Regulament de utilizare a resurselor IT în cadrul Universității Tehnice din Cluj Napoca și de desfășurare a activităților derulate prin intermediul tehnologiei și al internetului

I. Reguli generale de utilizare a resurselor IT în cadrul Universității

1. Resursele IT ale Universității includ toate echipamentele hardware, software, serviciile și resursele puse la dispoziție pentru derularea activității în cadrul Universității. Acestea includ toate rețelele de date (cu fir și fără fir), calculatoare, imprimante, echipamente mobile, echipamente de stocare, sisteme audio-video, sisteme suport pentru comunicarea electronică și servicii informaționale conexe, inclusiv de tip Cloud.
2. Utilizarea resurselor IT ale Universității și utilizarea lor pentru accesarea de resurse IT care nu sunt puse la dispoziție de Universitate trebuie să se încadreze în specificul activităților educaționale, de cercetare sau administrativă caracteristice învățământului superior. Utilizarea resurselor IT ale Universității în scop comercial privat, fără acordul Conducerii Universității, nu este permisă. Utilizarea resurselor IT ale Universității în contextul propagandei politice, religioase, defăimare sau orice altă acțiune care aduce prejudicii persoanelor sau universității sau pentru strângerea de fonduri/suport pentru cauze neasociate Universității nu este permisă.
3. Derularea activității curente în cadrul Universității trebuie să se realizeze pe sisteme informaționale și informatice puse la dispoziție de Universitate. Utilizarea de resurse și sisteme informaționale care nu sunt puse la dispoziție de Universitate furnizează un risc pentru datele Universității și prin urmare utilizarea acestora nu este permisă fără o aprobare prealabilă. De exemplu, (fără a fi o listă completă): se va utiliza serviciul de e-mail pus la dispoziție de Universitate in loc de gmail, hotmail, yahoo, etc; se va utiliza serviciul de stocare OneDrive (din licența instituțională Office 365) în loc de Dropbox; se va utiliza MS Teams (din licența instituțională Office 365) în loc de Zoom; se va utiliza MS Forms (din licența instituțională Office 365) în loc de SurveyMonkey / GoogleForms /etc.; se vor partaja pentru editare documente .docx/.xls utilizând facilitățile din licența instituțională Office 365 în loc de suita Google (pentru care instituția nu are încheiat un acord în acest sens).

4. Utilizarea în scop personal a resurselor IT ale Universității este permisă la un nivel rezonabil, dar care să nu prejudicieze sau să perturbe activitatea normală a Universității sau a altor utilizatori. Utilizarea în scop recreațional a rețelei de date din infrastructura de cazare (căminele) a Universității este de asemenea permisă, cu respectarea acelorași condiții.

5. Este interzisă conectarea oricărui dispozitiv activ de rețea la rețeaua de date a Universității, cum ar fi: switch-uri, hub-uri, acces point-uri, routere, repetoare de semnal, etc.. Nu este permisă conectarea la rețeaua de date a universității a dispozitivelor de rețea active (switch-uri, hub-uri, acces point-uri, routere, repetoare de semnal, etc.) care nu sunt în proprietatea Universității Tehnice din Cluj Napoca. Toate setările de rețea și toate adresele de rețea (IP) vor fi alocate și administrate de Centrul de Comunicații Kalman Pusztai al Universității Tehnice din Cluj Napoca. Toate echipamentele active de rețea (switch-uri, hub-uri, acces point-uri, routere, etc.) achiziționate din fondurile instituției (indiferent de sursa de finanțare) care se vor conecta la rețeaua de date a Universității necesită avizul reprezentanților Centrului de Comunicații Kalman Pusztai la nivelul fișei tehnice din procesul de achiziție. Toate echipamentele active de rețea (switch-uri, hub-uri, acces point-uri, routere, repetoare de semnal, etc.) se vor conecta la rețeaua de date a Universității sub supervizarea și administrarea reprezentanților Centrului de Comunicații Kalman Pusztai.

6. Dispozitivele active de rețea (cum ar fi: switch-uri, hub-uri, routere, acces-point-uri wireless, repetoare de semnal wireless, etc.) conectate de utilizatori fără acordul Centrului de Comunicații Kalman Pusztai al Universității Tehnice din Cluj Napoca, care pot perturba funcționarea rețelei, vor fi deconectate din rețea și predate gestionarului care le are în gestiune. Acestea vor putea fi reconectate doar după configurarea și monitorizarea funcționării de reprezentanții Centrului de Comunicații Kalman Pusztai al Universității Tehnice din Cluj Napoca.

7. Furnizarea accesului la resursele IT ale Universității unei persoane care nu face parte din Universitate se poate face doar în cazul în care există un regulament sau o decizie specifică în acest sens din partea Conducerii Universității.

8. Toți invitații / vizitatorii Universității care utilizează resursele IT ale Universității și/sau conexiunea de date a Universității trebuie să fie cunoscuți de către un membru al Universității, responsabil pentru acesta/aceștia. Responsabilul trebuie să informeze invitații/vizitatorii despre conținutul prezentului regulament, să poată identifica persoanele și acțiunile generale ale acestora și să își poată asuma responsabilitatea acțiunilor pentru care a furnizat accesul la aceste resurse.

9. Prin utilizarea resurselor IT ale Universității un utilizator acceptă și se conformează implicit tuturor regulamentelor, termenelor și condițiilor specifice de utilizare și măsurilor care guvernează respectiva resursă sau sistem. In mod specific, dar nu exhaustiv, utilizatorul are următoarele obligații:

    a. Să nu facă cunoscută parola proprie pentru conturile de utilizator primite pentru diversele resurse și să ia măsurile cuvenite legate de gestiunea acesteia;

    b. Să nu acceseze sau să încerce să acceseze resurse IT ale Universității (sau din altă parte) pentru care nu a primit permisiune și să nu mijlocească astfel de acțiuni pentru alte persoane;

    c. Să nu utilizeze/realizeze materiale sau resurse care să faciliteze modificarea neautorizată, coruperea, funcționarea defectuoasă sau accesul neautorizat la resursele IT ale Universității sau din altă parte;

    d. Să nu afișeze, stocheze, primească sau transmită imagini, texte, secvențe video/animate sau orice alte materiale care pot fi considerate ofensatoare și care pot aduce Universitatea în dispută. În această categorie se încadrează materiale de natură pornografică, pedofilică, sexistă, rasistă, calomniatoare, amenințătoare, defăimătoare, ilegală, discriminatorie, teroristă, etc.

    e. Din motive de securitate a informației, să nu stocheze date sensibile pe spațiile de stocare (harddisk-uri, ssd-uri, stick-uri de memorie, etc.) locale (laptop-uri, calculatoare de birou, etc.)

ale echipamentelor dedicate utilizării individuale furnizate de Universitate sau aflate în proprietate personală sau pe conturi personale de servicii de stocare Cloud. Datele sensibile includ, dar nu sunt limitate la: coduri numerice personale, date ale cardurilor bancare, date de accesare a diverselor conturi (username si parole in clar), date medicale, date privind membrii familiei, date privind orientarea politica / religioasă / sexuală, etc. Acestea se vor stoca pe sistemele de stocare / și serviciile de stocare puse la dispoziție de Universitate special pentru acest scop (vezi si capitolul II, art. 12, 13, 14, 15).

f. Să nu modifice/falsifice semnături și/sau elemente din antetul (header) mesajelor de poștă electronică; să nu inițieze și/sau să trimită mai departe (”forward”) mesaje de email cu conținut hărțuitor, de tip rețea/lanț (chain) sau nerelevant (junk); să nu pretindă că sunt alte persoane în comunicările realizate în mediul electronic și să nu genereze comunicări cu conținut ofensator sau nerelevant;

g. Să se asigure că toate dispozitivele cu care accesează resursele Universității sunt criptate cu un software de criptare corespunzător și accesul la ele este protejat cel puțin prin utilizarea unui cod pin sau a unei parole;

h. Să respecte drepturile de proprietate intelectuală ale tuturor materialelor și aplicațiilor software puse la dispoziție de Universitate sau de terțe părți și să nu utilizeze, descarce, copieze, stocheze sau să furnizeze astfel de materiale protejate prin drepturi de autor fără permisiunea prealabilă a deținătorului drepturilor sau cu încălcarea drepturilor de licențiere deținute de Universitate;

i. Atunci când procesează date cu caracter personal să respecte drepturile persoanelor vizate și în conformitate cu regulile generale de procesare a acestora;

j. Să se informeze cu privire la termenii și condițiile specifice de utilizare a fiecărei resurse IT (hardware, software, etc.) pusă la dispoziție de Universitate și să le utilizeze în conformitate cu instrucțiunile de utilizare ale producătorului/furnizorului și fără încălcarea termenilor acestora, inclusiv cele referitoare la accesul direct la anumite materiale și resurse care ar trebui accesate strict în cadrul Bibliotecii Universității, sălile de lectură sau în locurile special amenajate.

10. Orice utilizator al resurselor IT ale Universității care creează/deține/stochează obiecte informaționale pe infrastructura de resurse IT a Universității sau conectată cu aceasta are obligația de a furniza acces la acestea în cazul în care există suspiciuni de încălcare a regulilor de utilizare sau a cadrului legal. În cazul în care informația este criptată, utilizatorul are obligația de a furniza cheia de decriptare. Accesul la informații și verificarea suspiciunilor se poate realiza doar pe baza unor justificări care să îndreptățească Conducerea Universității să numească o Comisie în acest sens.

11. Dacă nu este altfel prevăzut, Universitatea nu răspunde de pierderile, distrugerile sau crearea vreunui inconvenient sau prejudiciu de orice fel născute direct sau indirect din utilizarea sau restricționarea utilizării oricărei resurse IT puse la dispoziție de Universitate sau prin intermediul acesteia.

12. Chiar dacă Universitatea ia toate măsurilor de securitate posibile împotriva accesului neautorizat, alterării/modificării datelor, dezvăluirii neautorizate, distrugerii sau pierderii accidentale a datelor sau datelor personale, aceasta nu poate și nu oferă nici o garanție utilizatorului cu privire la securitatea, confidențialitatea și integritatea datelor.

13. Toate condițiile aplicabile resurselor IT puse la dispoziție Universitate se aplică și echipamentelor care nu aparțin Universității (de ex. laptop personal, calculator personal, etc.) atunci când sunt conectate la rețeaua de date a Universității în mod direct și/sau prin VPN, pe durata de timp cât echipamentul utilizează rețeaua de date a Universității sau sistemele puse la dispoziție de aceasta pentru derularea activității.

II. Asigurarea generală a securității informațiilor și datelor în mediul IT al Universității

1. În cadrul infrastructurii de resurse IT ale Universității, atunci când accesul se face pe baza de nume de utilizator și parolă, pentru asigurarea unui grad suficient de protecție, se vor respecta următoarele reguli în definirea parolei:
    a. Lungimea minimă a parolei este de 8 caractere dacă nu există alte limitări
    b. O parolă trebuie sa conțină cel puțin 3 elemente (dacă nu există alte limitări) din următoarele:
        i. Un caracter numeric (0 – 9)
        ii. Un caracter cu litere mari (A – Z)
        iii. Un caracter cu literă mică (a – z)
        iv. Un caracter special (!, %, #, etc.)
    c. O parolă nu trebuie să conțină oricare dintre următoarele elemente:
        i. Un cuvânt (din dicționarul oricărei limbi sau un acronim comun sau din jargonul curent)
        ii. Un nume (de persoană sau de loc / localitate)
        iii. O dată calendaristică ușor de asociat (de ex. ziua de naștere a copilului / soțului / soției, etc.)
        iv. Informație ușor asociabilă propriei persoane (numărul de înmatriculare al mașinii, CNP, serie buletin, data nașterii, porecle, etc.)
        v. Numele de utilizator sau trunchieri ale acestuia (inclusiv concatenarea inversa a numelui și prenumelui sau abrevieri)
    d. La schimbarea parolei, aceasta trebuie să fie diferită de ultimele 6 versiuni anterioare utilizate (dacă nu există alte limitări).
2. Utilizatorii ale căror parole nu respectă condițiile prezentate, vor modifica imediat parola în conformitate cu cerințele. Utilizatorii vor fi contactați în acest sens de reprezentanții departamentelor care administrează resursele IT ale Universității în baza verificărilor/sugestiilor generate de sistemele automate de gestiune/verificare a conformității parolelor cu cerințele impuse.
3. Utilizatorii trebuie să își aleagă/definească o parolă pe care pot să o rețină cu ușurință și să evite scrierea acesteia și, în mod obligatoriu, să nu lase această parolă scrisă într-un loc accesibil altora.
4. Utilizatorilor le este interzisă partajarea parolei cu alte persoane, inclusiv cu reprezentanții departamentele din cadrul Universității care gestionează resursele IT puse la dispoziție.
5. Utilizatorul va lua măsurile de rigoare pentru a face dificil pentru alte persoane să vadă parola care este introdusă la nivelul unui sistem de calcul.
6. Utilizatorul nu își va introduce datele de acces (nume de utilizator și parolă) pe niciun site, formular online, aplicație, etc. decât dacă sunt convinși că respectiva solicitare vine de la un sistem / aplicație / context legitim pus la dispoziție de Universitate. Cea mai bună metoda pentru un utilizator de a se asigura ca accesul la un site / pagina web este legitim solicitat este prin introducerea manual în browser a adresei (sau din Bookmarks/Favorite) și domeniul este recunoscut ca fiind cel oficial. Se va evita accesarea prin link-uri venite pe email chiar dacă cel care a transmis email-ul pretinde a fi o persoană de încredere.

7. Dacă un utilizator are suspiciunea că parola sa este cunoscută de alții (accidental sau voit), atunci acesta are obligația schimbării imediate a parolei și raportarea suspiciunii / incidentului departamentelor din cadrul Universității care gestionează resursele IT puse la dispoziție.
8. Utilizatorilor resurselor IT ale Universității li se recomandă schimbarea periodică a parolei. În funcție de rolul deținut în cadrul aplicațiilor și sistemelor, perioada de valabilitate a unei parole este între 90 de zile și 1 an.
9. Acolo unde este tehnic posibil, se recomandă implementarea și configurarea opțiunilor de autentificare multifactor.
10. Echipele de asigurare și furnizare a resurselor IT ale Universității se vor asigura de actualizarea permanentă a resurselor. Atunci când resursele IT se află în administrarea directă a utilizatorilor sau când sunt utilizate resurse personale (laptop, calculator personal, dispozitive mobile de tip telefon sau tabletă, etc.) în/pentru accesarea resurselor Universității utilizatori au obligația și responsabilitatea menținerii actualizate a respectivelor resurse.
11. Echipele de asigurare și furnizare a resurselor IT ale Universității se vor asigura ca resursele relevante sunt protejate prin aplicații specifice antivirus. Atunci când resursele IT se află în administrarea directă a utilizatorilor sau când sunt utilizate resurse personale în/pentru accesarea resurselor Universității utilizatori au obligația și responsabilitatea instalării și configurării unei soluții antivirus.
12. Universitatea recomandă ca stocarea informațiilor sensibile să fie realizată strict pe spații de stocare cu un înalt grad de securitate și care deține garanții în acest sens. Astfel se recomandă utilizarea pentru salvarea și partajarea datelor a serviciilor de tip Cloud din subscripția instituțională Microsoft Office 365 (produsul OneDrive are documentație din partea furnizorului de conformare cu standardele ISO27001, HIPAA și FISMA, US-EU Safe Harbor framework, EU Data Protection Directive) sau, respectiv, serviciile de partajare de fișiere administrate de Departamentul de Informatică sau de Centrul de Comunicații Kalman Pusztai al Universității. Toți angajații și studenții au acces la facilitățile oferite prin subscripția instituțională Microsoft Office 365, iar fișierele partajate prin produsul OneDrive pot fi partajate și cu terți/externi.
13. Universitatea nu recomandă utilizarea altor servicii cloud de stocare pentru informațiile și datele sale deoarece acestea nu oferă întotdeauna și în mod consistent criptarea datelor, iar în caz de accesare accidentală sau incidente de securitate pot da naștere la situații care poate afecta în mod negativ Universitatea. Datele stocate pe serviciile de cloud care sunt in afara subscripției instituționale nu se află sub controlul Universității, având ca implicație faptul că furnizorii acestor servicii (mai ales în contextul în care acestea furnizate în mod gratuit) pot impune modificarea termenilor și condițiilor de furnizare a acestor servicii sau realiza actualizări ale serviciului fără obligația notificării prealabile.
14. Prin informații sensibile, și care este recomandat ca să fie întotdeauna criptate, la nivelul Universității se înțelege:
    a. Date și informații legate de procesul administrativ al Universității și de planificarea resurselor
    b. Date și informații legate de activitatea de cercetare și din cadrul activității de cercetare
    c. Date cu caracter personal așa cum sunt definite în legislația specifică (Regulamentul UE 679/2016, Legea 190/2018)
    d. Date financiare personale
    e. Date medicale care pot fi asociate unei persoane utilizate în activitățile de cercetare
    f. Date protejate prin acorduri de confidențialitate încheiate cu terțe părți
15. Utilizarea mediilor de stocare portabile (stick-uri de memorie USB, carduri de memorie, DVD-uri, hard-disk-uri portabile, etc.) pentru stocarea de informații sensibile nu este recomandată datorită riscului

ridicat de pierdere sau furt. Dacă se optează pentru utilizarea de astfel de medii este obligatorie criptarea informației și utilizarea unei parole de acces la mediul respectiv (vezi si capitolul I, art. 8, lit. e).

16. Dispozitivele mobile și tabletele puse la dispoziție de Universitatea sau aflate în proprietate personală dar utilizate pentru derularea activităților specifice din cadrul Universității prin conectarea la rețeaua de date a acesteia sau la sistemele și infrastructura utilizate de Universitate sunt predispuse la aceleași vulnerabilități ca și laptop-urile sau stațiile de lucru de tip PC. Aceste echipamente vor avea activate obligatorii facilitățile antifurt specifice (deblocare pe bază de modele sau PIN, localizare echipament, blocarea accesului sau ștergerea datelor de la distanță), vor avea datele stocate criptate, și nu vor avea stocate pe ele informații sensibile fără a fi sincronizate cu alte echipamente sau servicii Cloud de stocare.
17. În general, se recomandă tuturor utilizatorilor de resurse IT din cadrul Universității să respecte măsurile prezentate în Ghidurile actualizate de Securitate Cibernetică emise de Centru Național de Răspuns la Incidente de Securitate Cibernetică din România – CertRO (de ex. pt anul 2021 https://cert.ro/vezi/document/ghid-securitate-cibernetica-2021)

III. Reguli de comunicare în mediul electronic

1. Aplicațiile si serviciile care permit comunicarea in mediul electronic, inclusiv poșta electronica (e-mail) si calendarul / orarul sunt mijloace importante de schimb de informații in cadrul Universității si oferă un mijloc eficient de derulare a activității zilnice. Un „mesaj" este definit ca orice forma de informație scrisă, atașament, înregistrare, imagine / poză, sau alt fișier transmis, recepționat sau publicat utilizând aplicații software specifice. Universitatea utilizează exclusiv serverul intern de e-mail gestionat de Centrul de Comunicații Kalman Pusztai si serviciile Microsoft Office 365 pentru a oferi o platforma de comunicare integrată pentru activitățile didactice, de cercetare si administrative.
2. Comunicarea în mediul electronic / online în contextul derulării activității Universității, pe resursele puse la dispoziție de aceasta și atunci când se reprezintă Universitatea necesită utilizarea unei etichete care să încurajeze un comportament politicos, profesionist și bazat pe respect reciproc. Utilizarea unui comportament adecvat în comunicare se bazează pe:
    a. Utilizarea contului propriu pentru accesarea resurselor și participarea în procesul comunicării și fără impersonarea altor persoane (pretenția de a fi altă persoană) și/sau asumarea de prerogative false (de ex. mimarea deținerii unei anumite funcții deținute de altă persoană sau alte roluri sau responsabilități în acest sens);
    b. Oferirea de timp celorlalți pentru o comunicare eficientă, mai ales în discuțiile de grup; interacțiunile online pot încetini viteza de răspuns a anumitor persoane care nu stăpânesc anumite formate/soluții tehnice utilizate în comunicare;
    c. Acceptarea, recunoașterea și acordarea respectului cuvenit punctelor de vedere exprimate de alții, a opiniilor, interpretărilor sau contribuțiilor formulate de alții;
    d. Acordarea de timp pentru verificarea mesajului care se dorește a fi transmis înainte de transmiterea acestuia. Comunicarea online poate fi ușor interpretată diferit sau scoasă din context;
    e. Găsirea unui răspuns la întrebările care se doresc a fi adresate printre răspunsurile deja existente și disponibile deja online (la nivelul istoricului conversației, postări anterioare, etc.)
3. Acuzațiile de comportament nepotrivit la nivelul comunicărilor efectuate în mediul electronic al Universității, asociate cu Universitatea sau la nivelul utilizării acestor resurse puse la dispoziție de Universitate pot face obiectul investigațiilor disciplinare efectuate de Universitate prin organismele abilitate în acest sens, iar utilizatorii (angajați sau studenți) se vor supune sancțiunilor stabilite în urma

anchetei. Exemple de comportament neacceptat în cadrul comunicărilor în mediul electronic includ utilizarea de mijloace de exprimare catalogate ca fiind violente, indecente, amenințătoare, ofensatoare, defăimătoare sau de natură hărțuitoare. Studenții vor raporta astfel de incidente Consilierului de studii de care aparține. Angajații vor raporta astfel de incidente nivelului ierarhic superior.

4. Utilizarea ocazională sau incidentală în scop personal a serviciilor de comunicare electronică ale Universității sunt permise atâta timp cât acest fapt nu perturbă activitatea curentă din Universitate sau afectează derularea acesteia (de ex. prin volumul sau frecvența acestor comunicări) sau previne accesul la aceste servicii a altor utilizatori. Reprezentanții organizațiilor studențești, a studenților cu rol de reprezentare a studenților în structurile Universității și a studenților cu roluri administrative (de ex. membri în comitele de cămin) pot folosi serviciile de comunicare electronică puse la dispoziție de Universitate pentru derularea activităților respective.

5. În general, prin natura lor, serviciile de poșta electronică si calendar nu sunt servicii cu grad înalt de securitate / siguranța (de exemplu, exista posibilitatea ca persoane neautorizate să monitorizeze transmiterea mesajelor sau înregistrărilor in calendar sau să falsifice transmiterea unui mesaj in numele altei persoane). Prin urmare, utilizatorii nu vor transmite informații confidențiale sau date personale in cadrul unui astfel de mesaj fără criptarea acestora.

6. Utilizatorii vor acorda atenție sporită in / la completarea adresei destinatarului unui mesaj atunci când utilizează facilitățile de „Auto completare / Auto complete” deoarece acestea pot sugera adrese ale unor persoane diferite față de cele cărora le este adresat mesajul. Daca se transmit date sensibile sau date personale la o adresa de email incorectă, utilizatorul are obligația raportării acestei breșe de securitate conform procedurii.

7. Toți angajații și studenții sunt încurajați să își încarce și să utilizeze o fotografie recentă a lor (cu imaginea clară a feței) în secțiunea de profil de pe platforma instituțională Microsoft Office 365 pentru a le permite celorlalți să ii identifice mai ușor. În cazul în care se preferă să nu se partajeze public poza propriei persoane, trebuie ținut cont că nu este permisă utilizarea unei imagini care nu este o reprezentare adevărată a fizionomiei propriei persoane și prin urmare, imaginea de profil se va menține sub forma implicită disponibilă din cadrul platformei Microsoft Office 365.

8. La nivelul serviciilor de e-mail puse la dispoziție, toate mesajele din ”Casuța curentă / Inbox” mai vechi de 2 ani vor fi mutate automat in directorul „Arhiva / Archive”. Pentru căutarea / identificarea de mesaje mai vechi de 2 ani, utilizatorii vor accesa secțiunea „arhiva online”. Utilizatori au la dispoziție următoarele opțiuni la nivelului meniului „Acasa / Home”:

    a. Do not archive (toate mesajele de e-mail vor fi păstrate in directoarele implicite din serviciul de e-mail SquirrelMail/Outlook (e.g. Inbox si Sent Items) si nu vor fi arhivate automat

    b. Arhivează mesaje mai vechi de 2 ani

9. In managementul spațiului de stocare asociat conturilor de e-mail următoarele opțiuni sunt disponibile utilizatorilor pe perioada menținerii relației de colaborare cu Universitatea:

    a. Șterge mesajele mai vechi de 5 ani (mesajele mai vechi de 5 ani vor fi șterse automat, fără alte notificări);

    b. Șterge mesajele mai vechi de 10 ani (mesajele mai vechi de 10 ani vor fi șterse automat, fără alte notificări);

    c. Menține pe perioadă nedeterminată toate mesajele cu condiția respectării spațiului maxim de stocare alocat; în cazul depășirii spațiului de stocare alocat, utilizatorul este notificat prin e-mail să elibereze din spațiul de stocare utilizat în termen de 30 de zile; după expirarea termenului, se vor șterge în mod implicit, în ordine invers cronologică (începând cu cele mai vechi mesaje) mesajele din spațiul de stocare asociat conturilor de e-mail până la îndeplinirea condiției de ocupare a 90% din spațiul de stocare alocat.

10. La încetarea colaborării cu Universitatea (angajați sau studenți / cursanți), contul electronic utilizat pentru accesarea serviciilor de comunicare electronică va fi blocat/suspendat în data părăsirii oficiale a instituției. Căsuța de e-mail și restul serviciilor asociate contului de utilizator nu vor mai fi accesibile. La 12 luni după data plecării, contul va fi șters în totalitate, fapt care va implica ștergerea totală a conținutului căsuței de e-mail după alte 30 de zile. Foștii angajații pot solicita Universității menținerea activă a contului (și căsuței de e-mail) pentru asigurarea continuității activităților în care au fost implicați pentru o perioada suplimentară de maxim 3 ani de zile. Acest lucru trebuie aprobat de superiorul ierarhic al persoanei.
11. Pentru menținerea continuității activității Universității după părăsirea instituției de către un angajat, superiorul ierarhic al respectivului angajat poate avea acces la conținutul căsuței de email și la fișierele acestuia de pe resursele IT ale Universității cu acordul și decizia Consiliului de Administrație a Universității. Angajatul, la părăsirea instituției are obligația ștergerii tuturor email-urilor cu caracter personal și a datelor și fișierelor cu caracter personal care se regăsesc pe infrastructura Universității și sunt asociate contului său electronic. Astfel, la părăsirea instituție se consideră că în conținutul căsuței de poștă electronică sau pe resursele IT ale Universității fostul angajat nu mai are date cu caracter personal asociate contului electronic.
12. Universitatea oferă tuturor angajaților/colaboratorilor și studenților un cont electronic (nume de utilizator și parolă) cu servicii de comunicare electronică asociate (poștă electronica / e-mail) pentru a furniza un mediu sigur și de încredere de comunicare și pentru a exista un nivel asigurator a transmiterii mesajelor între părți. Nivelul de asigurare/confirmare a transmiterii și recepționării mesajelor nu poate fi asigurat dacă angajații sau studenții utilizează conturi și adrese de e-mail externe sau auto-forwarding (redirecționare automată) spre adrese de e-mail externe. Prin urmare, utilizarea de servicii externe de email pentru derularea curentă a activității din cadrul Universității nu este permisă și auto-forwarding (redirecționare automată) spre adrese de email externe nu este permisă.
13. Dacă se consideră că există un motiv valid de redirecționare a adresei de e-mail din cadrul Universității spre o adresă externă de email, angajații pot depune o cerere în acest sens la Conducerea Universității.
14. Căsuțele de e-mail ale angajaților care au acces privilegiat la sistemele Universității (de ex. administratori de sisteme, administratori de baze de date, etc.) și ale angajaților cu responsabilități în aprobarea cheltuielilor și plăților din cadrul Universității nu vor avea, sub nici o circumstanță, activate opțiuni de redirecționare automată a email-ului instituțional.

IV. Monitorizarea comunicării și activității în mediul electronic al Universității

1. Comunicarea electronică în sens general reprezintă apelurile de telefonie, mesajele fax, toate tipurile de mesaje, incluzând poșta electronică (email), mesaje instant, SMS-uri, tweet-uri, conținut web (site-uri, blog-uri, pagini wiki, forumuri, secvențe video, secvențe audio, etc.), postări și comentarii (blog, forumuri, inclusiv pe rețelele de socializare), etc. Universitatea, în derularea curentă a activității, nu ia nici o măsură de monitorizare generală a conținutului comunicărilor electronice ale angajaților sau studenților săi și este împotriva oricăror măsuri de acest fel. De asemenea, Universitatea nu realizează nici prin sondaj și cu intervenție umană acțiuni periodice de verificare a conținutului comunicărilor electronice sau a comunicărilor electronice în general. Totuși, are loc scanarea automată și computerizată a traficului de e-mail pentru scopul declarat al interceptării mesajelor de poștă electronică nesolicitate transmise în masă (denumite generic mesaje ”spam”) și, respectiv, interceptării mesajelor cu conținut vătămător (viruși informatici, tentative de fraudă, etc.).
2. În conformitate cu legislația europeană și națională în vigoare, trebuie menționat că Universitatea poate intercepta, fără consimțământul persoanei, conținutul comunicărilor electronice ale acesteia pentru scopuri clar definite cum sunt: înregistrarea de dovezi privind tranzacțiile efectuate, asigurarea

respectării legislației aplicabile, detectarea de fapte care se pedepsesc conform Codului Penal și/sau utilizarea ne-autorizată a infrastructurii de comunicații, respectiv asigurarea operării în bune condiții a sistemului de comunicații. Astfel, Universitatea aduce la cunoștința tuturor utilizatorilor serviciilor proprii puse la dispoziție că astfel de interceptări pot să aibă loc, fără nici o altă notificare prealabilă sau fără obținerea consimțământului explicit, atunci când sunt întrunite condițiile legale aplicabile.

3. Scopurile pentru care Universitatea nu are nevoie de obținerea consimțământului prealabil pentru interceptarea și accesul la comunicările electronice pot fi cel puțin unul dintre următoarele:
    a. Stabilirea existenței unor dovezi relevante pentru Universitate, de exemplu înregistrările de tip jurnal al diverselor sisteme de comunicații pentru cazurile in care se dorește probarea unor elemente specifice din procesul de comunicare (de ex. data transmiterii unor mesaje, etc.)
    b. Evaluarea și monitorizarea îndeplinirii anumitor metrici sau proceduri relevante pentru Universitate, sau care sunt impuse Universității (de ex. monitorizarea gradului de securitate a sistemelor de comunicații)
    c. Evaluarea / monitorizarea sau demonstrarea îndeplinirii anumitor standarde care trebuie atinse în utilizare de către persoane specifice (de ex. monitorizarea pentru controlul calității sau eficacitatea instruirii personalului)
    d. Prevenirea sau detecția faptelor cu caracter penal (de ex. monitorizarea sau înregistrarea pentru detecția fraudei, a utilizării necorespunzătoare a resurselor IT sau alte activități ilegale)
    e. Investigarea și detectarea utilizării neautorizate a sistemelor și resurselor IT ale Universității așa cum este specificat în prezentul Regulament.
    f. Asigurarea operării efective a infrastructurii și resurselor IT ale Universității (de ex. monitorizarea și ștergerea virușilor informatici, verificarea și oprirea amenințărilor la nivelul sistemelor și resurselor cum sunt atacurile de tip ”denial of service”, ”acces ne-autorizat”, etc.), monitorizarea proceselor automate cum sunt cele legate de fluxurile de date, jurnalele cu transmiterea mesajelor e-mail, activitatea de caching, distribuirea efortului la nivelul resurselor (”load distribution and balancing”).
    g. Verificarea în vederea determinării relevanței comunicărilor electronice pentru buna desfășurare a activității curente a Universității (de ex. verificarea conținutului căsuței de e-mail pe durata absenței de la locul de muncă a angajatului) în baza unei decizii a șefului ierarhic aprobate de Conducerea Universității.
4. Utilizatorii serviciilor de comunicații electronice și a resurselor IT puse la dispoziție de Universitate înțeleg în acest context faptul că, periodic, personalul implicat în administrarea resurselor IT și a sistemelor de comunicații electronice din cadrul Universității monitorizează transmisiile de date sau observă informații legate de tranzacțiile/operațiile efectuate în cadrul acestora pentru asigurarea funcționării în bune condiții a acestor servicii. Cu aceste ocazii sau în alte contexte care țin strict de furnizarea acestor servicii, acest personal poate în mod accidental să intre în contact cu conținutul comunicărilor electronice efectuate. Cu excepția cazurilor stipulate în legile naționale și europene aplicabile sau a celor stipulate în prezentul regulament, acest personal are obligația păstrării confidențiale a acestor informații (dezvăluirea sub orice formă a informațiilor sau datelor, parțială sau totală este interzisă) și îi este interzis cu desăvârșire să examineze intenționat sau voit conținutul tranzacțiilor / operațiilor efectuate de un anumit utilizator sau conținutul efectiv al acestor comunicări, chiar dacă solicitarea vine din partea unui nivel ierarhic superior. În cazul descoperirii de încălcări a acestor prevederi, persoanele îndreptățite se vor adresa nivelului ierarhic competent din cadrul Universității.
5. Conținutul comunicărilor electronice poate fi inspectat și în cazul special al comunicărilor electronice care nu au putut fi livrate implicit pentru a putea fi șterse sau redirecționate către destinatarul corect.

Astfel de inspectări ale comunicării electronice care nu pot fi evitate sunt reduse la un nivel minim de examinare necesar retransmiterii comunicării spre un destinatar corect. Re-transmiterea unor astfel de comunicări va fi obligatoriu însoțită de o notificare către destinatar că respectiva comunicare a fost inspectată pentru scopul identificări corecte a destinatarului.

6. Înafara situațiilor stipulate anterior, Universitatea va solicita consimțământul utilizatorului înaintea inspectării datelor acestuia sau fiind asociate cu acesta (conturi de e-mail, spații de stocare, înregistrări din jurnalele de acces, etc.). Totuși, în următoarele situații datele se vor accesa chiar dacă nu s-a furnizat acest consimțământ:
    a. Când există o solicitare legală în acest sens
    b. Când există motive suficiente de suspiciune de încălcare a regulilor și regulamentelor Universității bazate pe dovezi (diferite de zvonuri, bârfe sau acuzații defăimătoare).
    c. Când există situații urgente, ca de exemplu atunci când lipsa unei acțiuni poate conduce la afectarea gravă a sănătății unei persoane, la pierderi sau distrugeri materiale importante, la pierderea semnificativă de date și dovezi incriminatorii în cazul unei încălcări a legii sau regulamentelor Universității, respectiv la afectarea în mod grav a Universității sau a comunității academice a Universității
    d. Când lipsa unei acțiuni poate afecta în mod grav abilitatea Universității de a funcționa și de a-și îndeplini obligațiile
7. In cazul accesării datelor unui utilizator fără consimțământul prealabil al acestuia, se aplică următoarele:
    a. Situații de urgență: se va accesa minimum de conținut necesar pentru soluționarea urgenței și se vor lua doar acțiunile minimale necesare; se va obține în cel mai scurt timp, fără întârziere, autorizarea necesară sau consimțământul persoanei pentru inspectări suplimentare sau acțiuni suplimentare;
    b. În orice alt caz: inspectarea/accesul se va face cu autorizarea în scris a directorului ierarhic al persoanei căreia îi sunt inspectate/accesate datele și a unui reprezentant al Conducerii Universității (Rector, Prorector). Se va menține o evidență scrisă a justificării cu motivele pentru care s-a acordat accesul și evidența datelor accesate;
    c. Datele criptate: când pe o resursă IT a Universității se regăsesc informații criptate va fi furnizată în mod obligatoriu, la cerere, o cheie de decriptare de către persoana care a criptat datele;
    d. Date create de angajați sau studenți sau asociate acestora și care nu mai sunt angajați ai Universității, respectiv studenți/cursanți ai Universității devin proprietate a Universității. Prin urmare, nu mai este necesară obținerea consimțământului persoanei pentru accesarea și inspectarea acestor informații. Este însă necesară obținerea unei autorizări din partea directorului ierarhic al structurii unde a fost angajată persoana (decanul facultății în cazul studenților sau directorul programului de studii) și a unui reprezentant al Conducerii Universității (Rector, Prorector);
8. Dacă accesul la datele (inclusiv cele din cadrul comunicărilor electronice) unei persoane este necesar pentru motive ce țin de derularea curentă a activității Universității pe perioada în care respectiva persoana nu este disponibilă (de ex. este în concediu) este obligatorie solicitarea în primă instanță a consimțământului respectivei persoane. Dacă persoana nu poate fi contactată, directorul ierarhic al persoanei împreună cu un reprezentant al Conducerii Universității (Rector, Prorector) trebuie să autorizeze în scris accesul la datele angajatului. Se va menține o evidență scrisă a persoanei/persoanelor care vor avea acces la date și a măsurilor luate pentru obținerea consimțământului cu menționarea mijloacelor prin care s-a încercat comunicarea (și a celor minim 2 persoane martor la încercare), justificarea cu motivele pentru care s-a acordat accesul și evidența datelor accesate care se va înmâna inclusiv persoanei in cauza la data revenirii în Universitate.

9. La obținerea unei autorizări pentru accesarea/inspectarea datelor de pe o resursă IT a Universității (inclusiv de tip comunicare electronică) aceasta va fi tratată în următorul mod:
    a. Conținutul și materialele legate de activitatea la Universitate se vor procesa conform tipicului acestora și rolului pe care îl deservesc în buna derulare a activității Universității;
    b. Conținutul și materialele care par a fi de natură personală vor fi inspectate/accesate doar dacă există un temei și un interes legitim al Universității să facă acest lucru;
    c. Utilizatorii resurselor IT ale Universității (angajați, studenți / cursanți) sunt direct responsabili să își șteargă toate datele personale și informațiile de natură personală disponibile pe aceste resurse înainte de data la care părăsesc Universitatea;
10. Orice inspecție sau acces la date și informații autorizată și realizată în conformitate cu prezentul regulament se va realiza respectând dreptul la intimitate și viață personală a utilizatorilor. Conținuturi și materiale care par a fi de natură personală/privată vor fi supuse unei inspecții minimale necesare pentru finalizarea procesului de verificare/căutare. Orice informație confidențială întâlnită accidental și care nu face subiectul căutării/inspecției nu va fi partajată cu terțe părți și va rămâne confidențială în continuare. Dacă, în timpul verificărilor, se descoperă în mod accidental materiale și conținuturi care sunt ilegale sau contravin regulamentelor Universității, situația va fi deferită organelor legale abilitate pentru anchetă, respectiv Conducerii Universității și entităților din cadrul Universității cu rol în investigarea și monitorizarea respectării regulamentelor și regulilor interne.

V. ***Protecția datelor cu caracter personal în timpul activităților derulate prin intermediul tehnologiei și al internetului***

1. Desfășurarea activităților curente din Universitate, în special a celor cu caracter didactic, (așa cum sunt ele definite ca scop al contractelor încheiate între Universitate și studenți) , prin intermediul tehnologiei și al internetului implică procesarea sistematică a următoarelor date cu caracter personal: nume, prenume, fizionomie, voce, adresă de e-mail, datele de conectare la platforma utilizată, nume de utilizator și parolă, rezultatele evaluărilor. Temeiurile legale în baza cărora se procesează aceste date sunt furnizate de Ordonanța de Urgență nr. 141 din 19 august 2020 privind instituirea unor măsuri pentru buna funcționare a sistemului de învățământ și pentru modificarea și completarea Legii educației naționale nr. 1/2011 și Nota 260/21.09.2020 a Direcției Generale Învățământ Universitar din Ministerul Educației și Cercetării, împreună cu cadrul legal stabilit prin Legea educației naționale nr. 1/2011 cu completările ulterioare.
2. Utilizarea resurselor IT, în general, permite vizualizarea sincronă (în timp real) a imaginilor și sunetelor furnizate de participanții la întâlniri de studiu organizate în spațiul virtual. Acestea nu sunt înregistrate automat cu excepția în care utilizatorul/owner-ul evenimentului a specificat setările pentru înregistrare automată. Numele și prenumele participanților și/sau adresa de e-mail sunt folosite de cadrele didactice pentru invitarea participanților la întâlniri. Ele vor fi stocate de sistemul utilizat pentru a permite atât accesul la următoarele întâlniri, cât și derularea celorlalte activități asincron (teme de control, lucrări de verificare, materiale didactice etc).
3. În cazul în care cadrul didactic consideră că înregistrarea întâlnirii poate fi folosită ca resursă educațională, acesta trebuie să solicite acordul (consimțământul) participanților la întâlnire pentru a înregistra întâlnirea. Consimțământul se dă prin exprimare liberă. Acordarea consimțământului nu trebuie să constituie o condiție pentru participarea la întâlnire. Înregistrarea va fi păstrată doar pe platforma pe care s-a făcut înregistrarea până la finalul semestrului și cu drept de acces nominal acordat doar studenților îndreptățiți să acceseze respectiva resursă educațională. Dacă un student participant nu dorește să își dea consimțământul atunci înregistrarea nu va fi făcută. Anterior înregistrării studenții

își vor închide microfoanele, camerele web și pe ecranul care se înregistrează se vor ascunde zonele cu afișarea numelor studenților. Pe timpul desfășurării cursului studenții pot pune întrebări profesorului folosind sistemul chat (text sincron). Procedura este valabilă și pentru înregistrarea activităților similare specifice învățământului la distanță și cu frecvență redusă.

4. Cadrele didactice care intenționează să folosească alte platforme decât cele recomandate de Universitate (Microsoft Teams 365) vor întreprinde toate diligențele ce se impun pentru respectarea drepturilor persoanelor asupra datelor personale și furniza inclusiv documentația produsului / soluției respective referitoare la modul de respectare a Regulamentului UE 679/2016 privind protecția datelor cu caracter personal.
5. Studenții care participă la activitățile didactice prin intermediul tehnologiei și al internetului au următoarele obligații (cfrm Nota 260/21.09.2020 a Direcției Generale Învățământ Universitar din Ministerul Educației și Cercetării):
    a. utilizează aplicația/platforma educațională informatică doar în conformitate cu prevederile legale și conform manualelor și instrucțiunilor de utilizare ale acestora
    b. răspund pentru toate mesajele, videoclipurile, fișierele expediate sau pentru orice alte materiale prelucrate prin utilizarea aplicației/platformei educaționale informatice;
    c. să nu înregistreze, să nu disemineze și să nu folosească informații care conțin date cu caracter personal în alt mod care excedează scopului prelucrării acestor date.
6. Anterior desfășurării de întâlniri în spațiul virtual / online se vor respecta următoarele:
    a. se va furniza (la cerere) organizatorului întâlnirii online de către student adresa de e-mail instituțională, furnizată de Universitate pentru înrolarea (înscrierea) pe platforma online (de tipul prenume.initiala.nume@student.utcluj.ro). Există posibilitatea ca studenții să fie înrolați direct de cadrele didactice sau personal al Universității.
    b. se vor lua măsuri de protejare a spațiului personal (dacă este folosit un astfel de spațiu) de unde studentul / cadrul didactic intră prin conexiunea internet în întâlnire (se va avea în vedere orientarea camerei web astfel încât să nu fie furnizate alte date cu caracter personal: locație, imaginea altor persoane, voce etc);
    c. se vor lua măsuri să se folosească o conexiune securizată la internet;
    d. organizatorul întâlnirii se va asigura că toate setările întâlnirii sunt conforme cu specificul acesteia și că are controlul deplin asupra desfășurării ei;
    e. fiecare participant își va salva/configura numele și prenumele propriu la nivelul informațiilor afișate în interfața platformei pentru ca un cadru didactic să identifice nominal corect participanții la întâlnirea online;
    f. se va face un test de imagine luându-se măsuri corective.
7. Pe timpul desfășurării de întâlniri în spațiul virtual / online se vor respecta următoarele:
    a. se vor folosi camerele video și microfoanele în funcție de recomandarea cadrului didactic (cu sau fără microfon, cu sau fără video);
    b. nu se va înregistra (audio și/sau video) întâlnirea folosind facilitățile platformei sau orice alte soluții software sau echipamente (camere video, reportofoane, telefoane mobile, tablete, camere web etc);
    c. facultativ: dacă un cadru didactic consideră că înregistrarea întâlnirii poate fi folosită ca resursă educațională acesta trebuie să solicite acordul (consimțământul) participanților la întâlnire pentru a înregistra întâlnirea. (vezi art.3, secțiunea V)

d. nu se vor fotografia participanții folosind facilitățile platformei (captura de ecran / screen shot) sau orice alte soluții software sau echipamente (camere video, reportofoane, telefoane mobile, tablete, camere web etc);

e. prezența se va face în conformitate cu regulamentul Universității folosind facilitățile platformei fără a utiliza mijloace intruzive care să afecteze intimitatea participanților (captură de ecran, foto cu aparat extern). Se pot folosi liste de prezență offline sau salvate în platformă;

8. După desfășurarea de întâlniri în spațiul virtual / online se vor respecta următoarele:

   a. nu se vor disemina date cu caracter personal indiferent de forma colectată;

   b. se va închide aplicația evitând astfel o colectare accidentală a datelor cu caracter personal;

   c. dacă un cadru didactic a înregistrat întâlnirea, cu acordul participanților, vizionarea acesteia se va face exclusiv pe platforma online unde este diseminată și cu stabilirea clară a listei nominale de persoane care au acest drept. Este interzisă postarea oricăror materiale rezultate din activitatea virtuală în afara platformei

9. La finalul sesiunilor de examinare prevăzute în calendarul activităților din anul universitar se vor respecta următoarele:

   a. Se vor șterge sau arhiva spațiile de lucru utilizate pentru organizarea de întâlniri online pe durata semestrului sau se vor anula drepturile de acces la acestea pentru studenții promovați precum și orice date cu caracter personal colectate pe durata semestrului. Accesul la spațiile de lucru pentru studenții care nu au promovat disciplina se va gestiona de fiecare cadru didactic fie prin menținerea în spațiul existent (după ștergerea celor promovați) fie prin crearea/adăugarea la un spațiu dedicat studenților aflați în situația de nepromovare a disciplinei. Personalul Universității cu atribuții în administrarea resurselor IT ale Universității pot implementa, cu anunțarea prealabilă a cadrelor didactice a Universității, măsuri de ștergere automată a spațiilor a căror creare și utilizare a fost intenționată pentru anii universitari anteriori.

   b. Conținuturile electronice în baza cărora s-au făcut evaluări ale competențelor studenților se vor arhiva pe o perioadă de 3 ani în condițiile de stocare asimilate informațiilor sensibile după care se vor șterge permanent.

VI. Sancțiuni și penalități pentru utilizarea neconformă a resurselor IT în cadrul Universității

1. Nerespectarea prevederilor prezentului regulament de către personalul responsabil cu gestionarea resurselor IT din cadrul Universității se va constitui în motiv de cercetare disciplinară a activității conform regulilor stabilite în cadrul legislativ din România și din Universitate. Sancțiunile care se pot stabili în acest caz sunt cele aferente legislației muncii. Suplimentar, dacă se constată existența unui prejudiciu la nivelul Universității sau altor entități (persoane fizice sau juridice) cauzate direct de acțiunile realizate de către personalul responsabilul cu gestionarea resurselor IT din cadrul Universității în contradicție cu prevederile prezentului regulament sau a cadrului legal conex, persoanele vătămate, inclusiv Universitatea, se pot constitui în parte vătămată împotriva acesteia, în conformitate cu cadrul legal aplicabil.

2. Nerespectarea prevederilor prezentului regulament de utilizatorii resurselor IT din cadrul Universității se poate sancționa, în funcție de situație, sub următoarea formă:

   a. Retragerea temporară a dreptului de accesare a rețelei de date a Universității

   b. Retragerea permanentă a dreptului de accesare a rețelei de date a Universității

c. Retragerea temporară a accesului la numite servicii electronice

d. Retragerea permanentă a dreptului de acces a anumitor resurse

3. Dacă aplicarea sancțiunii duce la imposibilitatea derulării curente a activității situația va fi deferită spre analiză Comisiilor de cercetare disciplinară din cadrul Universității (în cazul angajaților), respectiv Consiliilor Facultăților responsabile de programul de studii aferent (în cazul studenților).

Anexa – nota de informare atașată comunicărilor de tip poștă electronică de toți utilizatorii acestor servicii

Informare

Prezentul mesaj și orice documente atașate pot conține informații confidențiale sau sensibile care aparțin Universității Tehnice din Cluj-Napoca (UTCN). În mod implicit, și dacă nu este altfel specificat sau reglementat, mesajul, împreună cu documentele atașate, este destinat spre utilizare și cunoaștere strict persoanei fizice sau juridice căreia îi este adresat și nu poate fi dezvăluit sau utilizat de către altcineva. Dacă ați primit acest mesaj dintr-o eroare, vă rugăm să anunțați imediat UTCN, ca răspuns la mesajul de față, și să ștergeți apoi din sistemul dvs. mesajul fără a-l copia sau deschide. Prin prezenta sunteți notificat de faptul că orice dezvăluire, copiere, distribuire sau inițierea/omiterea unor acțiuni pe baza prezentelor informații, în condițiile în care nu este altfel specificat sau reglementat, sunt strict interzise și atrag răspunderea civilă și/sau penală (art. 302 Noul Cod Penal). Prin natura tehnologiei de transmitere a mesajelor de poștă electronică, UTCN nu este răspunzătoare pentru modificările care pot fi aduse prezentului mesaj și nici pentru întârzierile care pot surveni în recepționarea acestuia. De asemenea, UTCN nu poate garanta integritatea mesajului și nici că acesta este lipsit de viruși, interceptări sau interferențe de orice natură.