UNIVERSITATEA DE VEST
"VASILE GOLDIŞ"

ROMÂNIA
MINISTERUL EDUCAŢIEI
UNIVERSITATEA DE VEST „ VASILE GOLDIŞ" din ARAD
310025 Arad, România Bd. Revoluţiei nr. 94-96, tel./fax 0040/0257/280260,
e-mail: rectorat@uvvg.ro, web: www.uvvg.ro

NORME ŞI PROCEDURI PRIVIND APLICAREA POLITICILOR DE SECURITATE A SISTEMULUI DE RESURSE INFORMATICE ŞI DE COMUNICAŢII DIN CADRUL UNIVERSITĂŢII DE VEST "VASILE GOLDIŞ" DIN ARAD

Secţiunea 1. Preambul

Resursele informatice şi de comunicaţii din cadrul universităţii sunt bunuri strategice ale Universităţii de Vest „Vasile Goldiş" din Arad şi sunt parte integrantă a acesteia. Universitatea de Vest „Vasile Goldiş" din Arad a investit substanţial în resurse financiare şi umane pentru a putea crea acest sistem şi de aceea trebuie administrat ca atare. Compromiterea securităţii acestor resurse poate afecta capacitatea Universităţii de Vest „Vasile Goldiş" din Arad de a oferi servicii informatice şi de comunicaţii şi poate conduce la fraude, incidente legate de confidenţialitatea datelor cu caracter personal, la distrugerea datelor, la violarea clauzelor contractuale, divulgarea secretelor, la afectarea credibilităţii Universităţii în faţa partenerilor săi.

Reglementariile privind politica de securitate, normele şi procedurile de aplicareu au ca scop asigurarea integrităţii, confidenţialităţii şi disponibilităţii sistemelor informatice din cadrul Universităţii de Vest Vasile Goldis din Arad.

Confidenţialitatea se referă la protejarea datelor împotriva accesului neautorizat. Utilizatorul răspunde personal de confidenţialitatea datelor încredinţate prin procedurile de acces la Sistemele Informatice şi de Comunicaţii.

Integritatea se referă la măsurile şi procedurile utilizate împotriva modificărilor sau distrugerii neautorizate.

Disponibilitatea se asigură prin funcţionarea continuă a tuturor componentelor sistemelor informatice şi de comunicaţii. Sistemele informatice utilizate au nevoie de nivele diferite de disponibilitate în funcţie de impactul său daunele produse ca urmare a nefuncţionării corespunzătoare.

Pentru a oferi o protecţie cât mai bună infrastructurii IT în faţa acestor ameninţări, este necesară elaborarea de *normele de utilizare a Resurselor Informatice şi de Comunicaţii* (RIC) şi *procedurile de aplicare a politicilor de securitate RIC* . Acestea sunt elaborate pentru a stabili un cadru corect, legal şi eficient de utilizare a tehnologiei informaţiei şi comunicaţiilor în Universitatea de Vest „Vasile Goldiş" din Arad (UVVG).

Secţiunea 2. Scop

Prezentul document descrie aspecte ce au ca scop principal protejarea utilizatorilor împotriva atacurilor de orice tip (cu sau fără intenţie). De asemenea are ca scop protejarea imaginii Universităţii şi a investiţiilor acesteia pentru dezvoltarea sistemul informatic şi de comunicaţii. În acord cu legislaţia în vigoare în România, Resursele Informatice şi de Comunicaţii sunt valori ale Universităţii care trebuie exploatate şi administrate ca resurse publice în proprietatea universităţii.

Scopul acestor norme si proceduri este acela de a asigura:

- stabilirea unor reguli corecte, echitabile şi eficiente pentru folosirea resurselor informatice şi de comunicaţii în vederea sprijinirii procesului educaţional şi a cercetării ştiinţifice;
- protejarea imaginii Universităţii;
- protejarea investiţiilor Universităţii 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 administrativ, studenţi, colaboratori, etc.;
- educarea utilizatorilor RIC în ceea ce priveşte responsabilităţile asociate cu utilizarea acestora.

Secţiunea 3. Audienţă

Normele de utilizare a resurselor informatice şi de comunicaţii ale Universităţii de Vest "Vasile Goldiş" din Arad se aplică nediscriminatoriu tuturor persoanelor cărora li s-a permis accesul la acestea.

Secţiunea 4. Elaborarea, modificare şi aprobare a normelor de utilizare

a. Normele de utilizare a Resurselor Informatice şi de Comunicaţii ale Universităţii se elaborează pentru fiecare activitate specifică domeniului şi trebuie concepute în aşa fel încât fiecare să poată fi folosit cvasi-independent de celelalte.
b. Normele si procedurile vor fi elaborate de către Departamentul de Tehnologie a Informaţiei (DTI) şi vor fi propuse pentru aprobare conducerii Universităţii de Vest „Vasile Goldiş" din Arad.
c. Normele de utilizare a sistemului Resurselor Informatice şi de Comunicaţii vor fi disponibile în format electronic pe site-ul universităţii www.uvvg.ro şi/ sau pagina web a departamentului.
d. Modificarea prevederilor din prezentul document se face cu aprobarea conducerii Universităţii.
e. Prezentul document va fi conţine o listă a tuturor normelor aplicabile în sistemul Resurselor Informatice şi de Comunicaţii.

Secţiunea 5. Norme şi proceduri specifice

5.1. Norme privind utilizarea permanentă a Resurselor Informatice şi de Comunicaţii

a. Utilizatorii trebuie să anunţe DTI în cazul în care se observă orice problemă/breşă în sistemul de securitate a RIC din cadrul Universităţii cât şi orice posibilă întrebuinţare greşită sau încălcare a normelor în vigoare.
b. Este interzis utilizatorilor, ca prin acţiunile lor, 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 în cadrul sistemului RIC al Universităţii.
c. Este interzis utilizatorilor să încerce să acceseze date sau programe din RIC pentru care nu au autorizaţie sau consimţământ explicit.
d. Utilizatorii nu au dreptul 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.

e. Este interzis utilizatorilor să facă copii neautorizate sau să distribuie materiale protejate prin legile privind proprietatea intelectuală (copyright).
f. Utilizatorii nu au dreptul 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 respecte măsurile de securitate impuse prin normele în vigoare..
g. Este interzis utilizatorilor 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 prezentele norme.
h. RIC ale Universităţii nu trebuie folosite pentru beneficiul personal.
i. Accesul la reţeaua Internet prin intermediul RIC se supune aceloraşi regulii care se aplică utilizării din interiorul instituţiei şi Normelor privind utilizare Internet-ului şi Intranet-ului. Angajaţii nu au voie să permită membrilor familiei sau altor persoane accesul la RIC ale Universităţii.
j. Utilizatorii care au acces la sistemul RIC al Universităţii au obligaţia de a purta acte şi sau legitimaţii care să ateste calitatea de utilizator autorizat în spaţiile Universităţii
k. Este interzis utilizatorilor să se angajeze în acţiuni împotriva scopurilor Universităţii folosind RIC.
l. Utilizatorii nu au permisiunea de a utiliza reţeaua UVVG pentru a transmite, a copia, a posta, a distribui, a reproduce, a utiliza, a încărca sau a prelucra in orice alt mod materiale:
   - ilegale, obscene, vulgare, calomniatoare, ameninţătoare, abuzive, materiale care îndeamnă la ura rasiala, etnica sau sunt in orice alt mod defăimătoare;
   - pentru care nu are dreptul legal de transmitere, reproducere sau difuzare, sub orice sistem juridic, românesc sau străin;
   - care conţin viruşi sau orice alt tip de cod, fişiere, sau programe care sunt create să distrugă, întrerupă sau să limiteze funcţionarea oricărui alt software, componente hardware sau echipament de telecomunicaţii.
m. Utilizatorul nu are dreptul:
   - de a utiliza serviciul în scopul instigării la, lansării sau coordonării de atacuri informatice de orice tip împotriva oricărui sistem sau utilizator de Internet sau de pe alte reţele conectate sau nu la Internet, prin metode wired, wireless sau în alte tehnologii existente sau viitoare, incluzând, dar fără a se limita la atacuri Denial of Services (DoS) sau Distributed DoS, trimiterea de mesaje spam, furt de identitate electronica sau obţinerea de foloase necuvenite prin exploatarea vulnerabilităţilor sistemelor (phising, pharming, click fraud, spyware, keylogging, sniffing, etc.);
   - de a utiliza adresa de IP primită ca urmare a utilizării Serviciului, în programe rulate pe un calculator de orice tip cu scopul de a obţine informaţii/rapoarte de la alte calculatoare utilizate pentru scopuri ilegale, cum ar fi spamming sau alte acţiuni ilegale.
n. Pentru toate informaţiile, datele, programele, precum şi orice alte materiale incluzând, dar fără a se limita la muzică, sunet, fotografii, grafice, materiale video, mesaje, indiferent dacă au fost afişate în mod public sau transmise/accesate individual, prin intermediul serviciului, persoana care a fost sursa unor astfel de materiale este responsabilă. Ca urmare, utilizatorul este în întregime responsabil pentru toate materialele pe care le încarcă, reproduce, pune la dispoziţie în mod public.

5.2. Norme privind utilizarea ocazională a Resurselor Informatice şi de Comunicaţii

În anumite situaţii este permisă utilizarea ocazională a RIC. În aceste situaţii se aplică următoarele restricţii:

a. 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.
b. Utilizarea ocazională a RIC nu trebuie să aibă drept rezultate costuri directe pentru Universitate.
c. Utilizarea ocazională a RIC nu trebuie să afecteze activitatea normală a angajaţilor.
d. Nu este permisă trimiterea sau recepţionarea documentelor sau fişierelor care pot cauza acţiuni legale împotriva Universităţii sau prejudicierea, indiferent de formă, a intereselor Universităţii.

5.3. Norme privind confidenţialitatea serviciilor informatice şi de comunicaţii

a. Utilizatorii trebuie să raporteze orice slăbiciune în sistemul de securitate al calculatoarelor din cadrul Universităţii, orice incident de posibilă întrebuinţare greşită sau încălcare a normele de utilizare (prin contactarea DTI).
b. Un mare număr de utilizatori (inclusiv studenţi) pot accesa informaţii din exteriorul sistemului de comunicaţii al Universităţii. În aceste condiţii este obligatorie păstrarea confidenţialităţii informaţiilor transmise din exteriorul RIC şi a informaţiilor obţinute din interior.
c. Utilizatorii nu trebuie să încerce să acceseze informaţii sau programe de pe sistemele Universităţii pentru care nu au autorizaţie sau consimţământ explicit.
d. Nici un utilizator al sistemului RIC al Universităţii 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 Universitatea.
e. 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 Universităţii se transmit în aşa fel încât să se asigure confidenţialitatea şi integritatea acestora.

5.4. Norme privind accesul administrativ

a. Utilizatorii trebuie să cunoască şi să accepte toate normele privind securitatea RIC înainte de a li se permite accesul la un cont.
b. Utilizatorii care au conturi de acces administrativ trebuie sa aibă respecte instrucţiunile de administrare, documentare, instruire şi autorizare a conturilor.
c. 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 DTI.
d. 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.
e. Accesul administrativ trebuie să fie conform Normelor privind utilizarea parolelor de acces.
f. Parola pentru un cont cu acces privilegiat nu va fi utilizată de mai multe persoane decât cu acordul scris al DTI şi trebuie să fie schimbată atunci când persoana care utilizează acest cont îşi schimbă locul de muncă din cadrul Departamentului, Facultăţii sau a Universităţii, sau în cazul unei modificări a listei de personal ale terţilor (furnizor desemnat) în contractele cu Universitatea.
g. 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;
   - contul va fi şters atunci când nu mai este necesar.

5.5. Norme privind accesul fizic la RIC

a. Toate sistemele de securitate fizică (de exemplu: acces-control în clădire, sisteme pentru prevenirea incendiilor, etc.) a RIC trebuie să fie instalate în conformitate cu normele in vigoare
b. Toate încăperile în care sunt instalate RIC trebuie să fie protejate fizic, în funcţie de importanţa acestora şi tipul datelor vehiculate sau stocate.
c. Pentru fiecare încăpere în care sunt instalate echipamente esenţiale 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.
d. Personalul care are drepturi de acces trebuie să deţină legitimaţie de serviciu şi acte de identitate care să-i ateste calitatea.
e. Acordarea drepturilor de acces (folosind card-uri, chei, parole etc.) se face de către DTI sau, după caz, Departamentul sau Facultatea care utilizeaza încăperea şi resursele.
f. Nu este permis transferul dreptului de acces indiferent de motiv.
g. Cardurile şi/sau cheile de acces care nu mai sunt folosite trebuie predate Departamentului sau Facultăţii care le-a eliberat.
h. Pierderea sau furtul cardurilor şi/sau cheilor de acces trebuie raportate imediat Departamentului sau Facultăţii care le-a eliberat.
i. Cardurile şi/sau cheile nu trebuie să aibă informaţii de identificare, altele decât informaţia de contact necesară pentru returnare.
j. Accesul vizitatorilor în spaţiile protejate este permis, doar cu un însoţitor.
k. Fiecare Departament şi/sau Facultate 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.
l. Fiecare Departament şi/sau Facultate trebuie să anuleze drepturile de acces ale cardurilor şi/sau cheilor utilizatorilor care îşi schimbă locul de muncă din Universitate sau nu au relaţii contractuale cu Universitatea..

5.6. Norme privind accesul la reţeaua de comunicaţii

a. Utilizatorilor le este permis să utilizeze numai parametrii pentru conectare la reţea specificaţi de către DTI.
b. Departamentele şi Facultăţile trebuie să aprobe conectarea dispozitivelor de calcul la RIC ale Universităţii.
c. Conectarea sistemelor de calcul care nu sunt proprietatea Universităţii se face cu acordul DTI, Departamentelor sau Facultăţilor.
d. Accesul de la distanţă la reţeaua Universităţii se va realiza numai prin sistemele instalate în acest sens şi folosind protocoale aprobate de către DTI.
e. Utilizatorii RIC din interiorul Universităţii nu se pot conecta la altă reţea.
f. Utilizatorii nu trebuie să extindă sau să retransmită serviciile de reţea în nici un fel. Nu este permisă instalarea de conexiuni de reţea neautorizate indiferent de motiv.
g. Este interzis utilizatorilor să instaleze echipamente hardware sau programe care furnizează servicii de reţea fără aprobarea DTI.
h. Sistemele computerizate din afara Universităţii care necesită conectare la reţea trebuie să se conformeze cu standardele reţelei interne ale Universităţii.
i. 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.

j. Utilizatorii nu au dreptul să modifice, reconfigureze, instaleze, dezinstaleze echipamente de reţea, cabluri, prize de conexiuni.
k. Serviciul de nume şi administrarea adreselor IP sunt deservite exclusiv de către DTI.
l. Serviciile de interconectare a reţelei Universităţii cu alte reţele sunt realizate exclusiv de către DTI.
m. Nu este permisă instalarea şi/sau modificarea echipamentelor utilizate pentru conectare la reţea (inclusiv plăci de reţea) fără aprobarea DTI.

5.7. Norme privind configurarea sistemelor informatice pentru acces la reţeaua de comunicaţii

a. Infrastructura de comunicaţii, reţeaua de comunicaţii digitale, a Universităţii este administrată de către DTI, care este responsabil cu întreţinerea şi dezvoltarea acesteia.
b. Pentru a furniza o infrastructură de comunicaţii unitară cu posibilităţi de modernizare toate componentele acesteia sunt instalate de către DTI sau de către un furnizor avizat explicit de către DTI.
c. Toate echipamentele, fără excepţie, conectate la reţeaua de comunicaţii trebuie configurate conform specificaţiilor DTI.
d. Modificarea configuraţiei oricărui dispozitiv activ conectat la reţeaua de comunicaţii se face numai cu aprobarea DTI.
e. Infrastructura de comunicaţii de date a Universităţii 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 DTI.
f. Adresele de reţea sunt alocate dinamic sau static numai de către DTI.
g. Toate conectările în reţeaua de comunicaţii a Universităţii sunt responsabilitatea DTI, conectarea se va face în baza unei cereri aprobată de către Departament sau Facultate şi de către conducerea Universităţii.
h. Echipamentele de protecţie a reţelei de comunicaţie a Universităţii (firewall) se vor instala de către DTI.
i. Utilizarea sistemelor de protecţie (firewall) din Departamente şi Facultăţi nu este permisă fără autorizare din partea DTI. Această restricţie se aplică şi în cazul în care se folosesc adrese private de reţea.
j. Utilizatorii nu au dreptul să extindă sau să retransmită în nici un fel serviciile reţelei (este interzisă instalarea unui modem, router, switch, hub sau punct de acces la reţeaua Universităţii) fără aprobare din partea DTI.
k. Utilizatorilor li se interzice instalarea de dispozitive hardware de reţea sau programe care furnizează servicii de reţea fără aprobarea DTI.
l. Utilizatorilor nu le este permis accesul la dispozitivele hardware ale reţelei.

5.8. Norme privind tratare a incidentelor de securitate

a. În cazul incidentelor de securitate din Universitate, membrii DTI au funcţii şi responsabilităţi predefinite care pot fi prioritare îndatoririlor obişnuite.
b. Ori de câte ori un incident de securitate este suspectat sau confirmat, precum un virus, vierme, descoperirea unor activităţi suspecte, informaţii modificate etc., scopul principal va fi micşorarea riscurilor.
c. DTI este responsabil cu înştiinţarea şi coordonarea pentru tratarea incidentului.
d. DTI este responsabil cu strângerea dovezilor fizice şi electronice ce vor face parte din documentaţia pentru tratarea incidentului.
e. Folosind resurse tehnice speciale se va monitoriza nivelul daunelor şi gradul de eliminare sau atenuare a vulnerabilităţilor acolo unde este cazul.

f. DTI va stabili conţinutul comunicatelor pentru utilizatori privind incidentele şi va determina nivelul şi modul de distribuire a acestei informaţii.
g. DTI trebuie să comunice proprietarului sau producătorului resursei afectate de un incident informaţiile utile pentru eliminarea sau diminuarea vulnerabilităţilor care au cauzat incidentul.
h. DTI este responsabil cu documentarea anchetei privind incidental.
i. DTI este responsabil de coordonarea activităţilor de comunicare cu terţi pentru rezolvarea incidentului.
j. În cazul în care incidentul nu implică acţiuni contrare legilor în vigoare DTI va recomanda sancţiuni disciplinare.
k. În cazul în care incidentul implică aplicarea legilor civile sau penale DTI va recomanda sesizarea organelor în drept ale statului şi va acţiona ca ofiţer de legătură cu acestea.

5.9. Norme privind monitorizarea RIC

a. Monitorizarea RIC se va face astfel încât să fie posibilă detectarea în timp util a atacurilor informatice şi a situaţiilor de încălcare a normelor de securitate. Echipamentele utilizate pentru monitorizare vor urmări şi înregistra la nevoie:
   - 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 de campus, 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).
b. Fişierele jurnal vor fi examinate regulat în vederea detectării eventualelor atacuri informatice şi abateri de la normele de securitate ale Universităţii. În această categorie intră următoarele (fără a se limita doar la acestea):
   - jurnale ale sistemelor de detectarea automată a intruşilor;
   - jurnale firewall;
   - jurnale ale scanărilor;
   - jurnale ale erorilor din sisteme şi servere.
c. Periodic, sau în urma unor reclamaţii, DTI va acţiona in vederea detectării şi eliminării:
   - echipamentelor de reţea conectate neautorizat;
   - serviciilor de reţea neautorizate;
   - serverelor de pagini de web neautorizate;
   - echipamentelor ce utilizează resurse comune nesecurizate;
   - utilizării de modemuri neautorizate;
   - software nelicenţiat
d. Orice neregulă privind respectarea normelor de securitate va fi raportată către DTI în scopul efectuării de investigaţii.

5.10. Norme privind securizarea serverelor

a. Un server nu trebuie conectat la reţeaua Universităţii până când nu este verificat şi securizat de către DTI.
b. Securizarea 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 driver-lor 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.

c. Se vor utiliza sisteme de tip DDS (Intrusion Detection System) în scopul de a detecta tentativele de intruziune, asigurând o protecţie sporită prin diverse metode cum ar fi analiza automată a log-urilor cu blocarea accesului dinspre adresele IP care au demonstrat recent un comportament suspect sau verificarea integrităţii fişierelor din sistem şi avertizarea administratorului de sistem în situaţia în care sunt detectate modificări neaşteptate ale acestor fişiere.
d. Serviciile vor fi reconfigurate astfel încât să nu mai permită accese care presupun transmiterea în formă necriptată prin reţea a informaţiilor sensibile cum ar fi nume de utilizator şi parolă de acces, toate accesele urmând să aibă loc pe canale criptate (utilizând certificate digitale corespunzătoare), în scopul de a elimina posibilitatea ca aceste informaţii să fie capturate de un eventual agent software maliţios care, din diverse motive, a ajuns să fie activ în reţeaua locală.
e. DTI va monitoriza obligatoriu pentru serverele principale procesul de instalare şi aplicare regulată a patch-urilor de securitate şi, prin sondaj, pentru serverele departamentale sau a grupurilor de lucru.

5.11. Norme privind crearea şi utilizarea copiilor de siguranţă (Backup)

a. Frecvenţa, dimensiunea şi conţinutul copiilor de siguranţă trebuie să fie în concordanţă cu importanţa informaţiei şi cu riscul acceptat de proprietarul datelor.
b. Procedura de creare a copiilor de siguranţă şi de recuperare pentru fiecare sistem din cadrul RIC trebuie să fie documentată.
c. Copiile de siguranţă trebuie să fie periodic testate pentru a asigura faptul că informaţiile stocate sunt recuperabile.
d. Accesul la mediile de *backup* ale Universităţii stocate la furnizori externi sau în interior se va face conform Normelor privind accesul fizic la RIC. Accesul trebuie interzis pentru persoanele autorizate care îşi schimbă locul de muncă.

5.12. Norme privind detectarea accesului neautorizat

a. 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).
b. Trebuie activate funcţiile de anunţare a persoanelor responsabile oferite de firewall-uri şi sistemele de control al accesului la reţea.
c. Trebuie activate funcţiile de înregistrare a evenimentelor pe dispozitivele firewall şi pe toate sistemele de control al accesului.
d. Înregistrările de verificare ale dispozitivelor de control al accesului trebuie monitorizate/revizuite (examinate) zilnic de către administratorul de sistem.
e. 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.
f. Înregistrările de verificare pentru serverele şi host-urile din reţeaua internă trebuie revizuite cel puţin săptămânal.
g. Se vor verifica periodic programele utilitare pentru detectarea tentativelor de acces neautorizat.
h. Toate rapoartele privind incidentele trebuie revizuite în vederea detectării de indicii ce ar putea implica o activitate de acces neautorizat.
i. Toate indiciile suspecte sau confirmate de accesări sau încercări de accesare neautorizate trebuie raportate imediat către DTI.
j. Utilizatorii sunt obligaţi să raporteze orice anomalii în performanţa sistemelor utilizate cât şi orice semne ale unor posibile infracţiuni la DTI.

5.13. Norme privind securitatea informaţiilor în cazul utilizării calculatoarelor portabile

a. 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 parolate.
b. Transmiterea datelor prin reţele de tip wireless se poate face numai prin reţelele instalate de către DTI; acestea vor utiliza protocoale de criptare pentru protejarea datelor transmise.
c. Toate accesările de la distanţă a RIC trebuie să se efectueze prin intermediul serviciului autorizat conform Normelor privind accesului la Reţeaua de Comunicaţii.
d. Conectarea sistemelor de calcul care nu sunt proprietatea Universităţii se face respectând Normele privind accesul la Reţeaua de Comunicaţii.

5.14. Norme privind modificările şi modernizările RIC

a. Orice modificare asupra unei componente a RIC din cadrul Universităţii, cum ar fi: sisteme de operare, componente hardware, echipamente şi componente de reţea, aplicaţii, este supusă normelor si procedurilor de utilizare şi trebuie să urmeze aspectele în vigoare.
b. 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 de către Departamentul sau Facultatea care administrează resursele afectate.
c. Toate propunerile de modernizare şi extindere a elementelor de infrastructură a sistemului RIC vor fi supuse documentării către DTI şi Departamentului administrativ al UVVG. Nu este permisă modificarea de către utilizatori a elementelor de infrastructură a RIC.

5.15. Norme privind utilizare reţelei Internet şi Intranet

a. Programele pentru acces la reţeaua Internet sunt destinate utilizatorilor autorizaţi pentru a fi folosite în scopuri academice şi de cercetare.
b. Toate programele utilizate pentru acces la reţeaua Internet trebuie să facă parte din pachetul de programe aprobat de către DTI. Aceste programe trebuie să includă toate patch-urile de securitate puse la dispoziţie de către producător.
c. 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.
d. Toate programele pentru acces Internet/Intranet trebuie să permită folosirea sistemelor proxy şi/sau firewall.
e. Toate informaţiile accesate în reţeaua Internet trebuie să se conformeze Normelor privind utilizarea permanentă a Resurselor Informatice şi de Comunicaţii.
f. Orice activitate a utilizatorilor folosind RIC poate fi înregistrată şi ulterior examinată.
g. Conţinutul tuturor site-urilor web ale Universităţii trebuie să se conformeze Normelor privind utilizarea permanentă a Resurselor Informatice şi de Comunicaţii şi să folosească numele de domeniu al Universităţii (uvvg.ro).
h. Nu este permisă utilizarea RIC ale Universităţii în scop personal sau pentru solicitări personale ce nu au legătură cu Universitatea.
i. Cumpărăturile pe Internet care nu au legătură cu atribuţiile de serviciu sunt interzise. Cumpărăturile în interes de serviciu se vor supune regulilor de achiziţie ale Universităţii.
j. Fişierele electronice se supun aceloraşi reguli de păstrare ce se aplică şi altor documente şi trebuie păstrate în conformitate cu regulile stabilite prin prezentele norme şi regulamentele proprii fiecărui Departament sau Facultate.

5.16. Norme privind managementul paginilor web

a. Prezentarea Universităţii de Vest „Vasile Goldis" din Arad pe web se face exclusiv pe site-ul www.uvvg.ro, pe care îl denumim pagină web oficială a Universităţii de Vest „Vasile Goldiş" din Arad. Aceasta poate conţine legături (link-uri) către alte pagini de web ale unor structuri ale universităţii, în condiţiile prezentate in acest document.
b. Paginile web sunt găzduite de serverele UVVG, serverelor dedicate pentru acest scop.
c. Toate paginile web proprii şi domeniile structurilor UVVG, stocate pe serverele UVVG sau externe, vor putea fi accesate direct de pe pagina oficială a UVVG sau din pagini cu link-uri succesive dependente de pagină web UVVG.
d. Serverele UVVG nu vor găzdui sau stoca pagini personale angajaţilor sau studenţilor UVVG, cu excepţia celor solicitate de conducerea universităţii.
e. Responsabilitatea administrării paginii web oficiale a UVVG revine Departamentul de Tehnologie a Informaţiei, în speţă persoanei desemnate prin fişa postului.
f. În cazul organizării de diferite manifestări culturale, ştiinţifice etc., orice structură a UVVG va colabora cu responsabilul cu întreţinerea conţinutului paginii www.uvvg.ro pentru includerea evenimentului şi pe pagina oficială a universităţii, având în prealabil aprobarea rectorului / prorectorului desemnat.
g. Caracterul informaţiilor scrise şi multimedia nu va încălca reglementările legale în vigoare:
   - sunt interzise informaţiile scrise şi multimedia care îndeamnă la desfăşurarea activităţilor de organizare şi propagandă politică;
   - se interzice prozelitismul religios;
   - sunt interzise informaţiile scrise şi multimedia care încalcă normele generale de moralitate sau care primejduiesc sănătatea fizică sau psihică a tineretului;
   - informaţiile postate pe Internet vor respecta prevederile legale privind accesul liber la informaţiile de interes public;
   - sunt interzise informaţiile multimedia care încalcă reglementările în vigoare privind drepturile de autor.
h. Conţinutul şi grafica paginilor web proprii diferitelor structuri ale UVVG va respecta o linie strict academică. Scopul paginilor va fi de a promova activitatea de bază a structurii, fiind interzisă alocarea de spaţiu publicitar pe pagina proprie.
i. Responsabilitatea pentru conţinutul publicat pe pagină web proprie revine în exclusivitate structurii care administrează pagina.

5.17. Norme privind administrarea conturilor de e-mail

a. Toate conturile utilizator se vor crea după un anumit format.
b. Crearea conturilor se face in urma existenţei unei cereri in acest sens.
c. Toţi utilizatorii sunt obligaţi să păstreze confidenţialitatea informaţiilor privind contul de acces.
d. Toate conturile trebuie să se poată identifica în mod unic, utilizând numele de cont asociat.
e. Toate parolele pentru conturi trebuie să fie create şi folosite în conformitate cu Normele privind parolele de acces.
f. DTI trebuie să aibă o documentaţie de modificare a conturilor utilizator pentru a se pune de acord în situaţii precum schimbări ale numelor de familie, modificări privind contul (numele contului) modificări ale drepturilor de utilizator.
g. DTI trebuie să furnizeze o listă cu toţi utilizatorii (listă de conturi) pentru sistemele pe care le administrează, la cererea conducerii autorizate din Universitate.

5.18. Norme privind parolele de acces

a. Toate parolele trebuie să îndeplinească următoarele condiţii:

- să fie schimbate de utilizator în mod regulat, cel puţin o dată la 90 de zile;
- să aibă o lungime minimă de 5 caractere;
- să fie parole cât mai complexe;
- reutilizarea parolelor este interzisă;
- parolele stocate trebuie criptate;
- parolele de cont utilizator nu trebuie divulgate nimănui.

b. Dispozitivele de securitate (ex. card acces) trebuie returnate după terminarea relaţiilor cu Universitatea.
c. Dacă se suspectează că o parolă a putut fi divulgată aceasta trebuie schimbată imediat.
d. Administratorii de sistem nu trebuie să permită schimbarea parolelor utilizatorilor folosind contul administrativ.
e. 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.
f. Procedurile de schimbare a parolei asistate de administratorul de sistem trebuie să respecte următoarele aspecte:

- utilizatorul se va legitima, administratorul va verifica drepturile de acces a persoanei la contul utilizator;
- se va genera o parolă care va fi comunicată utilizatorului;
- utilizatorul va schimba parola temporară, comunicată anterior, în maxim 24 ore.

5.19. Norme privind sistemul de mesagerie electronică

a. Următoarele activităţi sunt interzise:
   - 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.
b. 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.
c. Toate informaţiile şi datele confidenţiale ale Universităţii, transmise către alte reţele externe, trebuie să respecte Normele privind Confidenţialitatea Serviciilor Informatice şi de Comunicaţii.
d. Toate activităţile utilizatorilor ce implică accesul şi/sau folosirea RIC ale Universităţii pot fi oricând înregistrate şi analizate.
e. Utilizatorii serviciilor de mesagerie electronică nu trebuie să dea impresia că reprezintă, că îşi spun opinia sau dau declaraţii în numele Universităţii cu excepţia situaţiilor în care aceştia sunt autorizaţi în mod corespunzător să facă acest lucru. Atunci când este cazul, se va include o declaraţie explicită prin care utilizatorul specifică faptul că nu reprezintă Universitatea.

5.20. Norme privind detectarea şi eliminarea virusilor

a. Toate staţiile de lucru de sine stătătoare sau conectate la reţeaua de comunicaţii a Universităţii, trebuie să utilizeze programe antivirus aprobate de către DTI.

b. Programele antivirus nu trebuie dezactivate.
c. Configuraţia programului antivirus trebuie să nu fie modificată într-un mod care să reducă eficacitatea programului.
d. Frecvenţa actualizărilor automate a programului antivirus trebuie asigurată de către utilizator.
e. 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.
f. 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.
g. Orice virus care nu a putut fi înlăturat automat de către programul antivirus constituie un incident de securitate şi trebuie raportat imediat DTI.

5.21. Norme privind relaţiile cu terţi

a. Orice activitate desfăşurată de furnizor care implică acces la RIC trebuie să fie conforme cu normele în vigoare ale Universităţii.
b. În toate convenţiile şi contractele încheiate cu Furnizori trebuie specificate următoarele:
- informaţiile din cadrul Universităţii, 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 Universităţii aflate în posesia Furnizorului, la încheierea contractului.

c. Furnizorul trebuie să folosească sistemul RIC din cadrul Universităţii numai în scopul stipulat în contract.
d. Orice altă informaţie din sistemul RIC al Universităţii obţinută de Furnizor pe durata contractului nu poate fi folosită în interes propriu de către Furnizor sau divulgată altora.
e. Toate echipamentele de întreţinere ale Furnizorului, aflate în reţeaua internă a Universităţii şi care se pot conecta în exterior prin intermediul reţelei, a liniilor telefonice sau a liniilor închiriate, precum şi toate conturile de utilizator create temporar pentru Furnizor şi necesare pentru acces la RIC ale Universităţii, vor fi scoase din uz la încheierea relaţiilor contractuale.
f. Accesul Furnizorului trebuie să fie identificat în mod unic, iar administrarea parolelor sau metodele de autentificare trebuie să fie în conformitate cu Normele privind Parolele de Acces ale Universităţii şi Normele de Acces Administrativ.
g. Activităţile principale ale Furnizorului trebuie să fie documentate de acesta şi puse la dispoziţia conducerii Universităţii, la cerere. Acestea trebuie să cuprindă, dar să nu fie limitate la, evenimente precum: schimbări de personal, schimbări de parolă, schimbări majore în derularea proiectului, timpii de sosire, de plecare şi de livrare.
h. În cazul retragerii din contract a unui angajat al Furnizorului, indiferent de motiv, Furnizorul se va asigura că toate informaţiile sensibile sunt colectate şi predate Universităţii sau distruse în cel mult 24 de ore de la producerea evenimentului.
i. În cazul terminării/rezilierii contractului sau la cererea Universităţii, Furnizorul va preda sau distruge toate informaţiile ce aparţin Universităţii şi va oferi certificate în scris privind predarea sau distrugerea informaţiilor în decurs de 24 de ore de la producerea evenimentului.
j. În cazul încheierii contractului sau la cererea Universităţii, Furnizorul trebuie să predea imediat toate legitimaţiile, cartelele de acces, echipamentele şi stocurile Universităţii. Echipamentele şi/sau stocurile care urmează a fi reţinute de către Furnizor trebuie documentate şi autorizate de Conducerea Universităţii.

5.22. Procedură pentru alocarea de adrese de e-mail

Această procedură se adresează tuturor angajaților din UVVG care doresc un cont de e-mail pe serverul de mail al universității.

a. Toate cadrele didactice, toți doctoranzii, cercetătorii, precum și toți angajații care aparțin personalului administrativ, auxiliar didactic sau nedidactic au dreptul de a deține o adresă de email institutionala
b. Adresa de mail a unui angajat UVVG este recomandata sub forma nume.prenume@uvvg.ro dar la solicitare sunt posibile si alte combinatii in prefixul adresei.
c. Alocarea adresei de email se face in momentul angajarii informatiile necesare fiind transmise de Biroul Resurse Umane.
d. Emailul se poate verifica online pe https://portal.office.com sau instala pe orice device de tip desktop/mobil prin aplicatia Microsoft Outlook

5.23. Procedură pentru alocarea de subdomenii .uvvg.ro

Această procedură se adresează subunităților UVVG care doresc un subdomeniu de tip „.uvvg.ro" pentru găzduira unei pagini web sau pentru alte servicii Internet și prevede:

a. Consultarea responsabilului cu subdomeniile .uvvg.ro al Departamentul de Tehnologia Informației în vederea:
   - determinării unui subdomeniu disponibil dupa regulile de la punctul 3;
   - specificării unui server pe care va fi găzduit subdomeniul.
. Completarea formularului tip (Anexa 1) care trebuie semnat de către solicitant, coordonatorul Departamentul de Tehnologie a Informației și aprobat de Rectorul universității.
3. Reguli de alocare a subdomeniilor .uvvg.ro
   - Fiecare poate facultate/filiala centru poate avea propriul subdomeniu (ex. medicina.uvvg.ro)
   - Departamentele/Birourile/Serviciile pot avea alocat un subdomeniu propriu (ex: dti.uvvg.ro)
   - Centrele, institutele, extensiile, publicațiile care nu au un nume de domeniu pot solicita alocarea unui subdomeniu web, a cărui prefix va fi ales împreună cu solicitantul.

5.24. Procedură operațională solicitare înregistrări sistem supraveghere video

1.Prezenta procedură prezintă modul în care se fac solicitările pentru înregistrările sistemului de supraveghere video din cadrul UVVG.

2. Pentru a primi acces la înregistările sistemuluide supraveghere video,studentul/cadrul didactic /angajatul UVVG urmează următoarea procedură:

I. Solicitantul sesizează administratorul locației și completează cerere model menționând dată, ora și locul unde a avut loc evenimentul pentru care solicită acces la înregistrările sistemului de supraveghere video;
II. Solicitarea este analizată de administrator și:
   - dacă aceasta nu este întemeiată sau dacă în spațiul în care a avut loc evenimentul nu există camere de supraveghere video, refuză solicitarea, justificând refuzul;
   - • dacă solicitarea este întemeiată, îi pune la dispoziție solicitantului o cerere (Anexa 2) pe care acesta o completează și semnează.
III. Cererea este înaintata spre avizarea Directorului General Administrativ
IV. Directorul general administrativ:
   - • nu aprobă cererea, aceasta se întoarce la biroul administrator care notifica solicitantul cu privire la faptul că cererea nu a fost aprobată;
   - aprobă cererea și o trimite către Departamentul IT

V. Angajaţii DTI cauta în sistemele de supraveghere înregistrarea, este exportata şi predata administratorului

VI. Administratorul contactează solicitantul şi îi prezintă inregistrarea.

3. Toate solicitările se înregistrează şi îndosariază în cadrul Direcţiei General Administrativ UVVG

PREŞEDINTE SENAT,
Prof. univ. dr. Neli Kinga OLAH

Vizat COMISIA PENTRU CODURI, REGULAMENTE ŞI PROBLEME JURIDICE,
Preşedinte,
Conf. univ. dr. Daniela CREŢ

Anexa 1

Formular pentru alocarea de subdomenii .uvvg.ro

1. Numele entităţii solicitante (facultate, catedră, centru, department, institut, etc

_____

2. Motivul (scopul) cererii de subdomeniu

_____

3. Persoana responsabilă cu subdomeniul din partea entităţii solicitante
   a. Nume _____
   b. Funcţie _____
   c. Telefon _____
   d. Adresă mail (din .uvvg.ro) _____
   e. Semnătura _____

4. Numele subdomeniului negociat cu Departamentul de Tehnologie a Informaţiei conform "Procedurii pentru alocarea de subdomenii .uvvg.ro"

_____

5. Adresa IP a serverului unde va fi găzduit subdomeniul(daca este cazul) :
6. Data expirării domeniului (dacă este cazul):

Data: Semnătură solicitant:

Anexa 2

Solicitare înregistrări sistem supraveghere video

Domnule Director

Subsemnatul(a),_____, legitimat(ă) cu CI seria ___ nr. _____ angajat(ă)/student(ă) în cadrul_____ _____, cu funcția de_____ _____, vă rog să-mi aprobați accesul la înregistrările sistemului de supraveghere video din cadrul UVVG în care este surprins următorul eveniment: În data de ____/____/_____, ora/intervalul orar _____ _____ _____ _____ _____ _____ _____ _____ _____ _____

Data

_____

Semnătura

_____

AVIZAT ADMINISTRATOR

AVIZAT DIRECTOR GENERAL ADMINISTRATIV

AVIZAT DIRECTOR IT