fie revizuite cel puţin anual.
- Verificarea copiilor de siguranţă se va face după o procedură documentată şi revizuită
  periodic.
- Copiile de siguranţă trebuie să fie periodic testate pentru a asigura faptul că informaţiile stocate sunt recuperabile.
- Accesul la mediile de backup ale Universităţii stocate la furnizori externi sau în interior se va face folosindu-se proceduri specifice de acces. Acestea trebuie revizuite periodic (anual).

Anexa 7

REGULI
de securizare a serverelor

- Un server va fi conectat la rețeaua Universității numai dacă se află într-o stare sigură, acreditat de către Compartimentul IT (C.I.R.P.I.).
- Procedura de securizare a serverelor trebuie să includă, obligatoriu, următoarele:
  - Instalarea sistemului de operare dintr-o sursă aprobată;
  - Aplicarea patch-urilor furnizate de producător;
  - Inlăturarea programelor, a serviciilor sistem și a driverelor 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.
- Compartimentul IT (C.I.R.P.I.) va monitoriza în mod obligatoriu, procesul de instalare a serverelor principale (enterprise) și aplicarea regulată a patch-urilor de securitate. De asemenea, va monitoriza prin sondaj procesul de instalare și aplicarea regulată a patch-urilor de securitate pentru servere sau a grupurilor de lucru.

Anexa 8

REGULI
de monitorizare a Resurselor Informatice şi de Comunicaţii

Monitorizarea Resurselor Informatice şi de Comunicaţii (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 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 Universităţii. În această categorie intră următoarele (fără a se limita doar la acestea):

- Jurnale ale sistemelor de detectare 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.

Compartimentul IT (C.I.R.P.I.) va efectua, în mod regulat (cel puţin o dată la şase luni), verificări pentru detectarea:

- Echipamentelor de reţea conectate neautorizat;
- Serviciilor de reţea neautorizate;
- Serverelor de pagini de web neautorizate;
- Echipamentelor ce utilizează resurse comune nesecurizate;
- Utilizării de modem-uri neautorizate;
- Licenţelor pentru sistemele de operare şi programele instalate.

Orice neregulă privind respectarea regulamentelor de securitate va fi raportată către Compartimentul IT (C.I.R.P.I.) în scopul efectuării de investigaţii.

***Anexa* 9**

REGULI
privind detectarea viruşilor

- Toate staţiile de lucru de sine stătătoare sau conectate la reţeaua de comunicaţii a Universităţii, trebuie să utilizeze programe antivirus aprobate de către Compartimentul IT (C.I.R.P.I.). Programele antivirus nu trebuie dezactivate.
- Configuraţia programului antivirus trebuie să nu fie modificată într-un mod care să reducă eficacitatea programului.
- Frecvenţa actualizărilor automate a programului antivirus trebuie asigurată de către utilizator.
- Orice server de fişiere conectat la reţeaua instituţiei trebuie să utilizeze un program antivirus aprobat în scopul detectării şi curăţirii viruşilor care pot infecta fişierele puse la dispoziţie.
- Orice server sau gateway pentru e-mail trebuie să folosească un program antivirus pentru e-mail aprobat şi trebuie să respecte regulile de instalare şi de 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 Compartimentul IT (C.I.R.P.I.).

***Anexa* 10**

REGULI
privind securitatea informaţiilor în cazul utilizării calculatoarelor portabile

- Calculatoarele portabile trebuie să fie protejate prin parole.
- Se va evita stocarea datelor care privesc Universitatea pe dispozitivele portabile.
- În cazul în care nu există o altă alternativă de stocare locală, toate datele care privesc Universitatea trebuie criptate utilizând tehnici aprobate.
- Transmiterea datelor prin reţele de tip wireless se poate face numai prin reţelele instalate de către Compartimentul IT (C.I.R.P.I.); acestea vor utiliza tehnici de criptare pentru protejarea datelor transmise.
- Toate accesările de la distanţă a Resurselor Informatice şi de Comunicaţii trebuie să se efectueze prin intermediul serviciului autorizat, conform *Regulilor de acces la reţeaua de comunicaţii.*
- Conectarea sistemelor de calcul care nu sunt proprietatea Universităţii se face numai cu aprobarea scrisă a Compartimentul IT (C.I.R.P.I.), la recomandarea Departamentelor sau a Facultăţilor.

***Anexa* 11**

REGULI
de acces la reţeaua de comunicaţii

- Utilizatorilor le este permis să utilizeze numai parametrii pentru conectare la reţea specificaţi de către Compartimentul IT (C.I.R.P.I.).
- Accesul de la distanţă la reţeaua Universităţii se va realiza numai prin echipamente aprobate, sau prin intermediul unui Furnizor de Servicii Internet (Internet Service Provider (ISP)) agreat de către Universitate şi folosind protocoale aprobate de către Departamentul IT.
- Utilizatorii RIC din interiorul Universităţii nu se pot conecta la altă reţea.
- Utilizatorii nu trebuie să extindă sau să retransmită serviciile de reţea în niciun fel, pe nicio cale. Nu este permisă instalarea de conexiuni de reţea neautorizate indiferent de motiv. Autorizarea tuturor conexiunilor se face la propunerea Facultăţilor şi a Departamentelor de către Compartimentul IT (C.I.R.P.I.).
- Utilizatorii nu trebuie să instaleze echipamente hardware sau programe care furnizează servicii de reţea fără aprobarea Compartimentului IT (C.I.R.P.I.).
- Sistemele computerizate din afara Universităţii care necesită conectare la reţea trebuie să se conformeze cu standardele reţelei interne ale Universităţii.
- 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 Universităţii nu au dreptul să ruleze programe de spargere a parolei, sustragere de pachete, scanare a porturilor, în timp ce sunt conectaţi la reţeaua Universităţii.
- Utilizatorii nu au dreptul să modifice, reconfigureze, instaleze, dezinstaleze echipamente de reţea, cabluri, prize de conexiuni.
- Serviciul de nume şi administrarea adreselor IP sunt deservite exclusiv de către Compartimentul IT (C.I.R.P.I.).
- Serviciile de interconectare a reţelei Universităţii cu alte reţele sunt realizate exclusiv de către Compartimentul IT (C.I.R.P.I.).
- Nu este permisă instalarea şi/sau modificarea echipamentelor utilizate pentru conectare la reţea (inclusiv plăci de reţea) fără aprobarea Compartimentului IT (C.I.R.P.I.). Tipul şi modelul plăcilor de reţea şi tuturor echipamentelor care se pot conecta în reţea trebuie să fie aprobate de către Compartimentul IT (C.I.R.P.I.).

***Anexa* 12**

REGULI
de administrare a conturilor de email

- Fiecare cont de email creat pe domeniul *uav.ro* trebuie să aibă asociate o cerere şi o aprobare corespunzătoare.
- 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 *Regulile privind Parolele de Acces*
- Utilizatorilor **nu le este permis** să păstreze în directoarele proprii de pe server *(Inbox, Sent, Trash)* **mesaje mai vechi de 14 zile calendaristice.** Excepţie de la această regulă fac persoanele care au funcţii de conducere, precum şi cele din secretariate.
- 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.
- Regula de la punctul 5. nu se aplică pentru perioadele de vacanţă. Orice altă situaţie particulară (izolată) trebuie precizată Compartimentului IT (C.I.R.P.I.).

***Anexa* 13**

REGULI
pentru modificări şi modernizări ale Resurselor Informatice şi de Comunicaţii

Orice modificare asupra unei componente a Resurselor Informatice şi de Comunicaţii (RIC) din cadrul Universităţii (cum ar fi: sisteme de operare, componente hardware, echipamente şi componente de reţea, aplicaţii) trebuie să respecte regulile de mai jos:

- Toate modificările care afectează mediul de funcţionare a sistemelor componente ale RIC (ex: aparate de aer condiţionat,) trebuie să fie anunţate şi aprobate de către Departamentul sau Facultatea care administrează resursele afectate.
- Toate propunerile de modernizare şi extindere a elementelor de infrastructură a sistemului RIC vor fi documentate şi aprobate de către Compartimentul IT (C.I.R.P.I.). Nu este permisă modificarea de către utilizatori a elementelor de infrastructură a RIC.
- Modificările şi modernizările sistemelor de calcul vor fi documentate de către utilizator şi aprobate de către conducerea Departamentului sau Facultăţii.

***Anexa* 14**

REGULI
pentru modificări şi modernizări ale Resurselor Informatice şi de Comunicaţii

Orice modificare asupra unei componente a Resurselor Informatice şi de Comunicaţii (RIC) din cadrul Universităţii (cum ar fi: sisteme de operare, componente hardware, echipamente şi componente de reţea, aplicaţii) trebuie să respecte regulile de mai jos:

Toate modificările care afectează mediul de funcţionare a sistemelor componente ale RIC (ex: aparate de aer condiţionat, instalaţii de apă, încălzire, instalaţii electrice şi alarme) trebuie să fie anunţate şi aprobate în scris de către Departamentul sau Facultatea care administrează resursele afectate.
Toate propunerile de modernizare şi extindere a elementelor de infrastructură a sistemului RIC vor fi documentate şi aprobate de către Compartimentul IT (C.I.R.P.I.).
Nu este permisă modificarea de către utilizatori a elementelor de infrastructură a RIC.
Modificările şi modernizările sistemelor de calcul vor fi documentate de către utilizator şi aprobate de către conducerea Departamentului sau Facultăţii.
Orice cerere de modificare planificată trebuie să obţină o aprobare formală din partea Departamentului sau Facultăţii care administrează resursele supuse modificărilor.
Modificările planificate trebuie anunţate cu cel putin 48 ore înainte de a fi executate.
Cererile de modificare planificată pot fi respinse în următoarele cazuri: planificare inadecvată, planuri de refacere a serviciilor inadecvate, durata modificării poate afecta în mod negativ o activitate importantă a instituţiei sau resursele corespunzătoare necesare nu pot fi disponibile imediat.
Se va întocmi un raport pentru orice modificare, indiferent dacă a fost planificată sau neplanificată, sau dacă s-a realizat ori nu cu succes.
Trebuie întreţinută o bază de date care să cuprindă toate modificările. Aceasta trebuie să conţină cel puţin următoarele informaţii:

- data la care s-a făcut cererea pentru modificare şi data la care s-a făcut modificarea;
- informaţii de contact pentru utilizator;
- natura modificării;
- indicarea succesului sau nereuşitei modificării.