Anexa 1 la Hotărârea Consiliului de administrație nr. 83 din 19 august 2024

Președintele Consiliului de administrație,

Prof. univ. dr. ing. habil. Marian BARBU

REGULAMENT

de utilizare a Rețelei pentru Comunicații Digitale și a calculatoarelor conectate la rețea din cadrul Universității „Dunărea de Jos" din Galați

2024

Universitatea „Dunărea de Jos" din Galați

Avertisment:

CUPRINS

LISTA ABREVIERILOR

UDJG – Universitatea „Dunărea de Jos" din Galați;

DIT – Direcția IT;

DFCTT – Departamentul de Formare Continuă și Transfer Tehnologic;

DPPD – Departamentul pentru Pregătirea Personalului Didactic;

ARNIEC/RoEduNet – Agenția de Administrare a Rețelei Naționale de Informatică pentru Educație și Cercetare;

UE – Uniunea europeană;

RCD – Rețeaua pentru Comunicații Digitale;

RRCD – Responsabilul cu funcționarea RCD;

RRCDD – Responsabilul cu funcționarea RCD nivel departamental;

SPEUDJ – Sistem de poștă electronică al Universității „Dunărea de Jos";

SGWUDJ – Sistemul de găzduire web al Universității „Dunărea de Jos";

SI – Sistem informațional;

DHCP – Dynamic HostConfiguration Protocol;

BOOTP – Bootstrap Protocol.

IP – Internet protocol;

IPv4 – Internet protocol versiunea 4;

VPN – Virtual Private Network;

MTA – Message Transfer Agent.

GDPR – Regulamentul UE privind protecția datelor (UE) 2016/679 („GDPR") este un regulament al legislației UE privind protecția datelor și viața privată a tuturor persoanelor din Uniunea Europeană (UE) și Spațiul Economic European (SEE). Se referă, de asemenea, la exportul de date cu caracter personal în afara zonelor UE și SEE.

CAPITOLUL I – INTRODUCERE ȘI ASPECTE LEGISLATIVE

I.1 Introducere

În acord cu prevederile din prezentul document RCD reprezintă una din resursele strategice ale UDJG.

Rețeaua pentru Comunicații Digitale a UDJG constituie unul din principalele mijloace de exploatare a resurselor informatice. Aceasta include toate echipamentele, cablurile, canalele de cabluri, punctele de acces, punctele de distribuție și nodurile principale. Este important ca aceasta să se dezvolte controlat și continuu, iar dezvoltarea rețelei de comunicații să se facă având în vedere atât cerințele utilizatorilor privind furnizarea de servicii avansate și diferențiate, cât și cerințele privind securitatea întregului ansamblu.

Utilizarea inadecvată și compromiterea securității RCD poate afecta capacitatea DIT a Universității de a oferi servicii de comunicații digitale, poate conduce la fraude sau distrugerea datelor, violarea clauzelor contractuale, divulgarea secretelor, afectarea credibilității Universității în fața partenerilor săi.

Acest regulament este stabilit astfel încât:

a) să fie în conformitate cu statutul, regulamentele, legile și alte documente oficiale în vigoare privind administrarea resurselor informatice publice,
b) să instruiască utilizatorii care au dreptul de folosire a RCD a UDJG privind responsabilitățile asociate unei astfel de utilizări.

I.2 Scop

Scopul prezentului regulament este acela de a asigura:

a) stabilirea unor reguli corecte, echitabile și eficiente pentru folosirea resurselor oferite de RCD a UDJG, în vederea sprijinirii procesului educațional și a cercetării științifice;
b) protejarea imaginii UDJG;
c) protejarea investițiilor UDJG pentru dezvoltarea unei rețele proprii pentru comunicații digitale;
d) protejarea proprietății intelectuale și a tuturor informațiilor stocate și transportate folosind RCD ale utilizatorilor autorizați: cadre didactice, personal administrativ, studenți, colaboratori etc.;
e) educarea utilizatorilor RCD în ceea ce privește responsabilitățile asociate cu utilizarea acestora;
f) compatibilitatea cu regulamentele, statutul și atribuțiile stabilite pentru administrarea resurselor informatice și de comunicații.

I.3 Audiență

Regulamentul de utilizare a Rețelei de Comunicații digitale și a calculatoarelor conectate la rețea din cadrul UDJG se aplică nediscriminatoriu tuturor persoanelor cărora li s-a permis accesul la orice resursă implicată în procesul de comunicații digitale în cadrul UDJG.

Următoarele entități și utilizatori sunt vizați în mod distinct de prezentul Regulament:

- angajații cu contract de muncă pe perioadă determinată sau nedeterminată care au acces la RCD;
- colaboratorii UDJG care au acces la RCD;
- studenții UDJG;
- alte persoane, entități sau organizații care au acces la RCD.

I.4 Aspecte legislative

- Prezentul regulament este realizat în conformitate cu legile în vigoare și are la bază următoarele legi, regulamente și referințe:
- Legea nr. 161 din 19 aprilie 2003 privind unele măsuri pentru asigurarea transparenței în exercitarea demnităților publice, a funcțiilor publice și în mediul de afaceri, prevenirea și sancționarea corupției, cu actualizările și modificările ulterioare;
- Legea nr. 506/2004 privind prelucrarea datelor cu caracter personal și protecția vieții private în sectorul comunicațiilor electronice;
- Legea nr. 129/2018 pentru modificarea și completarea Legii nr. 102/2005 privind înființarea, organizarea și funcționarea Autorității Naționale de Supraveghere a Prelucrării Datelor cu Caracter Personal;
- Legea nr. 455 din 18 iulie 2001 privind semnătura electronică, cu actualizările și modificările ulterioare;
- Legea nr. 544 din 12 octombrie 2001 privind liberul acces la informațiile de interes public, cu actualizările și modificările ulterioare;
- Hotărârea nr. 1259 din 13 decembrie 2001 privind aprobarea Normelor tehnice și metodologice pentru aplicarea Legii nr. 455-2001 privind semnătura electronică, cu actualizările și modificările ulterioare;
- Decizia nr. 99/2018 privind încetarea aplicabilității unor acte normative cu caracter administrativ emise în aplicarea Legii nr. 677/2001 pentru protecția persoanelor cu privire la prelucrarea datelor cu caracter personal și libera circulație a acestor date;
- HG nr. 781 din 25 iulie 2002 privind protecția informațiilor secrete de serviciu, cu actualizările și modificările ulterioare;
- Legea nr. 182 din 12 aprilie 2002 privind protecția informațiilor clasificate, cu actualizările și modificările ulterioare;
- Legea nr. 362/2018 privind asigurarea unui nivel comun ridicat de securitate a rețelelor și sistemelor informatice, cu actualizările și modificările ulterioare;
- Regulamentul de Organizare și Funcționare al Agenției ARNIEC/RoEduNet (Agenția de Administrare a Rețelei Naționale de Informatică pentru Educație și Cercetare) la care este afiliată UDJG;
- Legea nr. 64/2004 - pentru ratificarea Convenției Consiliului Europei privind criminalitatea informatică, adoptată la Budapesta la 23 noiembrie 2001, cu modificările și completările ulterioare;
- Directiva 2013/40/UE a Parlamentului European și a Consiliului din 12 august 2013 privind atacurile împotriva sistemelor informatice și de înlocuire a Deciziei-cadru 2005/222/JAI a Consiliului;
- Definiția sistemului informatic art. 35 din Legea 161/2003, art. 181 alin 1 Cod Penal, cu actualizările și modificările ulterioare;
- Definiția datelor informatice în Legea 455/2001,modificată prin Legea nr. 187/2012 pentru punerea în aplicare a Legii nr. 286/2009 privind Codul penal și completat de Ordonanța de urgență nr. 39/2020 pentru completarea Legii nr. 455/2001 privind semnătura electronică;

- EU Cybersecurity Act, Regulamentul (UE) 2019/881 al Parlamentului European și al Consiliului din 17 aprilie 2019 privind ENISA (Agenția Uniunii Europene pentru Securitate Cibernetică) și privind certificarea securității cibernetice pentru tehnologia informației și comunicațiilor, cu actualizările și modificările ulterioare;
- Directiva (UE) 2016/1148 a Parlamentului European și a Consiliului din 6 iulie 2016 privind măsuri pentru un nivel comun ridicat de securitate a rețelelor și a sistemelor informatice în Uniune (Legea 362/201,cu actualizările și modificările ulterioare);
- Legea nr. 190 din 18 iulie 2018 privind măsuri de punere în aplicare a Regulamentului (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor) din 27 aprilie 2016,cu actualizările și modificările ulterioare;
- Referințele la hărțuirea și violența cibernetică din Legea nr. 217 din 22 mai 2003 modificată prin Legea nr. 146/2021 privind monitorizarea electronică în cadrul unor proceduri judiciare și execuțional penale pentru prevenirea și combaterea violenței domestice, cu actualizările și modificările ulterioare;
- Legea nr. 196/2003 modificată de Legea nr. 187/2012 pentru punerea în aplicare a Legii nr. 286/2009 privind Codul penal- privind prevenirea și combaterea pornografiei, cu actualizările și modificările ulterioare.

CAPITOLUL II – ORGANIZARE ȘI ATRIBUȚII

II.1 Definiții și organizare

Rețeaua pentru Comunicații Digitale (RCD): toate dispozitivele capabile să transmită, să stocheze, să administreze date electronice, incluzând, dar nu limitat la: mainframe-uri, servere, calculatoare personale, laptop-uri, notebook-uri, tablete, sisteme de procesare distribuită, resurse de telecomunicații, medii de rețea, telefoane, telefoane inteligente, faxuri, imprimante și alte accesorii, precum și orice alt dispozitiv/echipament electronic, indiferent de uz, care se conectează la rețea. La acestea se adaugă procedurile, echipamentul, facilitățile, programele și datele care sunt proiectate, construite, puse în funcțiune (operaționale) și menținute pentru a crea, colecta, înregistra, procesa, stoca, primi, afișa și transmite informația.

Responsabilul cu funcționarea RCD (RRCD): răspunde de funcționarea în bune condiții a RCD. Funcția RRCD este asumată de către directorul DIT.

Responsabilul cu funcționarea RCD nivel Departamental (RRCDD): persoana responsabilă de funcționarea subrețelelor RCD și de monitorizarea și implementarea controalelor de securitate și a procedurilor pentru RCD la nivelul unui Departament sau al unei Facultăți sau al unei Catedre. Acesta este desemnat de către conducătorul Departamentului / Facultății / Catedrei / Direcției / Serviciului / Compartimentului și transmisă către RRCD.

Entitate: orice formă organizatorică (compartimente, birouri, servicii, direcții, departamente, facultăți) din cadrul UDJG sau o entitate externă Universității aflată în relații contractuale cu Universitatea și conectată la RCD.

Sistem de poștă electronică al Universității „Dunărea de Jos" din Galați (SPEUDJ): sistem organizațional-tehnic care asigură schimbul electronic de corespondență între utilizatorii înregistrați în sistemul de poștă electronică, precum și între utilizatorii sistemului și alte persoane. Fiecărui utilizator înregistrat în SPEUDJ îi va fi atribuită o cutie poștală unică.

Sistemul de găzduire web al Universității „Dunărea de Jos" din Galați (SGWUDJ): ansamblul de sisteme și servicii destinate găzduirii site-urilor web ale entităților Universității.

Sistem informațional (SI): ansamblu de procedee și mijloace de colectare, prelucrare și transmitere a informației, necesar procesului de conducere a instituțiilor, ministerelor, etc.

Administrator: utilizator specializat în efectuarea unor operații tehnice sau manipularea unor echipamente.

Utilizator: o persoană, o aplicație automatizată sau proces utilizator autorizat de către UDJG, în conformitate cu procedurile și regulamentele în vigoare, să folosească resursele și serviciile oferite prin intermediul RCD.

Utilizator al SPEUDJ: o entitate sau angajat autentificat, care utilizează serviciile acestuia în scopuri de serviciu.

Furnizor: persoană fizică/juridică care oferă bunuri sau servicii UDJG în baza unui contract comercial sau de colaborare.

Active de rețea: echipamentele care conțin cel puțin o sursă de tensiune sau de curent, care poate furniza energie rețelei de calculatoare pe termen nedefinit (de exemplu switch, router, punct de acces la rețea fără fir, etc.).

Software rău intenționat (malware): orice formă ostilă, intruzivă sau supărătoare de software, cel mai des întâlnit fiind cel proiectat cu intenția de a extrage date dintr-un computer sau rețea de computere, sau de a le afecta funcționarea.

Virus: un program care se auto-atașează la un fișier executabil sau la o aplicație vulnerabilă și care generează efecte deranjante sau distructive. Un fișier virus se execută în momentul în care este accesat un fișier infectat.

Înșelătorie electronică (Phishing): activitate infracțională care constă în obținerea de date confidențiale, prin trimiterea de către atacator a unui mesaj electronic, în care utilizatorul este solicitat să ofere date confidențiale, cum ar fi date de acces pentru aplicații de tip bancar, folosind tehnici de manipulare a datelor identității unei persoane sau ale unei instituții.

Spam: mesaje e-mail nesolicitate, de obicei având conținut publicitar pentru produse și servicii dubioase, trimise unui număr mare de destinatari.

IP: un protocol prin care datele sunt trimise de la un calculator la altul prin intermediul Internetului. Fiecare calculator (cunoscut sub denumirea de „gazdă") are pe Internet cel puțin o adresă IP unică, care îl identifică între toate computerele din rețea. Alocarea adreselor IP nu este arbitrară; ea se face de către organizații însărcinate cu distribuirea de spații de adrese.

IPv4: versiunea a patra a standardului pentru comunicarea în Internet, în cadrul căruia adresa IP este reprezentată pe 32 de biți (de ex. 192.168.0.1).

DHCP: un protocol care permite unui server dintr-o rețea locală să atribuie adrese IP temporare unui computer sau altor dispozitive din rețea.

BOOTP: protocol de rețea de computere, utilizat în rețelele Internet Protocol (IP), pentru a atribui automat o adresă IP statică dispozitivelor de rețea de la un server de configurare.

VPN: rețea privată virtuală; un mijloc de accesare în siguranță a resurselor dintr-o rețea prin conectarea la un server de acces la distanță prin Internet sau altă rețea.

Proxy: un tip special de server care funcționează ca o legătură intermediară între o aplicație client (cum ar fi un browser web) și un server real.

Scor MTA: caracterizarea reputației agenților de transfer de e-mail (MTA), de către entități specializate, pentru a determina riscul de securitate în mesajele e-mail. În mod normal, MTA-urile primesc mesaje electronice de la alți clienți. Când un destinatar al unui mesaj nu este găzduit local, atunci mesajul va fi direcționat automat către următorul MTA.

II.2 Canale oficiale de comunicație cu DIT

Telefon: (0336) 130 121

E-mail: support.it@ugal.ro – suport tehnic RCD

support@ugal.ro – suport general, cu excepția suportului tehnic RCD (suport e-mail, funcționalități aplicații software, hosting și cloud)

Notă: vor fi ignorate mesajele recepționate din afara domeniului ugal.ro (ex: gmail, yahoo, hotmail etc.)

Proceduri: procedurile elaborate de către DIT se regăsesc pe website-ul UDJG: https://ugal.ro/informatii/organizare/serviciile-universitatii/directia-it/proceduri-dit.

În aceste proceduri sunt indicate modalitățile de interacțiune cu DIT.

II.3 Atribuții și responsabilități

Atribuțiile manageriale includ:

Persoanele care au funcții cu atribuții de management trebuie să se asigure că orice angajat sau entitate a UDJG respectă prevederile prezentului Regulament în cazul utilizării serviciilor oferite prin intermediul RCD.

Totodată, persoanele cu funcții de management, trebuie să respecte actualul regulament în deciziile privind sarcinile de lucru curente.

Atribuțiile DIT includ:

- elaborează și propune pentru aprobare Regulamentul și politicile de securitate a RCD;
- elaborează și propune modificări ale regulamentului și politicii de securitate a RCD;
- elaborează proceduri pentru gestionarea conturilor de utilizator RCD;
- gestionează și operează resursele RCD pentru asigurarea serviciilor specifice comunicațiilor de date în contextul utilizării acestora în scopuri academice (educaționale, culturale, științifice), administrative și/sau în scop personal necomercial;
- ia măsuri în cazul descoperirii oricărei utilizări neautorizate sau ilegale a resurselor RCD;
- ia măsuri de restricționare a accesului la resursele oferite de RCD asupra utilizatorilor care încalcă prevederile prezentului Regulament;
- tratează incidentele de securitate și cele generate de utilizarea inadecvată în scopul minimizării efectului distructiv al acestora asupra RCD.

Pentru asigurarea condițiilor optime de funcționare a RCD, DIT poate lua măsuri privind restricționarea accesului utilizatorilor la diverse resurse RCD care pot fi afectate prin utilizarea necorespunzătoare sau resurse externe care pot afecta funcționarea RCD.

Atribuții ale utilizatorilor:

- să cunoască și să respecte prevederile Regulamentului de utilizare a RCD;
- să utilizeze resursele oferite de RCD în mod egal și etic, pentru desfășurarea activității specifice și în scopuri academice (educaționale, culturale, științifice), administrative și/sau în scop personal necomercial adiacent activității specifice, cu respectarea legislației în vigoare.

Utilizatorul răspunde, ca urmare a activităților și acțiunilor sale, pentru orice utilizare neautorizată sau ilegală a resurselor RCD, precum și pentru prejudiciile aduse resurselor RCD.

Alte atribuții:

Toți partenerii UDJG (furnizori, agenți, colaboratori etc.) trebuie să accepte și să respecte prezentul document și regulamentele specifice privind utilizarea RCD.

CAPITOLUL III - REGULI

III.1 Reguli generale de utilizare a RCD

1. Utilizarea rețelei de comunicații digitale se face pentru îndeplinirea **atribuțiilor de serviciu și a activităților specifice**.

2. Utilizatorii trebuie să anunțe DIT utilizând canalele de comunicații specificate în regulament în cazul în care se observă orice problemă/breșă în sistemul de securitate al rețelei de comunicații digitale, cât și orice posibilă întrebuințare greșită sau încălcare a regulamentelor în vigoare.

3. Utilizatorii, prin acțiunile lor, nu trebuie să încerce să compromită protecția sistemelor informatice și de comunicații și nu trebuie să desfășoare în mod deliberat acțiuni care pot afecta confidențialitatea, integritatea și disponibilitatea informațiilor de orice tip.

4. Utilizatorii nu trebuie să încerce să obțină acces la date sau programe pentru care nu au autorizație sau consimțământ explicit folosind resursele puse la dispoziție prin intermediul RCD.

5. **Utilizatorii nu trebuie să divulge sau să înstrăineze nume de conturi, parole, Numere de Identificare Personală (PIN-uri), dispozitive pentru autentificare (ex.: Smartcard) sau orice dispozitive și/sau informații similare utilizate în scopuri de autorizare și identificare. Aceste informații nu vor fi solicitate niciodată de DIT, nici prin mesaje e-mail, nici prin alte canale de comunicare. Informare: conturile de utilizator RCD nu sunt corelate cu date cu caracter personal și cu informații financiare**.

6. Utilizatorii au următoarele responsabilități în utilizarea resurselor informatice ale UDJG:

    a. să nu facă copii neautorizate sau să distribuie materiale protejate prin legile privind proprietatea intelectuală (copyright) și/sau GDPR;

    b. să nu se angajeze într-o activitate care ar putea hărțui sau amenința alte persoane;

    c. să nu acceseze sau furnizeze informații cu caracter frivol, cu caracter obscen sau pornografic;

    d. să nu împiedice accesul unui utilizator autorizat la serviciile oferite de RCD;

    e. să nu încerce să obțină alte resurse în afara celor alocate;

    f. să nu încerce să acceseze resurse protejate pentru care nu au autorizare;

    g. să nu încerce că creeze sau să utilizeze instrumente software destinate penetrării sistemelor de securitate ale altor calculatoare;

    h. să nu încerce să provoace defecțiuni hardware sau software;

    i. să nu încerce să descopere și/sau să utilizeze parolele altor utilizatori;

    j. să nu se angajeze într-o activitate care ar putea să degradeze performanțele RCD;

k. să nu ignore măsurile de securitate impuse prin regulamente sau anunțate oficial de către DIT prin canalele de comunicații.

7. Utilizatorii nu trebuie să descarce, să instaleze și să ruleze programe de securitate sau utilitare care expun sau exploatează vulnerabilități ale securității RCD.

8. RCD va fi utilizată doar pentru desfășurarea activităților academice (educaționale, culturale, științifice), a activităților administrative sau în scop personal necomercial adiacent activității specifice. Orice tentativă de folosire a RCD în scopuri comerciale va atrage răspunderea utilizatorului, restricționarea acestuia la resursele RCD și eventuale măsuri disciplinare.

9. Utilizatorii nu trebuie să acceseze, să creeze, să stocheze sau să transmită materiale pe care UDJG le poate considera ofensatoare, indecente sau obscene (altele decât cele în curs de cercetare academică unde acest aspect al cercetării are aprobarea scrisă explicită a conducerii Universității).

10. Utilizatorii obțin acces la RCD conform procedurilor aprobate la nivelul UDJG.

11. Utilizatorii nu trebuie să se angajeze în acțiuni împotriva UDJG folosind RCD.

12. Serviciile de poștă electronică trebuie folosite doar de către utilizatorii acreditați de universitate și nu pot fi transferate altor persoane sau membrilor de familie.

13. Prin utilizarea RCD nu trebuie să se ajungă la costuri directe sau indirecte pentru UDJG, altele decât cele legate de costurile curente generate de achizițiile oficiale pentru funcționarea RCD.

14. Utilizatorii RCD sunt direct răspunzători pentru trimiterea sau recepționarea documentelor sau fișierelor care pot cauza acțiuni legale împotriva UDJG sau prejudicierea, indiferent de formă, a intereselor Universității.

15. Mesajele, fișierele și documentele localizate în spațiile de stocare puse la dispoziție de DIT prin intermediul RCD se supun legislației naționale în vigoare.

16. Utilizatorii trebuie să cunoască și să accepte toate prevederile prevăzute în prezentul regulament privind securitatea RCD înainte de a li se permite accesul la un cont. Luarea la cunoștință a prezentului regulament trebuie certificată odată cu semnarea contractului de muncă.

17. Nerespectarea acestor reguli poate duce la interzicerea accesului la RCD și la eventuale măsuri disciplinare dispuse de către conducerea UDJG.

III.2 Reguli privind configurarea parametrilor de acces la RCD

1. Infrastructura RCD a UDJG este administrată de către DIT, care este responsabilă cu întreținerea și dezvoltarea acesteia.

2. Pentru a furniza o infrastructură de comunicații unitară și scalabilă cu posibilități de modernizare, toate componentele acesteia vor fi achiziționate și instalate conform unui set de reguli și/sau cerințe tehnice specifice stabilite prin consultarea DIT în momentul întocmirii referatului și a specificațiilor tehnice din documentația de achiziție de către toți beneficiarii.

3. Toate echipamentele, fără excepție, conectate la rețeaua de comunicații trebuie configurate conform specificațiilor personalului DIT.

4. Modificarea configurației oricărui dispozitiv din punctele de acces se face numai de către reprezentanți ai DIT.

5. Adresele de rețea sunt alocate dinamic sau static numai de către reprezentanți ai DIT (conform uneia dintre schemele de alocare prezentate în Anexa 1).

6. Toate conectările activelor de rețea la RCD a UDJG se fac cu acordul DIT, conform specificațiilor de conectare.

7. Toate conectările dintre rețeaua de comunicații a UDJG și alte rețele de comunicații, publice sau private, sunt responsabilitatea exclusivă a DIT.

8. Echipamentele de protecție ale rețelei de comunicație a UDJG (firewall) se vor instala și configura de către personalul DIT.

9. Utilizatorii nu au dreptul să extindă sau să retransmită în nici un fel serviciile rețelei (este interzisă instalarea unui telefon, fax, modem, router, switch, hub, punct de acces la rețeaua Universității sau orice alt echipament pentru extinderea rețelei sau a serviciilor oferite de aceasta) fără **avizul tehnic din partea DIT**.

10. Utilizatorilor li se interzice instalarea de dispozitive hardware de rețea sau de programe care furnizează servicii de rețea fără aprobarea DIT. Utilizatorii sunt direct responsabili pentru conexiunile active la RCD și sunt direct răspunzători pentru eventualele consecințe negative ale acestora.

11. Utilizatorilor nu le este permis accesul la dispozitivele hardware ale RCD.

III.3 Reguli privind conectarea la resursele și serviciile RCD

1. Utilizatorilor le este permis să utilizeze numai parametrii pentru conectare la rețea specificați de către DIT.

2. RRCDD răspunde pentru subrețeaua pe care o are în administrare, iar entităților trebuie să li se aprobe, în scris, conectarea activelor de rețea la RCD. În cazul în care nu există un RRCDD, până la identificarea unei persoane care poate prelua această atribuție, administrarea subrețelei va fi atribuită compartimentelor de specialitate din cadrul DIT.

3. Conectarea activelor de rețea care nu sunt proprietatea UDJG se face numai cu aprobarea în scris a DIT și la recomandarea entităților.

4. Accesul de la distanță la rețeaua Universității se va realiza folosind protocolul securizat de tip VPN pus la dispoziție de către DIT. Utilizarea oricărei alte soluții de acces la distanță, în afară de protocolul VPN sau a unei soluții agreate, implică asumarea consecințelor care decurg în urma acestei utilizări.

5. Utilizatorii nu trebuie să extindă sau să retransmită serviciile de rețea în nici un fel (pe nici o cale). Nu este permisă instalarea de conexiuni de rețea neautorizate, indiferent de motiv. Aceste conexiuni pot fi realizate în urma propunerii entităților, după autorizarea de către DIT.

6. Utilizatorii nu trebuie să instaleze active de rețea sau programe care furnizează servicii de rețea fără aprobarea DIT.

7. Sistemele computerizate, servicii de proiectare și configurare soluții de tip web, software din afara Universității care necesită conectare la RCD trebuie să se conformeze standardelor RCD ale Universității.

8. Utilizatorii nu au dreptul să descarce, să instaleze sau să ruleze programe de compromitere a securității care pot dezvălui vulnerabilități în securitatea unui sistem (de ex. programe de spargere a parolei, sustragere de pachete, scanare a porturilor, colectare de pachete, etc.) în timp ce sunt conectați la RCD.

9. Utilizatorii nu au dreptul să modifice, să reconfigureze, să instaleze și să dezinstaleze active de rețea, cabluri, prize de conexiuni.

10. Serviciul de nume și administrarea adreselor IP sunt deservite exclusiv de către DIT. La cerere se pot delega responsabilitățile pentru segmentele de rețea care necesită administrare separată. Delegarea responsabilităților se face de către DIT către RRCDD din cadrul entităților implicate.

11. Serviciile de interconectare a RCD cu alte cu alte structuri de rețea ce se vor integra în cadrul RCD sunt realizate exclusiv de către DIT;

12. Reglementarea utilizării sistemului de găzduire web al Universității „Dunărea de Jos" din Galați (**SGWUDJ**) este prezentată în Anexa 2.

III.4 Reguli privind accesul la resursele RCD

A. Accesul cu drepturi de administrare

1. Entitățile Universității trebuie să prezinte la DIT o listă cu informații de contact în plan administrativ pentru toate sistemele conectate la rețeaua de comunicații a Universității. Această listă trebuie refăcută și prezentată la DIT de fiecare dată când apar modificări de orice natură.

2. Utilizatorii care au conturi de acces de tip administrativ trebuie să respecte regulile și bunele practici privind administrarea. Un set minim de reguli este prezentat în Anexa 3 și poate fi completat de fiecare entitate în parte.

3. Accesul administrativ trebuie să se conformeze regulilor de utilizare a parolelor.

4. Parola pentru un cont cu acces privilegiat trebuie să fie schimbată atunci când persoana care utilizează acest cont își schimbă locul de muncă din cadrul entității sau al Universității, sau în cazul unei modificări a listei de personal ale terților (furnizori desemnați) în contractele cu Universitatea.

5. Pentru o subrețea a unei entități, administrată de un RRCDD, entitatea trebuie să elaboreze o procedură prin care o altă persoană, în afară de RRCDD, să poată avea acces la contul administratorului în caz de forța majoră pentru comunicarea cu DIT.

6. Conturile necesare pentru audit (verificare, control) intern sau extern, pentru dezvoltare sau instalare de software sau alte operațiuni definite, trebuie să îndeplinească următoarele condiții:

    a. să fie autorizate de către DIT;

    b. să fie create cu dată de expirare specifică;

    c. să fie șterse atunci când nu mai sunt necesare.

B. Accesul fizic

1. Toate sistemele de securitate fizică (de exemplu coduri de acces în clădire și coduri de acces pentru prevenirea incendiilor, etc.) a RCD trebuie să fie instalate în conformitate cu regulamentele Universității.

2. Accesul fizic la toate încăperile în care sunt instalate resursele majore (Data Center etc.) ale RCD trebuie să fie documentat și monitorizat.

3. Toate încăperile în care sunt instalate resurse majore ale RCD trebuie să fie protejate fizic, în funcție de importanța acestora și tipul datelor vehiculate sau stocate.

4. Pentru fiecare încăpere în care sunt instalate echipamente ale RCD se aprobă accesul doar pentru personalul care răspunde de buna funcționare a echipamentelor din încăperea respectivă și, dacă este cazul, părților contractante, ale căror obligații contractuale implică acces fizic.

5. Personalul care are drepturi de acces trebuie să dețină legitimație de serviciu și acte de identitate care să-i ateste calitatea.

6. Acordarea drepturilor de acces (folosind card-uri, chei, parole, etc.) se face în scris de către DIT sau, după caz, entitatea care deține încăperea și resursele.

7. Nu este permis transferul dreptului de acces indiferent de motiv.

8. Cardurile și/sau cheile de acces care nu mai sunt folosite trebuie predate entității care le-a eliberat.

9. Pierderea sau furtul cardurilor și/sau cheilor de acces trebuie raportate imediat entității care le-a eliberat.

10. Accesul vizitatorilor în spațiile protejate trebuie documentat într-un registru pentru fiecare încăpere și se va delega un însoțitor.

11. Fiecare entitate va ține o evidență a tuturor cardurilor și/sau cheilor de acces emise, retrase, pierdute sau furate.

12. Fiecare entitate trebuie să anuleze drepturile de acces ale cardurilor și/sau cheilor utilizatorilor care își schimbă locul de muncă din Universitate sau nu mai au relații contractuale cu Universitatea.

13. Pentru fiecare spațiu cu acces restricționat trebuie desemnată o persoană care să verifice periodic înregistrările de acces și să cerceteze orice acces suspect.

14. Accesul restricționat trebuie marcat.

III.5 Reguli privind administrarea conturilor instituționale

1. Toate conturile create trebuie să aibă asociată o cerere și o aprobare dată de către conducătorul entității.

2. Toate conturile de utilizator, pentru personalul aflat în contract cu universitatea, se vor crea în formatul prenume. nume, în condițiile în care numele contului nu se suprapune cu numele altui cont existent. Excepții sunt admise în momentul în care acestea sunt justificate, documentate și aprobate. Același format va fi utilizat și pentru conturile studenților din ciclul 3 (doctorat) care au activități de predare.

3. Toate conturile studenților din ciclurile 1 și 2 (licență și/sau masterat) vor fi create prin algoritmul următor: inițiala prenumelui, inițiala numelui și un număr care va fi incrementat, începând cu 100.Mai multe detalii despre conturile studenților sunt disponibile pe website-ul https://www.student.ugal.ro/. Conturile studenților din ciclul 3 (doctorat) care nu au activități de predare, precum și conturile altor tipuri de cursanți ai UDJG (DFCTT, DPPD etc.) vor fi create utilizând același algoritm.

4. Prin contractul de muncă, contractul de școlarizare și/sau alte documente toți utilizatorii acceptă prevederile prezentului regulament privind utilizarea resurselor și serviciilor RCD.

5. Toți utilizatorii sunt obligați să păstreze confidențialitatea informațiilor privind contul de acces.

6. Toate conturile trebuie să se poată identifica în mod unic, utilizând numele de cont asociat.

7. Toate parolele pentru conturi trebuie să fie create și folosite în conformitate cu regulile privind parolele de acces.

8. Toate conturile utilizator care nu au fost accesate timp de 180 de zile vor fi dezactivate.

9. Conturile de utilizator vor fi active până la încetarea relațiilor contractuale. După încetarea relațiilor contractuale acestea vor fi dezactivate și păstrate într-o arhivă timp de 12 luni, apoi vor fi șterse.

10. Administratorii de sisteme sau alt personal autorizat:

    a. sunt responsabili de ștergerea conturilor persoanelor (utilizatorilor) care nu mai lucrează în, sau care nu mai au relații cu Universitatea;

b. modifică conturile de utilizator pentru se pune de acord în situații precum schimbări ale numelor de familie, modificări privind contul (numele contului) modificări ale drepturilor de utilizator, și altele, în baza unor notificări sau a solicitări;

c. sunt subiectul verificărilor independente (audit, etc.);

d. trebuie să furnizeze o listă cu toți utilizatorii (listă de conturi) pentru sistemele pe care le administrează, la cererea conducerii Universității;

e. trebuie să coopereze cu RRCD și RRCDD pentru investigarea problemelor de securitate.

III.6 Reguli pentru alegerea și utilizarea parolelor de acces

1. Toate parolele trebuie să îndeplinească următoarele condiții:

- să fie schimbate de utilizator în mod regulat, cel puțin o dată la 90 de zile;
- să aibă o lungime minimă de 11 caractere și maximă de 16 caractere;
- să fie parole complexe: să conțină minim o literă mică, minim o literă mare, minim o cifră(caracter numeric). Caracterele numerice nu trebuie să se afle la începutul parolei. Caractere speciale ar trebui incluse în parole acolo unde sistemul permite acest lucru. Caracterele speciale permise sunt: - _ ! . , ; |. (Atenție! Caracterul spațiu nu este permis în parolă.);
- este interzisă reutilizarea ultimelor 5 parole;
- nu trebuie să coincidă sau să fie asemănătoare cu numele de utilizator (login-ul);
- nu trebuie să coincidă sau să fie asemănătoare cu numele;
- nu trebuie să coincidă sau să fie asemănătoare cu numele membrilor familiei;
- nu trebuie să coincidă sau să fie asemănătoare cu o eventuală poreclă (nickname);
- nu trebuie să coincidă cu codul numeric personal;
- nu trebuie să coincidă cu data nașterii;
- nu trebuie să coincidă cu adresa;
- nu trebuie să conțină numărul de telefon;
- nu trebuie să coincidă cu numele departamentului, etc.;
- parolele nu trebuie divulgate în nici o situație, nici măcar angajaților care răspund de securitatea sistemelor informatice. **Niciodată administratorii sistemelor informatice nu vor cere parola**;

- **parolele trebuie tratate ca informație confidențială**;

- parolele stocate trebuie criptate; excepție fac cazurile unde sistemele de autentificare necesită stocarea acestora în clar, caz în care vor fi luate măsuri suplimentare de restricționare a accesului la sistemele respective.

2. Dacă se suspectează că o parolă a putut fi divulgată aceasta trebuie schimbată imediat.

3. Administratorii de sistem, pe sistemele cu mai mulți utilizatori delegați cu gestiunea conturilor și schimbarea parolelor, nu trebuie să permită intervenția asupra conturilor prin folosirea unui cont administrativ.

4. Dispozitivele de calcul nu trebuie lăsate nesupravegheate fără a activa un sistem de blocare a accesului la acestea; deblocarea trebuie să se facă folosind o metodă securizată (parolă, pin, identificare facială, amprentă, etc).

5. Crearea conturilor și/sau schimbarea parolei, asistate de administratorul de sistem, trebuie să respecte următoarea procedură:

   a. Trebuie să existe o solicitare scrisă sau venită via e-mail, de la o adresă din domeniul ugal.ro, de la conducătorul entității de care aparține. Solicitarea trebuie să conțină numele complet al persoanei și numărul de telefon mobil al acesteia;

   b. Pentru conturile noi, solicitarea va fi luată în considerare numai după semnarea contractului de munca și introducerea acestuia în sistem de către entitățile abilitate în acest sens;

   c. Se va genera o parolă temporară care va fi comunicată prin SMS utilizatorului și/sau conducătorului entității care a efectuat solicitarea;

   d. Utilizatorul va schimba în maxim 48 ore parola temporară comunicată anterior.

III.7 Reguli privind utilizarea Intranet și Internet

1. Programele pentru acces la rețeaua Internet sunt destinate utilizatorilor autorizați pentru a fi folosite în scopuri academice, de cercetare și administrative.

2. Programele pentru acces la rețeaua internet și intranet trebuie să fie licențiate.

3. Înaintea instalării oricărui program trebuie citite cu atenție condițiile de utilizare publicate de către producător pentru ca acestea să nu contravină prevederilor prezentului regulament.

4. Toate fișierele care provin din rețeaua Internet trebuie să fie scanate cu un program antivirus actualizat.

5. Toate programele pentru acces Internet/Intranet trebuie să permită folosirea sistemelor proxy și/sau firewall.

6. Toate informațiile accesate în rețeaua Internet trebuie să se conformeze prezentului regulament de utilizare a resurselor și serviciilor RCD.

7. Conținutul tuturor siturilor web ale Universității trebuie să se conformeze regulamentelor de utilizare a resurselor și serviciilor RCD și să folosească numele de domeniu al Universității (ugal.ro). Excepții asupra numelor de domeniu sunt acceptate dacă acestea au fost aprobate în prealabil de către DIT.

8. Răspunderea pentru legalitatea informațiilor publicate și asigurarea securității și a licențelor soluțiilor software care vor fi instalate pe site-urile web găzduite de RCD a Universității revine în totalitate beneficiarului.

9. Utilizarea resurselor oferite de RCD trebuie să fie făcută în mod egal și etic, pentru desfășurarea activității specifice și în scopuri academice (educaționale, culturale, științifice), administrative **și/sau în scop personal necomercial, adiacent activității specifice**.

10. Fișierele electronice se supun acelorași reguli de păstrare aplicabile și altor documente trebuind a fi păstrate în conformitate cu regulile stabilite prin regulamentele proprii fiecărei entități.

11. Accesul la anumite resurse Internet poate fi restricționat în cazurile în care acest lucru se dovedește necesar pentru desfășurarea în condiții optime a activității din cadrul unei entități. Restricționarea se va face de către DIT, în limita resurselor și a capabilităților tehnice existente, la cererea în scris a conducătorului entității respective.

12. RCD este conectată la Internet via unul sau mai mulți furnizori de acces Internet. Toți utilizatorii RCD trebuie să se informeze despre politicile de acces și trafic impuse de furnizorii de acces Internet și sunt obligați să respecte regulile impuse de aceste politici.

13. Utilizatorii trebuie să se autoidentifice corect în RCD a universității.

14. Utilizatorii rețelei Intranet au dreptul la confidențialitate asupra corespondenței și datelor pe care le dețin în rețea.

III.8 Reguli privind folosirea de software sau servicii software

1. Este interzisă instalarea în sistemele de calcul utilizate a software-urilor, pachetelor software sau aplicațiilor care nu sunt licențiate în cadrul UDJG sau nu sunt deținute legal în condițiile respectării legislației în vigoare privind copyright-ul și drepturile de autor. Licențierea trebuie să ateste dreptul de utilizare a sistemelor software respective.

2. Utilizarea sistemelor software licențiate instalate este permisă în limita prezentului regulament și a drepturilor de utilizare stipulate în cadrul sistemului de licențiere pentru respectivele sisteme software.

3. Orice utilizare abuzivă a sistemelor de calcul din cadrul RCD poate duce la interzicerea accesului la RCD și eventuale măsuri disciplinare dispuse de către conducerea UDJG. Utilizarea abuzivă apare atunci când sunt folosite resursele existente pentru a provoca daune, blocări ale funcționării în parametri normali a RCD și a sistemelor conectate la RCD sau a utilizării sistemelor de calcul în scopuri nepermise de prezentul regulament sau de alte regulamente și legi care se aplică.

4. Fiecare utilizator al unui sistem de calcul conectat la RCD este direct responsabil de licențierea și utilizarea în parametri normali a sistemelor software instalate de către acesta în respectivul sistem de calcul. Excepție fac sistemele software instalate de către RRCD, RRCDD sau de către suportul tehnic autorizat în interiorul DIT, caz în care responsabilitatea revine acestora.

III.9 Reguli de acordare a accesului la SPEUDJ

1. Toate cadrele didactice, doctoranzii, cercetătorii, precum și toți angajații care aparțin personalului administrativ, auxiliar didactic sau nedidactic au dreptul de a deține o adresă de e-mail pe serverul Universității.

2. Accesul la SPEUDJ se realizează conform Regulamentului în scopul exercitării obligațiunilor funcționale.

3. Cererile de obținere a unui cont de e-mail pe serverul Universității în cadrul SPEUDJ se depun la DIT fiind inițiate de către Biroul personal din cadrul Direcției juridice și resurse umane sau de către conducătorul entității din cadrul UDJG în baza unei cereri standard.

4. Pentru fiecare utilizator al SPEUDJ se creează o cutie poștală având utilizatorul de forma: prenume. nume și adresa de e-mail de forma: prenume.nume@ugal.ro.

5. După crearea cutiei poștale, fiecare utilizator va primi credențialele de acces printr-un SMS, în cazul în care a fost specificat numărul de telefon al utilizatorului în cerere, sau prin intermediul conducătorului entității din care face parte, și devine persoana responsabilă pentru cutia sa poștală.

6. Utilizatorul SPEUDJ are obligația de a schimba parola inițială, generată la crearea contului de e-mail, și va respecta cerințele enunțate în subcapitolul III.6: Reguli pentru alegerea și utilizarea parolelor de acces.

7. Pe lângă conturile de utilizator se pot crea, la cerere, cu aprobarea conducerii instituției, conturi/adrese de corespondență pentru entități.

8. De asemenea, pe serverul de mail există posibilitatea de creare a unor adrese colective, care permit trimiterea unui mesaj către un număr mai mare de utilizatori interesați într-un anumit domeniu de activitate. Astfel, fiecărei entități îi poate fi atribuită o adresă de e-mail colectivă, în care vor fi incluși toți membrii entității.

9. Sistemul asigură schimbul electronic de corespondență 24/24 ore.

III.10 Reguli privind utilizarea sistemul de mesagerie electronică (e-mail)

1. Pentru comunicarea oficială, toți utilizatorii RCD, fără excepție, vor folosi adrese e-mail din domeniul ugal.ro și se consideră a fi informație de serviciu neputând fi utilizată în alt scop (toate adresele e-mail vor avea sufixul ugal.ro).

2. Pentru verificarea căsuței poștale este pusă la dispoziție o interfață web la adresa http://mail.ugal.ro sau https://webmail.ugal.ro. Aceasta poate fi accesată de pe orice calculator conectat la Internet, prin intermediul unui browser (Mozilla Firefox, Internet Explorer, Google Chrome, Opera, Safari, etc.) De asemenea, pe calculatorul fiecărui utilizator (din interiorul Universității sau personal) sau pe telefonul mobil se poate configura un client local de e-mail (exemple pentru calculator: Mozilla Thunderbird, Microsoft Outlook etc; exemple pentru telefoanele mobile: aplicația Mail oferită de majoritatea producătorilor de telefoane, GMail, K9Mail, etc.).

3. Toți utilizatorii sunt obligați să păstreze confidențialitatea informațiilor privind contul de acces și datele acestora.

4. Utilizatorii nu trebuie să trimită, retrimită sau să primească informații confidențiale sau senzitive ce privesc UDJG, folosind conturi utilizator care nu sunt proprietatea Universității. Exemple de astfel de conturi, sunt, dar nu sunt limitate numai la acestea: Hotmail, Yahoo mail, Gmail, Freemail, precum și adrese de e-mail puse la dispoziție de alți Furnizori de Servicii Internet.

5. Utilizatorii nu pot trimite/primi executabile sau alte fișiere cu extensii care pot transporta viruși. Cu toate acestea a fost permisă trimiterea/primirea de executabile în interiorul unei arhive. Dacă nu recunoașteți adresa de e-mail de la care vin asemenea emailuri vă rugăm să nu deschideți/ extrageți/ executați conținutul din aceste arhive (pentru a evita virusarea calculatorului, compromiterea datelor personale).

6. În nici un caz nu trebuie să se răspundă la un mesaj în care se întreabă/ se cer datele de conectare la sistemul de poștă electronică. Nu trebuie divulgată nimănui parola pentru contul de e-mail.

7. Atât clientul local cât și clienții de webmail accesează aceeași cutie poștală (aceleași foldere). În consecință dacă un mesaj este mutat sau șters de pe o interfață webmail, acesta nu mai apare nici pe clientul local (Outlook).

8. Utilizatorii sistemului de e-mail se vor conforma unui regulament tehnic de utilizare a serviciului de mail (Anexa 4) actualizat periodic de către DIT și transmis acestora.

9. Utilizatorilor le sunt interzise de regulament următoarele activități care împiedică buna funcționare a comunicațiilor în rețea și eficiența sistemelor de mesagerie electronică:

    a. să ofere datele de acces atribuite lor, terțelor persoane pentru utilizarea SPEUDJ;

    b. să citească sau să modifice mesajele poștale ale terților utilizatori fără permisiunea acestora;

    c. expedierea mesajelor cu caracter ofensator, ce conțin amenințări, propagandă, discriminări rasiale, violență sau alte mesaje ce propagă încălcarea drepturilor omului și a legislației în vigoare;

    d. trimiterea de mesaje cu caracter frivol, cu caracter obscen sau pornografic;

    e. folosirea sistemului de mesagerie electronică în scopuri personale;

    f. să efectueze orice încercare de acces neautorizat de SPEUDJ, la cutiile poștale ale terților utilizatori, precum și utilizarea mijloacelor tehnice sau de programe, destinate pentru obținerea accesului nepermis la SPEUDJ;

g. transmiterea în mod intenționat, cu ajutorul SPEUDJ, a unor mesaje ce conțin anexe malițioase, fișiere sau programe destinate pentru distrugerea sau limitarea funcționării mijloacelor tehnice sau a programelor;

h. folosirea sistemului de mesagerie electronică în scopuri politice sau pentru campanii politice;

i. încălcarea drepturilor de autor prin distribuirea neautorizată a materialelor protejate;

j. folosirea altei identități decât cea reală atunci când se trimite e-mail, exceptând cazurile când persoana este autorizată în scop de suport și administrativ;

k. trimiterea sau retrimiterea mesajelor e-mail în lanț;

l. trimiterea mesajelor nesolicitate către grupuri de persoane, exceptând cazurile în care aceste mesaje deservesc instituția;

m. trimiterea mesajelor de dimensiuni foarte mari;

n. trimiterea sau retrimiterea mesajelor ce pot conține viruși.

10. Utilizatorii nu trebuie să răspundă mesajelor de tip phishing prin accesarea link-urilor din interiorul acestora. Accesarea acestor link-uri poate duce la transmiterea credențialelor și a datelor personale, inclusiv a celor financiare dacă acestea sunt stocate pe dispozitivele utilizate. DIT nu va cere niciodată datele de acces.

11. Administratorului SPEUDJ i se interzice:

    a. să comunice datele de acces ale utilizatorului (nume de utilizator și parolă) unor terțe persoane exceptând cazurile prevăzute de legislația în vigoare;

    b. să întrerupă fără temei mecanismele de protecție și filtrare.

12. Utilizatorii SPEUDJ pot fi deconectați/suspendați în următoarele situații:

    a. în cazul nerespectării prevederilor prezentului Regulament;

    b. în cazul în care utilizatorul și-a divulgat credențialele de acces prin accesarea unui mesaj de tip „phishing" sau „spam". În cazul unui astfel de incident suspendarea va dura până în momentul în care incidentul se va stinge prin refacerea scorului MTA. Deblocarea se va realiza în urma unei solicitări scrise înaintată către DIT și prorectorul în a cărui subordine este aceasta;

    c. în cazul în care relațiile contractuale/ de studii cu instituția încetează, conform procedurii.

13. Utilizatorii SPEUDJ au următoarele drepturi:

    a. să beneficieze de poștă electronică și servicii calitative;

    b. să beneficieze de suport tehnic;

c. să beneficieze de suport tehnic împotriva mesajelor tip SPAM/ PHISHING și atașamentelor malițioase;

d. să utilizeze toate funcționalitățile oferite prin intermediul interfeței web.

DIT asigură confidențialitatea datelor personale sau a accesului la informații folosind poșta electronică sau alte instrumente de conversație electronică în limitele competențelor, a posibilităților tehnice existente și a limitelor impuse de prevederile legale în vigoare.

III.11 Reguli privind detectarea virușilor

1. Toate stațiile de lucru conectate la RCD trebuie să utilizeze programe antivirus actualizate.
2. Programele antivirus nu trebuie dezactivate.
3. Configurația programului antivirus nu trebuie modificată într-un mod care să reducă eficacitatea programului.
4. Orice server de fișiere conectat la rețeaua instituției trebuie să utilizeze un program antivirus actualizat în scopul detectării și curățării virușilor care pot infecta fișierele puse la dispoziție.
5. Orice server sau gateway pentru e-mail trebuie să folosească un program antivirus actualizat pentru e-mail aprobat și trebuie să respecte regulile de instalare și utilizare a acestui program.
6. Orice virus care nu a putut fi înlăturat automat de către programul antivirus constituie un incident de securitate și trebuie raportat imediat RRCD sau RRCDD.

III.12 Reguli în relațiile cu terți care implică acces la RCD

1. Orice activitate desfășurată de furnizor care implică acces la RCD trebuie să se conformeze cu prezentul regulament, precum și cu regulamentele în vigoare ale Universității.
2. În toate convențiile și contractele încheiate cu furnizori care implică acces la RCD trebuie specificate următoarele:
    a. informațiile din cadrul Universității la care furnizorul are drept de acces;
    b. modul în care informațiile la care furnizorul are drept de acces urmează a fi protejate de către acesta precum și măsuri ce vor fi luate în cazul nerespectării clauzelor;
    c. metodele de predare, distrugere sau de transfer al drepturilor informațiilor Universității aflate în posesia furnizorului, la încheierea contractului.
3. Furnizorul trebuie să folosească RCD din cadrul Universității numai în scopul stipulat în contract.

4. Orice altă informație din RCD a Universității obținută de furnizor pe durata contractului nu poate fi folosită în interes propriu de către furnizor sau divulgată altora.

5. Toate echipamentele de întreținere ale furnizorului, aflate în rețeaua internă a Universității și care se pot conecta în exterior prin intermediul rețelei, a liniilor telefonice sau a liniilor închiriate, precum și toate conturile de utilizator create temporar pentru furnizor și necesare pentru acces la RCD ale Universității vor fi scoase din uz la încheierea relațiilor contractuale.

6. Accesul furnizorului trebuie să fie identificat în mod unic iar administrarea parolelor sau metodele de autentificare trebuie să fie în conformitate cu regulile privind parolele de acces ale Universității și regulile privind accesul administrativ la resursele și serviciile RCD.

7. Activitățile principale ale furnizorului trebuie să fie documentate de acesta și puse la dispoziția conducerii Universității, 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 și de livrare.

8. În cazul retragerii din contract a unui angajat al furnizorului, indiferent de motiv, furnizorul se va asigura că toate informațiile sensibile sunt colectate și predate Universității sau distruse în cel mult 24 de ore de la producerea evenimentului.

9. În cazul terminării/rezilierii contractului sau la cererea Universității, furnizorul va preda sau distruge toate informațiile ce aparțin Universității și va oferi certificare în scris privind predarea sau distrugerea informațiilor în decurs de 24 de ore de la producerea evenimentului.

10. În cazul încheierii contractului sau la cererea Universității, furnizorul trebuie să predea imediat toate legitimațiile, cartelele de acces, și echipamentele Universității. Echipamentele care urmează a fi reținute de către furnizor trebuie documentate și autorizate de conducerea UDJG.

11. Toate programele folosite de furnizor în scopul furnizării serviciilor stipulate în contract către Universitate trebuie să fie documentate corespunzător și să posede drepturi de utilizare atestate prin licențe.

III.13 Reguli privind monitorizarea resurselor și serviciilor RCD

1. Monitorizarea RCD se face astfel încât să fie posibilă detectarea în timp util a atacurilor informatice și a situațiilor de încălcare a regulamentelor de securitate, în conformitate cu legislația în vigoare.

2. Fișierele jurnal vor fi examinate regulat în vederea detectării eventualelor atacuri informatice și abateri de la regulamentul UDJG privind utilizarea RCD.

3. Orice neregulă privind respectarea regulamentului de utilizare a resurselor și serviciilor oferite prin intermediul RCD va fi raportată DIGCD în scopul efectuării de investigații.

III.14 Măsuri disciplinare

1. Încălcarea prevederilor acestui regulament se sancționează prin măsuri disciplinare hotărâte de către conducerea UDJG.

2. Toate acțiunile care contravin legislației în vigoare vor fi raportate organelor competente.

III.15 Alte dispoziții

1. Întreg personalul este responsabil privind modul de utilizare resurselor oferite prin intermediul RCD. Fiecare utilizator este direct responsabil pentru acțiunile proprii care pot afecta securitatea și buna funcționare a RCD.

2. Personalul autorizat DIT, va lua toate măsurile necesare bunei funcționări a RCD, cu respectarea prezentului regulament și a legislației în vigoare.

3. Entitățile sunt responsabile de informarea și autorizarea utilizatorilor pentru folosirea adecvată a RCD.

4. Entitățile trebuie să asigure controlul accesului fizic în locațiile cu echipamente RCD, în scopul monitorizării RCD și protejării datelor. Accesul trebuie să fie documentat, autorizat și controlat în mod corespunzător.

CAPITOLUL IV – DISPOZIȚII FINALE

1. Toate procedurile și/sau regulamentele de utilizare a RCD sunt obligatorii pentru toți utilizatorii.

2. Prevederile prezentului Regulament vor fi incluse în contractul de muncă, contractul de școlarizare cu studenții și toate contractele cu terți (dacă activitatea acestora are legătură cu RCD).

3. Procedurile și/sau regulamentele de utilizare a RCD vor fi elaborate de către DIT și vor fi propuse pentru aprobare conducerii UDJG.

4. Prezentul Regulament va conține informații de identificare proprii și se va specifica data la care acestea a fost aprobat și data de la care intră în vigoare.

5. Prezentul Regulament va fi disponibil în format electronic tuturor angajaților UDJG.

6. În funcție de necesitățile prezente și viitoare, prezentul regulament poate fi modificat în scopul optimizării funcționării RCD.

7. Modificarea prevederilor unui Regulament/Procedură se face cu aprobarea conducerii UDJG. Fiecare modificare a conținutului va conduce la modificarea versiunii documentului și a informațiilor de identificare. Versiunea anterioară rămâne valabilă până în momentul în care noua versiune intră în vigoare.

8. Prezentul Regulament poate fi completat de anexe referitoare la aspecte specifice unei activități sau unui sistem informatic folosit în cadrul instituției. Aceste anexe vor fi elaborate de către DIT și apoi aprobate de către forurile implicate în activitățile de conducere ale instituției. Anexele vor fi aduse la cunoștința angajaților și vor face parte integrantă din acest regulament. Întrucât anexele conțin exclusiv parametri tehnici, acestea vor fi actualizate și publicate ori de câte ori este necesar.

Anexa 1 la Regulamentul de utilizare a Rețelei pentru Comunicații digitale și a calculatoarelor conectate la rețea din cadrul UDJG

Scheme de alocare pentru adresele IPv4 folosite în cadrul Rețelei pentru Comunicații digitale și a calculatoarelor conectate la rețea din cadrul UDJG

1. Adresele IPv4 necesare funcționării sistemelor de calcul de orice natură (calculatoare, servere, dispozitive fixe și mobile și orice echipament/dispozitiv care necesită conectivitate IP) în cadrul RCD sunt alocate și gestionate de către DIT.

2. În cadrul RCD, pentru segmentele de rețea dedicate entităților din cadrul UDJG vor fi folosite adrese IPv4 din clasele private, nerutabile Internet, conform RFC 1918.

3. Este interzisă folosirea altor adrese IPv4 în afară de cele alocate de către DIT. În cazul în care se constată utilizarea altor adrese decât cele asignate explicit unei entități din cadrul UDJG, DIT va lua măsuri pentru blocarea accesului la rețea a echipamentelor respective.

4. Serviciul de alocare dinamică pentru adresele IPv4 (DHCP, BOOTP) este implementat de către DIT. Este strict interzisă instalarea, configurare și punerea în funcțiune a unui serviciu informatic de acest gen, sau a oricărui alt sistem care realizează alocarea de adrese IP în cadrul unui segment de rețea al RCD fără aprobarea în prealabil de către DIT.

5. Fiecare entitate din cadrul UDJG primește un segment IPv4 cu o mască de rețea pe 24 de biți. În cazurile în care această alocare se dovedește a fi insuficientă pentru a acoperi necesarul de conectivitate în zona respectivă de rețea se pot folosi măști de rețea cu lungimi de 22 sau 23 de biți. Alegerea acestor măști de rețea se realizează de către DIT la solicitarea entității respective.

6. Alocarea adreselor IPv4 în cadrul unui segment destinat unei entități din cadrul UDJG trebuie să respecte una din următoarele scheme de adresare (aceste scheme sunt ilustrate pentru o mască de rețea de lungime de 24 de biți):

    a. Schema nr. 1:

        i. Adrese1 – 8: rezervate pentru administrare

        ii. Adrese9 – 128: disponibile pentru alocare manuală

        iii. Adrese129 – 209: alocare dinamică

        iv. Adrese210 – 249: alocare dinamică pentru dispozitivele de telefonie IP

        v. Adrese250 – 254: rezervate pentru administrare

b. Schema nr. 2:

   i. Adrese1 – 8: rezervate pentru administrare

   ii. Adrese9 –30: disponibile pentru alocare manuală

   iii. Adrese31 – 209: alocare dinamică

   iv. Adrese210 – 249: alocare dinamică pentru dispozitivele de telefonie IP

   v. Adrese250 – 254: rezervate pentru administrare

Se recomandă folosirea schemei nr. 1 de adresare pentru situațiile în care o entitate din cadrul UDJG dorește să folosească o adresare IPv4 fixă (prin configurări manuale) a majorității sistemelor de calcul pe care le exploatează. Se recomandă folosirea schemei nr. 2 de adresare pentru entitățile din cadrul UDJG care doresc să aibă un spațiu mai mare de adrese disponibile pentru adresare dinamică (configurarea automată a sistemelor conectate).

7. Adresele IPv4 folosite în cadrul adresării fixe (prin configurare manuală) se vor gestiona în cadrul fiecărei entități din cadrul UDJG de către RRCDD.

8. Adresele IPv4 publice pe care le folosește instituția vor fi gestionate în totalitate de către DIT.

9. Adresele IPv4 publice nu se alocă decât în cadrul unor segmente de rețea sigure, securizate prin metode fizice și logice. Utilizarea adreselor IPv4 publice trebuie să fie monitorizată de către DIT și trebuie menținută lista cu alocările efectuate.

Anexa 2 la Regulamentul de utilizare a Rețelei pentru Comunicații digitale și a calculatoarelor conectate la rețea din cadrul UDJG

Reguli de utilizare a Sistemului de găzduire web al Universității „Dunărea de Jos" (SGWUDJ)

DIT administrează Sistemul de găzduire web al Universității „Dunărea de Jos" din Galați (SGWUDJ) și pune la dispoziția entităților Universității servicii pentru găzduirea de site-uri web permanente sau de site-uri cu durată limitată (proiecte, evenimente, etc.). SGWUD oferă două tipuri de servicii de găzduire:

- găzduire partajată (sharedhosting); site-ul se află pe un server bazat pe LAMP (stiva de componente software Linux, Apache, MySQL și PHP), care găzduiește și alte site-uri, resursele fiind partajate, iar funcțiile de administrare a site-ului fiind limitate;
- găzduire server privat (VPS); oferă posibilitatea de instalare și administrare completă a sistemului de operare, beneficiarul putând decide ce tehnologii va folosi pentru site-ul web.

Pentru a găzdui un nou site web la SGWUDJ, conducătorul entității trebuie să facă o solicitare scrisă către support.web@ugal.ro, precizând următoarele:

1. Numele, adresa de e-mail instituțională și numărul de telefon mobil a persoanei responsabile care va primi datele de autentificare în vederea gestionării site-ului web, sau a serverului privat;
2. Numele complet și acronimul (dacă este cazul) al entității / proiectului / evenimentului care face obiectul găzduirii site-ului web;
3. Numele de domeniu al site-ului web (de ex. www.nume-site.ugal.ro);
4. Tipul de găzduire (găzduire partajată sau server privat);
5. Spațiul de disc, necesar fișierelor site-ului web - în cazul găzduirii partajate, sau dimensiunea discului necesar instalării sistemului de fișiere, dimensiunea memoriei RAM și numărul socluri și nuclee de procesor - în cazul serverului privat;
6. Numărul estimat de utilizatori care accesează simultan site-ul web;
7. Durata de funcționare a site-ului / serverului privat: permanent, sau perioadă determinată (de exemplu 5 ani);
8. Cerințele speciale.

Aprobarea solicitării găzduirii este acordată de către directorul DIT.

Administrarea site-urilor găzduite la SGWUDJ se face doar din intranet-ul Universității. Accesul în vederea administrării din exteriorul rețelei universității este posibil realizând o conexiune la sistemul VPN al Universității, cu un cont instituțional de utilizator.

Dacă este necesar accesul unei persoane care nu posedă un cont instituțional de utilizator, datele de autentificare la sistemul VPN pot fi generate de către responsabilul desemnat de către entitate, pentru gestionarea site-ului. Acest lucru se realizează în sistemul hr.ugal.ro (opțiunea Gestiune Wi-Fi), prin crearea un cont de acces temporar sau permanent în rețeaua Wi-Fi a Universității, ale cărui date de autentificare pot fi utilizate și pentru autentificarea în sistemul VPN.

Entității îi revine în totalitate răspunderea pentru legalitatea informațiilor publicate pe site-ul web și pentru asigurarea securității prin actualizarea pachetelor software instalate și aplicarea de corecții necesare eliminării de vulnerabilități și, de asemenea, de asigurarea legalității licențelor pentru software-ul pe care l-a instalat.

În cazul în care DIT va constata existența unor vulnerabilități care pot cauza probleme în ceea ce privește securitatea și a exploatarea corectă a resurselor informatice, responsabilul din partea entității va primi un mesaj de informare și site-ul va fi dezactivat până la eliminarea vulnerabilităților.

Anexa 3 la Regulamentul de utilizare a Rețelei pentru Comunicații digitale și a calculatoarelor conectate la rețea din cadrul UDJG

Ghid de reguli și bune practici privind administrarea

Scop

Scopul acestui ghid este de a instrui utilizatorii cu privire la utilizarea adecvată a accesului de administrator la resursele informatice și informatice de la UDJG și de a ajuta la interpretarea cerințelor stabilite în „Regulamentul de utilizare a Rețelei pentru Comunicații Digitale și a calculatoarelor conectate la rețea din cadrul Universității „Dunărea de Jos" din Galați", numit în continuare Regulament.

Unde se aplică

Acest ghid se aplică tuturor administratorilor de sisteme și de aplicații ale UDJG și oricărui alt utilizator care are acces cu drepturi administrative la resursele informatice ale universității.

Definiții

Accesul cu drepturi administrative este definit ca un nivel de acces superior celui al unui utilizator obișnuit. Această definiție este în mod intenționat vagă, pentru a permite flexibilitatea de aplicare la diferite sisteme și mecanisme de autentificare. De exemplu, într-un mediu tradițional Microsoft Windows, membrii grupurilor Power Users, Local Administrators, DomainAdministrators și Enterprise Administratorsse va considera că au acces cu drepturi administrative. În mediile UNIX sau Linux, utilizatorii cu acces la nivelul utilizatorului „root", sau cu permisiunea de a rula comanda „sudosu" vor fi considerați a avea acces de administrator. Într-un mediu de aplicație, utilizatorii cu roluri și responsabilități de administrator de sistem vor fi considerați a avea acces cu drepturi administrative.

Utilizatorii care au permisiunea de a utiliza conturi de acces cu drepturi administrative sau speciale, trebuie să folosească tipul de privilegiu cel mai potrivit activității pe care o desfășoară.

Utilizatorilor cu acces administrativ li se poate solicita să efectueze anumite activități de securitate, cum ar fi corecțiile și actualizările ale software-ului sau ale sistemului de operare, precum și monitorizarea activităților neobișnuite. Dacă se suspectează un incident de securitate, nu trebuie luate măsuri suplimentare înainte de a consulta DIT.

Utilizarea inadecvată a accesului administrativ

Suplimentar față de activitățile nepermise în Regulament, următoarele activități sunt considerate ca utilizări necorespunzătoare a accesului administrativ la resursele de calcul ale universității, cu excepția cazului în care sunt documentate și aprobate de conducere:

- eludarea controlului accesului utilizatorilor sau a oricăror alte forme de control de securitate ale universității;

- eludarea oricăror alte controale informatice formale ale desfășurate în universitate;
- eludarea procedurilor formale de activare/suspendare a contului;
- eludarea procedurilor oficiale de solicitare de modificare a accesului la cont.
- Următoarele acțiuni constituie utilizări necorespunzătoare a accesului administrativ la resursele de calcul ale universității în orice circumstanțe, indiferent dacă există sau nu, aprobarea conducerii:
- accesarea informațiilor non-publice care se află în afara domeniului de aplicare a responsabilităților specifice postului;
- expunerea sau dezvăluirea informațiilor non-publice către persoane neautorizate;
- utilizarea accesului pentru a satisface curiozitatea personală despre un individ, sistem, practică sau alt tip de entitate.

Notă: dacă există indicii că un cont cu acces administrativ sau un calculator este compromis, utilizatorii cu acces de administrator NU ar trebui să efectueze niciun tip investigații digitale și să notifice imediat DIT.

Raportarea utilizării inadecvate a accesului de administrator

După cum se precizează în Regulament, orice utilizator care suspectează o încălcare a acestuia, trebuie să contacteze imediat DIT. Aceasta include și suspectarea utilizării inadecvate a accesului cu drepturi administrative.

Referințe: Guidelines for Appropriate Use of Administrator Access - Carnegie Mellon University https://www.cmu.edu/iso/governance/guidelines/appropriate-use-admin-access.html

Anexa 4 la Regulamentul de utilizare a Rețelei pentru Comunicații digitale și a calculatoarelor conectate la rețea din cadrul UDJG

Regulament tehnic de utilizare a serviciului de mail

Sistemul de poștă electronică al Universității „Dunărea de Jos" din Galați (SPEUDJ) conține o serie de limitări tehnice, limitări care sunt actualizate periodic de către DIT.

- Utilizatorii sistemului de e-mail sunt limitați la trimiterea de maximum 10 mesaje e-mail/minut. La depășirea limitei specificate, utilizatorul nu va mai putea trimite mesaje e-mail pentru următoarele 10 minute. Dacă se dorește creșterea acestor limite trebuie contactat reprezentantul DIT;

- Dimensiunea maximă totală a fișierelor atașate este de 30 MB. Se menționează că aceste dimensiuni sunt calculate și acceptate de către serverul de e-mail după codarea mesajului. Este posibil, de exemplu, ca un fișier de 27 MB să nu poate fi trimis;

- Utilizatorii sistemului de e-mail nu pot trimite mesaje e-mail care au mai mult de 50 de destinatari. Utilizatorii pot utiliza grupurile de e-mail, ce pot fi definite prin interfața webmail și pot conține mai mult de 50 de destinatari;

- Dacă o parolă este introdusă greșit de mai mult de 2 ori (introducere greșită de către utilizator sau ca urmare a unor încercări externe de spargere a contului) contul utilizatorului va fi blocat pentru un interval de 15 minute, timp în care nu se va mai putea autentifica la acesta. Orice încercare de autentificare în aceste 15 minute duce la reluarea cronometrării.