Rector,
Conf. univ. dr. Ramona Flavia Rațiu

POLITICĂ IT&C
Cod: PLT-DPO-03
Ediția [I], Revizia [0], Data 01.10.2024

Avizat,
Prorector Managementul Calității și Proiecte
Conf. univ. dr. Bălan Sorina Mihaela

Elaborat,
Responsabil protecția datelor
AMPLUSNET S.R.L.

1. Scop

Având în vedere preocuparea ***UNIVERSITATEA "DIMITRIE CANTEMIR" DIN TÂRGU MUREȘ*** (*„Instituției"*) pentru respectarea legislației, în general și a normelor destinate să protejeze datele cu caracter personal și viața privată a persoanelor fizice, în special, se impune adoptarea acestei politici („**Politica**") care să guverneze gestionarea și utilizarea sistemelor informatice și de comunicații.
Politica are ca scop asigurarea integrității, disponibilității sistemelor informatice și de comunicații din cadrul ***UNIVERSITATEA "DIMITRIE CANTEMIR" DIN TÂRGU MUREȘ***, precum și asigurarea securității datelor cu caracter personal prelucrate prin aceste sisteme.

- Securitatea datelor cu caracter personal privește toate măsurile luate împotriva oricăror incidente ce conduc, în mod accidental sau ilegal, la distrugerea, pierderea, modificarea, sau divulgarea neautorizată a datelor cu caracter personal transmise, stocate sau prelucrate într-un alt mod prin sistemele informatice și de comunicații, sau la accesul neautorizat la acestea.Utilizatorul răspunde personal de securitatea datelor cu caracter personal încredințate prin procedurile de acces la Sistemele Informatice și de Comunicații.
- Integritatea se referă la măsurile și procedurile utilizate împotriva modificărilor, distrugerii, pierderii, în mod accidental sau ilegal, precum și împotriva accesului neautorizat la sistemele informatice și de comunicații.
- Disponibilitatea se asigură prin funcționarea continuă a tuturor componentelor sistemelor informatice și de comunicații. Sistemele informatice utilizate au nevoie de nivele diferite de disponibilitate în funcție de impactul sau daunele produse ca urmare a nefuncționării corespunzătoare.

De asemenea, Politica are ca scop stabilirea cadrului necesar pentru elaborarea procedurilor legate de gestionarea și utilizarea sistemelor informatice și de comunicații.

2. Domeniu aplicare

2.1. Domeniul de aplicare personal
Prezenta politică este aplicabilă următoarelor persoane, care sunt obligate să respecte prevederile acesteia: tuturor Departamentelor / Serviciilor / Birourilor din cadrul ***UNIVERSITATEA "DIMITRIE CANTEMIR" DIN TÂRGU MUREȘ***; tuturor Angajaților; tuturor Colaboratorilor (denumite în continuare „Utilizatorul").

2.2. Domeniul de aplicare material
Prezenta politică se aplică tuturor operațiunilor de prelucrare a datelor cu caracter personal prin sistemele informatice și de comunicare realizate de / în numele ***UNIVERSITATEA "DIMITRIE CANTEMIR" DIN TÂRGU MUREȘ.***

2.3. Domeniul de aplicare temporal

2.3.1. Politica se aplică operațiunilor de prelucrare a datelor cu caracter personal prin sistemele informatice realizate de / în numele ***UNIVERSITATEA "DIMITRIE CANTEMIR" DIN TÂRGU MUREȘ*** începând cu data de 25 mai 2018 (inclusiv), indiferent dacă prelucrările respective sunt în curs la data respectivă sau încep la sau după data respectivă.

2.3.2. Angajații și Colaboratorii vor fi înștiințați despre prevederile acesteia, iar Angajații și Colaboratorii cei mai importanți din punctul de vedere al activităților de prelucrare a

datelor în care sunt implicați au fost și vor fi instruiți cu privire la prevederile acesteia și ale legislației României și ale Uniunii Europene privind protecția datelor cu caracter personal.

3. Cadru legal, politici și proceduri adoptate de *UNIVERSITATEA "DIMITRIE CANTEMIR" DIN TÂRGU MUREȘ*

3.1. Cadru legal

Începând cu data de 25 mai 2018, principalul act normativ aplicabil la nivelul întregii Uniuni Europene este Regulamentul (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, cunoscut și sub denumirea Regulamentul general privind protecția datelor („GDPR" sau „Regulamentul").

Au fost analizate:

- Regulamentul (UE) 679/2016 al Parlamentului European și al Consiliului („GDPR" sau „Regulamentul")
- Legea nr. 190/2018 privind măsuri de punere în aplicare a Regulamentului (UE) 2016/679 al Parlamentului European și al Consiliului
- Politica *UNIVERSITATEA "DIMITRIE CANTEMIR" DIN TÂRGU MUREȘ* privind Protecția Datelor
- SR ISO/CEI 27001: 2013 - Tehnologia informației. Tehnici de securitate. Sisteme de management a securității informației;
- SR ISO/CEI 27002: 2018 - Tehnologia informației. Tehnici de securitate. Cod de bună practică pentru managementul securității informației;
- Ghidul de securitate informatică pentru funcționarii publici. CERT-RO;

Totodată, în vederea redactării Politicii au fost analizat Ghidurile și Opiniile emise de Comitetul European pentru Protecția Datelor.

3.2. Politici și proceduri IT&C asociate

Utilizatorii resurselor informatice și de comunicație ale UNIVERSITATEA "DIMITRIE CANTEMIR" DIN TÂRGU MUREȘ trebuie să respecte politicile și procedurile adoptate de *UNIVERSITATEA "DIMITRIE CANTEMIR" DIN TÂRGU MUREȘ*.

4. Sumarizarea politicii

4.1. Informații generale

Resursele informatice și de comunicații sunt bunuri strategice ale UNIVERSITATEA "DIMITRIE CANTEMIR" DIN TÂRGU MUREȘ și fac parte integrantă din activitatea acesteia. Sistemele informatice și de comunicații sunt esențiale pentru buna desfășurare a activităților întreprinse de *UNIVERSITATEA "DIMITRIE CANTEMIR" DIN TÂRGU MUREȘ* și de aceea se reclamă o cât mai bună administrare a acestora.

Compromiterea securității, disponibilității și integrității acestor resurse poate afecta capacitatea *UNIVERSITATEA "DIMITRIE CANTEMIR" DIN TÂRGU MUREȘ* de a oferi servicii informatice și de comunicații și poate conduce la fraude, încălcări ale protecției datelor cu caracter personal, la distrugerea datelor, la violarea clauzelor contractuale,

divulgarea secretelor, la afectarea reputației ***UNIVERSITATEA "DIMITRIE CANTEMIR" DIN TÂRGU MUREȘ***.

Această politică este stabilită astfel încât:

- să fie în conformitate cu statutul, regulamentele, legile şi alte documente oficiale în vigoare privind administrarea resurselor informatice şi de comunicaţii;
- să stabilească practici prudente şi acceptabile privind utilizarea resurselor informatice şi de comunicaţii ale ***UNIVERSITATEA "DIMITRIE CANTEMIR" DIN TÂRGU MUREȘ***;
- să instruiască utilizatorii care au dreptul de folosire a acestor resurse privind responsabilităţile asociate utilizării acestora;
- să protejeze această investiţie;
- să protejeze informaţiile conţinute în aceste sisteme;
- să protejeze renumele ***UNIVERSITATEA "DIMITRIE CANTEMIR" DIN TÂRGU MUREȘ.***

4.2. Confidenţialitate

În scopul administrării Resurselor Informatice şi de Comunicaţii şi pentru asigurarea securităţii acestora, personalul autorizat poate revizui sau utiliza orice informaţie stocată pe / sau transportată prin sistemele Resurselor Informatice şi de Comunicaţii în conformitate cu legile în vigoare şi cu respectarea în special a normelor privind protecţia datelor cu caracter personal.

Utilizatorii vor avea grijă să nu încalce drepturile şi libertăţile altor persoane atunci când utilizează echipamentele (de exemplu, când fac înregistrări audio-video la locul de muncă).

De asemenea, utilizatorii au obligaţia să raporteze orice slăbiciune în sistemul de securitate al sistemelor informatice şi de comunicaţii din cadrul ***UNIVERSITATEA "DIMITRIE CANTEMIR" DIN TÂRGU MUREȘ***, precum şi orice întrebuinţare realizată cu încălcarea acestei politici ori a normelor legale în general.

Utilizatorul trebuie să se asigure că informaţiile aparţinând sau aflate în custodia ***UNIVERSITATEA "DIMITRIE CANTEMIR" DIN TÂRGU MUREȘ*** rămân sub controlul ***UNIVERSITATEA "DIMITRIE CANTEMIR" DIN TÂRGU MUREȘ*** în orice moment.

Utilizatorilor le este interzis să acceseze informaţii sau programe de pe sistemele informatice şi de comunicaţii ale ***UNIVERSITATEA "DIMITRIE CANTEMIR" DIN TÂRGU MUREȘ*** pentru care nu au autorizaţie sau consimţământ explicit.

Nici un utilizator al Resurselor informatice şi de comunicaţii ale ***UNIVERSITATEA "DIMITRIE CANTEMIR" DIN TÂRGU MUREȘ*** nu poate divulga informaţiile la care are acces sau la care a avut acces ca urmare a unei vulnerabilităţi a sistemelor ce compun Resursele informatice şi de comunicaţii. Această obligaţie subzistă şi după ce raportul juridic dintre utilizator şi ***UNIVERSITATEA "DIMITRIE CANTEMIR" DIN TÂRGU MUREȘ*** s-a stins.

Stocarea de informaţii în interes de serviciu pe alte resurse informatice şi de comunicaţie decât cele aflate sub controlul ***UNIVERSITATEA "DIMITRIE CANTEMIR" DIN TÂRGU MUREȘ***, inclusiv pe sisteme IT & C administrate de terţi cu care ***UNIVERSITATEA "DIMITRIE CANTEMIR" DIN TÂRGU MUREȘ*** nu are o legătură contractuală, este strict interzisă. Această regulă implică şi intedicţia de a utiliza în interes de serviciu un cont de e-mail care nu este furnizat de ***UNIVERSITATEA "DIMITRIE CANTEMIR" DIN TÂRGU MUREȘ***.

Interdicţia de stocare antemenţionată nu se extinde şi asupra operaţiunii de transmitere, astfel încât anumite informaţii pot fi transmise prin intermediul resurselor de comunicaţii ale terţilor

în măsura în care se asigură confidențialitatea datelor respective. În acest sens, fără a se limita la aceasta, se vor lua în considerare tehnici de criptare a informațiilor transmise. Obligația de a asigura confidențialitatea și integritatea informațiilor ***UNIVERSITATEA "DIMITRIE CANTEMIR" DIN TÂRGU MUREȘ*** transmise pe această cale incumbă utilizatorilor.

4.3. Protecția datelor cu caracter personal

Având în vedere că resursele informatice și de comunicații ale ***UNIVERSITATEA "DIMITRIE CANTEMIR" DIN TÂRGU MUREȘ*** sunt utilizate și pentru prelucrarea datelor cu caracter personal, se cuvine a se reitera câteva dintre aspectele esențiale prevăzute de Politica privind Protecția Datelor cu Caracter Personal. Oricărei prelucrări a datelor cu caracter personal efectuată prin sistemele informatice și de comunicare ale ***UNIVERSITATEA "DIMITRIE CANTEMIR" DIN TÂRGU MUREȘ*** trebuie să îi fie atribuită un temei din cele prevăzute la art. 6 din GDPR, temeiuri care sunt detaliate și în Politica privind Protecția Datelor cu Caracter Personal a ***UNIVERSITATEA "DIMITRIE CANTEMIR" DIN TÂRGU MUREȘ***.
De asemenea, toate operațiunile de prelucrare vor fi efectuate în conformitate cu principiile enumerate de GDPR la art. 5 și Politica privind Protecția Datelor cu Caracter Personal a ***UNIVERSITATEA "DIMITRIE CANTEMIR" DIN TÂRGU MUREȘ***, mai precis vor respecta principiile legalității, echității, transparenței, exactității, integrității și confidențialității, precum și principiul reducerii la minimum a datelor.
În acest sens, ***UNIVERSITATEA "DIMITRIE CANTEMIR" DIN TÂRGU MUREȘ*** ia toate măsurile tehnice și organizatorice necesare pentru a asigura securitatea adecvată a datelor cu caracter personal, inclusiv protecția împotriva prelucrării neautorizate sau ilegale și împotriva pierderii, a distrugerii sau a deteriorării accidentale, măsuri care sunt detaliate și de prezenta politică.
Tot în scopul satisfacerii exigențelor impuse de GDPR, ***UNIVERSITATEA "DIMITRIE CANTEMIR" DIN TÂRGU MUREȘ*** își execută obligațiile corelative drepturilor ai căror titulari sunt persoanele vizate și anume: dreptul de acces, dreptul la rectificare, dreptul la ștergerea datelor, dreptul la restricționarea prelucrării, dreptul la portabilitatea datelor, precum și dreptul la opoziție.
Pentru mai multe detalii a se consulta Politica privind Protecția Datelor cu Caracter Personal a ***UNIVERSITATEA "DIMITRIE CANTEMIR" DIN TÂRGU MUREȘ.***

4.4. Administrarea conturilor

Administrarea și gestiunea conturilor de acces la sistemele informatice și de comunicație ale ***UNIVERSITATEA "DIMITRIE CANTEMIR" DIN TÂRGU MUREȘ*** se va realiza cu respectarea prevederilor din materia protecției datelor cu caracter personal. În acest sens, ***UNIVERSITATEA "DIMITRIE CANTEMIR" DIN TÂRGU MUREȘ*** îi incumbă toate obligațiile prevăzute de GDPR în sarcina operatorilor de date cu caracter personal față de utilizatorii persoane fizice ale căror date sunt prelucrate în scopul administrării conturilor de acces.
Conturile de acces se creează pe bază de cerere și aprobare corespunzătoare. Toate conturile de acces se vor crea în formatul standard cont utilizator prenume.nume.
Prin contractul de muncă și/sau alte acte juridice corespunzătoare utilizatorii declară că au luat la cunoștință și acceptă prevederile privind securitatea sistemului informatic și de comunicație.

Toţi utilizatorii sunt obligaţi să păstreze confidenţialitatea informaţiilor privind contul de acces.
Toate conturile trebuie să se poată identifica în mod unic, utilizând numele de cont asociat.
Toate parolele pentru conturi trebuie să fie create şi folosite în conformitate cu politica privind securitatea informaţiilor.
Toate conturile utilizator care nu au fost accesate timp de 90 de zile vor fi dezactivate. După încă 90 zile conturile vor fi şterse dacă nu s-a solicitat accesul la acestea.
Conturile de utilizator pot fi modificate doar pe baza procedurii de modificare a conturilor de utilizator de către Departamentul / Personalul IT&C în situaţii precum: schimbarea numelui de familie, modificarea drepturilor de utilizator, numele contului etc.

4.5. Politica pentru parole

Accesul la sistemul informatic al ***UNIVERSITATEA "DIMITRIE CANTEMIR" DIN TÂRGU MUREȘ*** este restricţionat pe bază de nume de utilizator şi parolă. Toţi utilizatorii care au acces la informaţii şi sisteme trebuie să respecte următorarele cerinţe referitoare la folosirea parolelor:
Alegerea unei parole:

- Utilizatorii trebuie să aleagă parole greu de ghicit. Astfel, parolele alese nu trebuie să se regăsească în dicţionar şi să nu reflecte aspecte din viaţa lor personală. Toate parolele trebuie să aibă cel puţin 12 caractere, iar lungimea lor minimă trebuie să fie impusă de sistem când acesta o permite. Utilizatorii trebuie să aleagă parole care includ caractere şi cifre.
- Când aleg parole, utilizatorii trebuie să urmeze standardele pentru parole implementate în ***UNIVERSITATEA "DIMITRIE CANTEMIR" DIN TÂRGU MUREȘ***.

Schimbarea parolelor

Parolele alese de utilizatori nu trebuie să fie refolosite. Acolo unde sistemele o permit parolele vor fi schimbate obligatoriu la 35 de zile şi vor fi schimbate atunci când sunt folosite prima data. Dacă sistemele o permit, ultimele 12 parole vor fi reţinute pentru a nu permite reutilizarea acestora. Dacă un utilizator suspectează că altcineva i-ar putea cunoaşte parola, aceasta trebuie schimbată imediat. Departamentul / Personalul IT&C nu va reseta parola unui utilizator decât dacă acesta este identificat.

Protejarea parolelor

Utilizatorii nu trebuie să divulge parolele nimănui, nici măcar managerilor şi colegilor. Utilizatorii trebuie să folosească mecanismele de autorizare pentru a partaja informaţia aşa cum sunt directoarele partajate de pe server, poşta electronica sau paginile de intranet. Utilizatorii nu trebuie să stocheze parolele în fişiere, precum ar fi script-urile sau programe de calculator, decât dacă parolele au fost criptate cu un program de criptare autorizat. Parolele nu trebuie să fie scrise pe hârtii. Toate parolele setate implicit de furnizorul echipamentului sau programului trebuie să fie schimbate înainte să fie folosite în activităţile ***UNIVERSITATEA "DIMITRIE CANTEMIR" DIN TÂRGU MUREȘ.***
Toate sistemele IT ale ***UNIVERSITATEA "DIMITRIE CANTEMIR" DIN TÂRGU***

MUREȘ vor fi setate în așa fel încât accesul utilizatorilor va fi blocat automat în cazul în care își introduc parola greșit de cinci ori consecutiv.

4.6. Acordare și retragere accesului la date, sisteme informatice și site-uri web

Trebuie precizat în primul rând că accesul la date, sisteme informatice și / sau site-uri web poate implica o prelucrare de date cu caracter personal suplimentară, având în vedere că prin resursele informatice și de comunicații ale ***UNIVERSITATEA "DIMITRIE CANTEMIR" DIN TÂRGU MUREȘ*** sunt prelucrate date cu caracter personal. Prin urmare, și în aceste situații se reclamă respectarea obligațiilor impuse de către legislția privind protecția datelor cu caracter personal.
Acordarea accesului pentru angajați se va face de către Departamentul / Personalul IT&C în urma transmiterii de către Personalul Resurse Umane a unui formular care va conține detalii legate de utilizator și drepturile acestuia. Formularul se va retrimite în cazul modificării numelui utilizatorului, a drepturilor utilizatorului ca urmare a schimbării postului de lucru sau în cazul încetării contractului de muncă.
Acordarea accesului pentru persoanele vizate se va face de către Departamentul / Personalul IT&C în urma transmiterii de către Management, a unui formular care va conține detalii legate de utilizator și drepturile acestuia.
Acordarea accesului pentru persoanele vizate, vizitatori, furnizori sau alte categorii de utilizatori, se va face de către Departamentul / Personalul IT&C în urma transmiterii de către Departamentele / Serviciile interesate a unui formular ce va conține detalii legate de utilizator precum și de durata activării contului de utilizator și drepturile acestuia.
Accesul la sistemele informatice și site-urile web utilizate de ***UNIVERSITATEA "DIMITRIE CANTEMIR" DIN TÂRGU MUREȘ*** se va face conform procedurilor de acces ale acestor sisteme informatice și site-uri web.

4.7. Identificare și autentificare

Utilizatorul este responsabil pentru securitatea datelor, a informațiilor de autentificare și a sistemelor aflate sub controlul său precum și de respectarea normelor privind protecția datelor cu caracter personal în situația în care efectuează operațiuni de prelucrare în accepțiunea GDPR.
Utilizatorul trebuie să păstreze credențialele de acces (nume utilizator, parolă, token etc.) în siguranță și să nu le împărtășească nici unei alte persoane (inclusiv colegi, membri ai familiei sau prieteni). Corelativ, utilizatorilor le este interzisă aflarea cu intenție a parolelor altor utilizatori ai resurselor informatice și de comunicații ale ***UNIVERSITATEA "DIMITRIE CANTEMIR" DIN TÂRGU MUREȘ***. În acest sens, ca o garanție suplimentară a confidențialității parolelor se interzice comunicarea acestora prin intermediul sistemelor de comunicații (e-mail, mesagerie instant, SMS etc.).
Cu toate acestea, în situații justificate este permisă utilizarea de aplicații autorizate de management al parolelor, totuși folosirea acestor aplicații pentru a stoca parole de domeniu, parole administrative sau parole de acces la aplicații sau servicii critice este interzisă.
Contul de acces poate fi utilizat numai de către persoana căreia i-a fost atribuit respectivul cont. Pe cale de consecință, asigurarea accesului unei alte persoane din culpa utilizatorului este interzisă. Aceasta cu atât mai mult cu cât accesul unei terțe persoane poate cauza compromiterea integrității și securității informațiilor cu care operează ***UNIVERSITATEA "DIMITRIE CANTEMIR" DIN TÂRGU MUREȘ*** prin intermediul sistemelor informatice

şi de comunicaţie.
Este strict interzis ca utilizatorul să acceseze fişiere, calculatoare sau orice alt dispozitiv din sistemul informatic şi de comunicaţii al ***UNIVERSITATEA "DIMITRIE CANTEMIR" DIN TÂRGU MUREŞ*** fără ca acesta să aibă autorizaţie în acest sens. Autorul acestei fapte va fi sancţionat sever potrivit legii.
Pentru a evita accesul neautorizat al altor persoane decât utilizatorul la contul acestuia din urmă, utilizatorul este obligat ca de fiecare dată când părăseşte dispozitivul cu care accesează resursele informatice şi de comunicaţie ale ***UNIVERSITATEA "DIMITRIE CANTEMIR" DIN TÂRGU MUREŞ*** să se deconecteze de la sistem prin funcţia „log off".

4.8. Acces administrativ

Serviciile şi Departamentele ***UNIVERSITATEA "DIMITRIE CANTEMIR" DIN TÂRGU MUREŞ*** trebuie să prezinte Departamentul / Personalul IT&C o listă cu persoanele de contact cu drept de administrator pentru toate sistemele informatice conectate la reţeaua de comunicaţii a UNIVERSITATEA "DIMITRIE CANTEMIR" DIN TÂRGU MUREŞ. Această listă trebuie refăcută şi prezentată Departamentul / Personalul IT&C de fiecare dată când apar modificări de orice natură.
Utilizatorii trebuie să cunoască şi să accepte toate prevederile privind securitatea sistemului informatic înainte de a li se permite accesul la un cont.
Utilizatorii care au conturi de acces de tip administrativ trebuie să aibă instrucţiuni de administrare, documentare, instruire şi autorizare a conturilor. Aceste instrucţiuni se vor elabora de către fiecare furnizor de sistem informatic şi vor fi incluse în fişa postului.
Utilizatorii cu drepturi de acces administrative sau speciale nu trebuie să folosească în mod abuziv aceste drepturi şi trebuie să facă investigaţii numai sub îndrumarea superiorului direct.
Cei care utilizează conturi de acces cu drepturi administrative sau speciale trebuie să folosească tipul de privilegiu cel mai potrivit activităţii pe care o desfăşoară.
Accesul administrativ trebuie să se conformeze politicii privind managementul parolelor.
Parola pentru un cont cu acces privilegiat nu va fi utilizată de mai multe persoane decât cu acordul scris al superiorului direct şi trebuie să fie schimbată atunci când persoana care utilizează acest cont îşi schimbă locul de muncă în cadrul ***UNIVERSITATEA "DIMITRIE CANTEMIR" DIN TÂRGU MUREŞ***, sau în cazul unei modificări a listei de personal care furnizează servicii din partea terţilor având contracte cu ***UNIVERSITATEA "DIMITRIE CANTEMIR" DIN TÂRGU MUREŞ***.
Unele conturi sunt necesare pentru audit (verificare, control) intern sau extern, pentru dezvoltare sau instalare de software sau alte operaţiuni definite. Acestea trebuie să îndeplinească următoarele condiţii:

- trebuie să fie autorizate;
- trebuie să fie create cu dată de expirare specifică;
- contul va fi şters atunci când nu mai este necesar.

4.9. Accesul la reţeaua de comunicaţii

Utilizatorilor le este permis să utilizeze numai parametrii pentru conectare la reţea specificaţi de către Departamentul / Personalul IT&C.
Conducătorii structurii organizatorice trebuie să aprobe, în scris, conectarea dispozitivelor de calcul la reţeaua de comunicaţii a ***UNIVERSITATEA "DIMITRIE CANTEMIR" DIN TÂRGU MUREŞ***. Pentru fiecare sistem conectat trebuie să existe o persoană care să răspundă

de acesta, numele şi datele de identificare ale acesteia se vor comunica către Departamentul / Personalul IT&C.
Conectarea sistemelor de calcul care nu sunt proprietatea ***UNIVERSITATEA "DIMITRIE CANTEMIR" DIN TÂRGU MUREŞ*** se face numai cu aprobarea în scris a superiorului direct al solicitantului.
Accesul de la distanţă la reţeaua ***UNIVERSITATEA "DIMITRIE CANTEMIR" DIN TÂRGU MUREŞ*** se va realiza numai prin echipamente aprobate, folosind protocoale aprobate de către Departamentul / Personalul IT&C şi managementul ***UNIVERSITATEA "DIMITRIE CANTEMIR" DIN TÂRGU MUREŞ***.
Utilizatorii din interiorul reţelei de comunicaţie a ***UNIVERSITATEA "DIMITRIE CANTEMIR" DIN TÂRGU MUREŞ*** nu se pot conecta la altă reţea.
Utilizatorii nu trebuie să extindă sau să retransmită serviciile de reţea în nici un fel (pe nicio cale). Nu este permisă instalarea de conexiuni de reţea neautorizate indiferent de motiv.
Utilizatorii nu trebuie să instaleze echipamente hardware sau programe care furnizează servicii de reţea fără aprobarea Departamentul / Personalul IT&C.
Sistemele computerizate din afara ***UNIVERSITATEA "DIMITRIE CANTEMIR" DIN TÂRGU MUREŞ*** care necesită conectare la reţea trebuie să se conformeze cu standardele reţelei interne ale ***UNIVERSITATEA "DIMITRIE CANTEMIR" DIN TÂRGU MUREŞ.***
Este interzis utilizatorilor să descarce, să instaleze sau să ruleze programe de securitate care pot determina vulnerabilităţi în securitatea unui sistem informatic şi de comunicaţii. De exemplu, utilizatorilor ***UNIVERSITATEA "DIMITRIE CANTEMIR" DIN TÂRGU MUREŞ*** le este interzis să ruleze programe de spargere a parolei, sustragere de pachete, scanare a porturilor, în timp ce sunt conectaţi la reţeaua ***UNIVERSITATEA "DIMITRIE CANTEMIR" DIN TÂRGU MUREŞ***.
Utilizatorii nu au dreptul să modifice, reconfigureze, instaleze, dezinstaleze echipamente de reţea, cabluri sau prize de conexiuni.
Serviciul de administrare a numelor şi adreselor IP este deservit exclusiv de către Departamentul / Personalul IT&C.
Serviciile de interconectare a reţelei ***UNIVERSITATEA "DIMITRIE CANTEMIR" DIN TÂRGU MUREŞ*** cu alte reţele sunt realizate exclusiv de către Departamentul / Personalul IT&C.
Nu este permisă instalarea şi/sau modificarea echipamentelor utilizate pentru conectare la reţea (inclusiv plăci de reţea) fără aprobarea Departamentului / Personalului IT&C. Tipul şi modelul plăcilor de reţea şi tuturor echipamentelor care se pot conecta în reţea trebuie să fie aprobate de către Departamentul / Personalul IT&C.

4.10. Configurarea sistemelor informatice pentru accesul la reţeaua de comunicaţii

Infrastructura de comunicaţii şi reţeaua de comunicaţii digitale a ***UNIVERSITATEA "DIMITRIE CANTEMIR" DIN TÂRGU MUREŞ*** este administrată de către Departamentul / Personalul IT&C, care este responsabil cu întreţinerea şi dezvoltarea acesteia.
Pentru a furniza o infrastructură de comunicaţii unitară cu posibilităţi de modernizare, toate componentele acesteia sunt instalate de către Departamentul / Personalul IT&C sau de către un furnizor avizat explicit de către Departamentul / Personalul IT&C.
Toate echipamentele, fără excepţie, conectate la reţeaua de comunicaţii trebuie configurate conform specificaţiilor Departamentului / Personalului IT&C.
Toate dispozitivele hardware, inclusiv plăcile de reţea, care se vor conecta la reţeaua ***UNIVERSITATEA "DIMITRIE CANTEMIR" DIN TÂRGU MUREŞ***, trebuie să fie

însoţite de o aprobare tip (producător, model etc.) din partea Departamentului / Personalului IT&C.
Modificarea configuraţiei oricărui dispozitiv activ conectat la reţeaua de comunicaţii se face numai cu aprobarea Departamentului / Personalului IT&C.
Infrastructura de comunicaţii de date a ***UNIVERSITATEA "DIMITRIE CANTEMIR" DIN TÂRGU MUREŞ*** suportă un set definit de protocoale de reţea (TCP/IP). Orice utilizare a altui set de protocoale trebuie să fie aprobată în scris de către Departamentul / Personalul IT&C.
Adresele de reţea sunt alocate dinamic sau static numai de către Departamentul / Personalul IT&C.
Toate conectările în reţeaua de comunicaţii a ***UNIVERSITATEA "DIMITRIE CANTEMIR" DIN TÂRGU MUREŞ*** reprezintă sarcină a Departamentului / Personalului IT&C. Conectarea se va face numai în baza unei cereri standard aprobată de către superiorul direct.
Toate conectările dintre reţeaua de comunicaţii a ***UNIVERSITATEA "DIMITRIE CANTEMIR" DIN TÂRGU MUREŞ*** „şi alte reţele de comunicaţii, publice sau private, sunt responsabilitatea exclusivă a Departamentului / Personalului IT&C.
Echipamentele de protecţie a reţelei de comunicaţie a ***UNIVERSITATEA "DIMITRIE CANTEMIR" DIN TÂRGU MUREŞ*** (firewall) se vor instala de către Departamentul / Personalul IT&C.
Utilizatorii nu au dreptul să extindă sau să retransmită în nici un fel serviciile reţelei (este interzisă instalarea unui modem, router, switch, hub sau punct de acces la reţeaua ***UNIVERSITATEA "DIMITRIE CANTEMIR" DIN TÂRGU MUREŞ***) fără aprobare din partea Departamentului / Personalului IT&C.
Utilizatorilor li se interzice instalarea de dispozitive hardware de reţea sau de programe care furnizează servicii de reţea fără aprobarea Departamentului / Personalului IT&C.
Utilizatorilor nu le este permis accesul la dispozitivele hardware ale reţelei.

4.11. Utilizarea echipamentelor

Utilizatorul este responsabil de păstrarea în siguranţă şi folosirea corectă în scopurile destinate şi autorizate a echipamentelor care i-au fost puse la dispoziţie de ***UNIVERSITATEA "DIMITRIE CANTEMIR" DIN TÂRGU MUREŞ***. Acestea includ staţii de lucru fixe şi mobile, imprimante, telefoane mobile şi fixe şi alte mijloace de procesare a informaţiilor, inclusiv software-ul asociat.
Toate staţiile de lucru trebuie să fie asigurate împotriva accesului neautorizat atunci când sunt lăsate nesupravegheate, mai ales că prin acestea utilizatorii prelucrează date cu caracter personal în scopurile declarate prin Politica ***UNIVERSITATEA "DIMITRIE CANTEMIR" DIN TÂRGU MUREŞ*** privind Protecţia Datelor cu Caracter Personal. Aceasta se poate face prin blocarea calculatorului, log off sau cu un Screensaver protejat cu parolă, cu funcţia de activare automată setată la 5 minute sau mai puţin. La sfârşitul programului de lucru acestea, precum şi orice aparatură electrică şi electronică, trebuie să fie oprite.
De asemenea:

- CD-urile, DVD-urile şi orice alte medii de stocare trebuie să fie păstrate într-o locaţie aptă să prevină orice încălcare a securităţii, mai ales că acestea ar putea conţine date cu caracter personal.
- Daca ele conţin date de maximă confidenţialitate, atunci la locaţia antemenţionată vor

avea acces doar persoanele autorizate în conformitate cu prevederile legale..

- Mai mult decât atât, CD-urile, DVD-urile şi mediile de stocare mobile trebuie păstrate departe de acţiunile mediului înconjurător cum ar fi: surse de căldura, lumina directă a soarelui şi câmpuri magnetice ce ar putea altera integritatea informaţiilor stocate.
- În măsura în care CD-urile, DVD-urile sau celelalte medii de stocare păstrează date cu caracter personal, atunci acestea vor fi stocate doar pentru perioada necesară efectuării prelucrării pentru care au fost colectate, în conformitate cu prevederile din materia protecţiei datelor cu caracter personal.

Dispozitivele care nu aparţin ***UNIVERSITATEA "DIMITRIE CANTEMIR" DIN TÂRGU MUREŞ*** şi care se conectează la reţeaua ***UNIVERSITATEA "DIMITRIE CANTEMIR" DIN TÂRGU MUREŞ*** trebuie să se conformeze *Procedurii privind utilizarea echipamentelor de proprietate personală.* Echipamentele conectate fară autorizare sunt expuse monitorizării şi vor fi blocate fară avertisment de îndată ce sunt detectate.

Următoarele acţiuni sunt strict interzise utilizatorilor:

- modificarea sau eliminarea măsurilor de securitate, inclusiv, dar fără a se limita la: dezinstalarea sau dezactivarea antivirusului ori modificarea setărilor de actualizare ale acestuia (actualizarea automată trebuie să fie activă), dezactivarea sau modificarea setărilor firewall-ului, instalarea de software neautorizat (vezi Lista de software autorizat) sau pentru care nu există licenţă valabilă la zi,
- interferenţa cu procedurile ***UNIVERSITATEA "DIMITRIE CANTEMIR" DIN TÂRGU MUREŞ*** referitoare la managementul dispozitivelor, inclusiv, dar fără a se limita la: schimbarea sau reinstalarea sistemului de operare, redenumirea calculatorului, scoaterea din domeniu, instalarea neautorizată de dispozitive suplimentare, modificarea configuraţiei hardware a echipamentului, scoaterea echipamentului în afara locaţiei fără autorizare prealabilă,
- introducerea şi utilizarea de produse care pun în pericol securitatea informaţiilor (dispozitive sau software de ascultare, conectare, înregistrare sau copiere neautorizată) sau a personalului (arme de orice fel, produse toxice sau explozive etc.),
- eliminarea nesigură a mediilor de stocare sau a echipamentelor care au în componenţă medii de stocare.

4.12. Securitatea echipamentelor şi resurselor în afara locaţiilor administrate de ***UNIVERSITATEA "DIMITRIE CANTEMIR" DIN TÂRGU MUREŞ***

Folosirea echipamentelor în afara locaţiilor aflate sub administrarea ***UNIVERSITATEA "DIMITRIE CANTEMIR" DIN TÂRGU MUREŞ*** cresc riscurile de securitate ale acestora, echipamentele fiind în special vulnerabile la daune fizice, pierdere şi furt. în acest caz, se vor aplica următoarele măsuri de securitate:

- în momentul părăsirii ***UNIVERSITATEA "DIMITRIE CANTEMIR" DIN TÂRGU MUREŞ***, echipamentul poate fi utilizat pentru resursele Online (ex. e-mail) şi va exista acces la informaţiile statice;
- Update-urile aplicaţiilor (de exemplu: sistem de operare, antivirus, Suita Office etc.) se vor face doar la revenirea cu echipamentul în reţeaua ***UNIVERSITATEA "DIMITRIE CANTEMIR" DIN TÂRGU MUREŞ***. Utilizatorul are obligaţia ca la un interval de maximum 2 săptămâni să introducă echipamentul în reţeaua internă a ***UNIVERSITATEA "DIMITRIE CANTEMIR" DIN TÂRGU MUREŞ*** pentru actualizări;
- Accesul la aplicaţiile de pe serverele ***UNIVERSITATEA "DIMITRIE CANTEMIR" DIN TÂRGU MUREŞ*** se va face prin VPN cu aprobarea superiorului direct,

aprobarea pentru utilizarea VPN-ului fiind comunicată Departamentului / Personalului IT&C;

- Documentele personale (valabil pentru toate echipamentele) se vor ţine într-un folder "Personal".

Furtul sau pierderea unui echipament scos în afara ***UNIVERSITATEA "DIMITRIE CANTEMIR" DIN TÂRGU MUREŞ*** vor fi raportate imediat superiorului şi Departamentului / Personalului IT&C.
Detalii suplimentare în *Politica privind dispozitivele mobile şi lucrul de la distanţă.*

4.13. Utilizarea echipamentelor proprietate personală

UNIVERSITATEA "DIMITRIE CANTEMIR" DIN TÂRGU MUREŞ poate permite angajaţilor sau persoanelor terţe să folosească echipamente proprietate personală (EPP) pentru îndeplinirea sarcinilor de serviciu.
Următoarele echipamente proprietate personală sunt permise:

- dispozitive de tip smartphone având sisteme de operare: iOS, Android, Blackberry sau Windows;
- tablete având sisteme de operare: iOS, Android, Windows;
- laptop-uri:
- dispozitive de stocare portabile: stick-uri de memorie USB, carduri de memorie, hard-disk-uri portabile etc.

Utilizarea echipamentelor proprietate personală este asociată cu o serie de riscuri de securitate a informaţiilor, cum ar fi:

- pierderea, dezvăluirea sau alterarea informaţiilor ***UNIVERSITATEA "DIMITRIE CANTEMIR" DIN TÂRGU MUREŞ*** stocate pe EPP; incidente care implică ameninţări la adresa infrastructurii informatice a ***UNIVERSITATEA "DIMITRIE CANTEMIR" DIN TÂRGU MUREŞ*** sau compromiterea acestei infrastructuri (de exemplu: viruşi, malware, hacking); nerespectarea legilor, reglementărilor şi obligaţiilor contractuale (de exemplu, protecţia datelor cu caracter personal, legislaţia anti-piraterie etc.);
- nerespectarea drepturilor de proprietate intelectuală pentru informaţiile ***UNIVERSITATEA "DIMITRIE CANTEMIR" DIN TÂRGU MUREŞ*** create, stocate, procesate sau transmise pe EPP.

Angajaţii care folosesc EPP pentru îndeplinirea sarcinilor de serviciu trebuie să fie autorizaţi în mod explicit să facă acest lucru. Autorizarea va fi dată de Departamentul / Personalul IT&C la cererea superiorului direct ca răspuns la o solicitare motivată. Pentru autorizare, Departamentul / Personalul IT&C va putea cere informaţii suplimentare despre EPP care va fi utilizat fără a afecta dreptul solicitantului la protecţia datelor cu caracter personal.
Utilizatorii trebuie să asigure aceleaşi măsuri de protecţie a informaţiilor ca şi cele aplicate pentru echipamentele ***UNIVERSITATEA "DIMITRIE CANTEMIR" DIN TÂRGU MUREŞ*** şi nu trebuie să introducă riscuri inacceptabile (exemplu: malware) în reţeaua ***UNIVERSITATEA "DIMITRIE CANTEMIR" DIN TÂRGU MUREŞ*** prin utilizarea de echipamente nesigure.
UNIVERSITATEA "DIMITRIE CANTEMIR" DIN TÂRGU MUREŞ îşi rezervă dreptul de a refuza sau de a retrage autorizarea în cazul în care consideră că echipamentul nu este adecvat şi/sau nu este folosit în interesul UNIVERSITATEA "DIMITRIE CANTEMIR" DIN TÂRGU MUREŞ.
În timp ce utilizatorii au o aşteptare rezonabilă de intimitate asupra informaţiilor lor personale

pe propriul echipament, dreptul ***UNIVERSITATEA "DIMITRIE CANTEMIR" DIN TÂRGU MUREȘ*** de a controla propriile date şi de a gestiona EPP poate duce ocazional la accesul neintenţionat al personalului de asistenţă la informaţiile lor personale. Pentru a evita un astfel de incident , utilizatorii trebuie să păstreze datele lor personale separat de datele ***UNIVERSITATEA "DIMITRIE CANTEMIR" DIN TÂRGU MUREȘ***, în directoare separate, denumite în mod sugestiv.

4.14. Securizarea serverelor

Niciun server nu trebuie conectat la reţeaua ***UNIVERSITATEA "DIMITRIE CANTEMIR" DIN TÂRGU MUREȘ*** până când nu se află într-o stare sigură, nu este apt să prevină orice încălcare a securității datelor din sistem şi nu este acreditat de către Departamentul / Personalul IT&C.
Procedura de securizare a serverelor trebuie să includă obligatoriu următoarele:

- Instalarea sistemului de operare dintr-o sursă aprobată;
- Aplicarea patch-urilor furnizate de producător;
- Înlăturarea programelor, a serviciilor sistem şi a driverelor care nu sunt necesare; Setarea/activarea parametrilor de securitate, a protecţiilor pentru fişiere şi activarea jurnalelor de monitorizare;
- Dezactivarea sau schimbarea parolelor conturilor predefinite;
- Securizarea accesului fizic la aceste echipamente.

Departamentul / Personalul IT&C va monitoriza obligatoriu pentru serverele principale, procesul de instalare şi aplicarea regulată a patch-urilor de securitate.

4.15. Detectarea accesului neautorizat

Procesele de înregistrare şi verificare a activităţii sistemelor de operare, conturilor utilizator şi programelor trebuie să fie funcţionale pe toate sistemele active (host, server, echipamente de reţea). Acestea sunt utilizate cu respectarea normelor privind protecţia datelor cu caracter personal, ele fiind folosite în scopul legitim al asigurării integrității, securității, precum şi disponibilității sistemelor informatice şi de comunicaţie ale ***UNIVERSITATEA "DIMITRIE CANTEMIR" DIN TÂRGU MUREȘ.***
Pe cale de consecință, în măsura în care procesele de înregistrare şi verificare a activității sistemelor de operare, conturilor utilizatorilor şi programelor implică şi o prelucrare de date cu caracter personal în accepțiunea GDPR, atunci se vor naşte toate obligațiile şi drepturile aferente în sarcina ***UNIVERSITATEA "DIMITRIE CANTEMIR" DIN TÂRGU MUREȘ*** şi, respectiv, în favoarea persoanelor vizate.
Trebuie activate funcţiile de anunţare a persoanelor responsabile oferite de firewall-uri şi sistemele de control al accesului la reţea.
Trebuie activate funcţiile de înregistrare a evenimentelor pe dispozitivele firewall şi pe toate sistemele de control ale accesului.
Înregistrările de verificare ale dispozitivelor de control al accesului trebuie monitorizate/revizuite (examinate) zilnic de către Departamentul / Personalul IT&C.
Verificările privind integritatea fiecărui sistem trebuie să se facă periodic. Această activitate este obligatorie şi pentru dispozitivele de tip firewall sau dispozitive de control al accesului.
Înregistrările de verificare pentru serverele din reţeaua internă trebuie revizuite cel puţin săptămânal.
Se vor verifica periodic programele utilitare pentru detectarea tentativelor de acces

neautorizat.
Toate rapoartele privind incidentele trebuie verificate în vederea detectării de indicii ce ar putea implica o activitate de acces neautorizat.
Toate indiciile suspecte sau confirmate de accesări sau încercări de accesare neautorizate trebuie raportate imediat către Departamentul / Personalul IT&C.
Utilizatorii sunt obligaţi să raporteze orice anomalii în performanţa sistemelor utilizate cât şi orice semne ale unor posibile fapte ilicite la Departamentul / Personalul IT&C.

4.16. Modificări ale configuraţiei sistemului

Orice modificare asupra unei componente a configuraţiei sistemului din cadrul ***UNIVERSITATEA "DIMITRIE CANTEMIR" DIN TÂRGU MUREŞ***, cum ar fi: sisteme de operare, componente hardware, echipamente şi componente de reţea, aplicaţii, este supusă prezentei politici şi trebuie să urmeze procedurile în vigoare.
Toate modificările care afectează mediul de funcţionare a sistemelor componente ale sistemului informatic (ex: aparate de aer condiţionat, instalaţii de apă, încălzire, instalaţii electrice şi alarme) trebuie să fie anunţate şi aprobate în scris de departamentul care administrează resursele afectate.
Toate propunerile de modernizare şi extindere a elementelor de infrastructură ale sistemului informatic vor fi documentate şi aprobate de către Departamentul / Personalul IT&C. Nu este permisă modificarea de către utilizatori a elementelor de infrastructură ale sistemului informatic.
Modificările şi modernizările sistemelor de calcul vor fi documentate de către utilizator şi aprobate de către conducerea departamentului sau de către managementul ***UNIVERSITATEA "DIMITRIE CANTEMIR" DIN TÂRGU MUREŞ***.
Modificările planificate trebuie anunţate cu cel puţin 48 ore înainte de a fi executate.
Cererile de modificare planificate pot fi respinse în următoarele cazuri: planificare inadecvată, planuri de refacere a serviciilor inadecvate, durata modificării poate afecta în mod negativ o activitate importantă a ***UNIVERSITATEA "DIMITRIE CANTEMIR" DIN TÂRGU MUREŞ*** sau resursele corespunzătoare necesare nu pot fi disponibile imediat.
Se va întocmi un raport pentru orice modificare, indiferent dacă a fost planificată sau neplanificată, sau dacă s-a realizat sau nu cu succes.
Trebuie întreţinută o bază de date care să cuprindă toate modificările. Aceasta trebuie să conţină cel puţin următoarele informaţii:

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

4.17. Utilizarea reţelei de Internet şi Intranet
Programele pentru acces la reţeaua Internet sunt destinate utilizatorilor autorizaţi pentru a fi folosite în scopul desfăşurării activităţii specificate în fişa postului.
Utilizatorul care foloseşte Internetul, e-mail-ul sau resurse de pe Internet este obligat:

- să se asigure că toate comunicaţiile se fac în scopuri profesionale şi nu interferează cu productivitatea personală.
- ca în situaţia în care va plasa sau trimite pe Internet materiale, conţinutul acestora din urmă (text, imagine, audio sau de orice altă natură) să nu afecteze prestigiul şi renumele ***UNIVERSITATEA "DIMITRIE CANTEMIR" DIN TÂRGU MUREŞ***. Utilizatorul răspunde pentru toate aceste comunicaţii, iar la fiecare dintre acestea va

fi ataşat numele angajatului. Angajatul este obligat să cunoască şi să respecte toate politicile IT&C şi procedurile asociate ale ***UNIVERSITATEA "DIMITRIE CANTEMIR" DIN TÂRGU MUREŞ*** şi de asemenea să păstreze secretul înregistrărilor la nivel personal sau de grup definit prin această politică.

Toate programele utilizate pentru acces la reţeaua Internet trebuie să facă parte din pachetul de programe aprobat de către Departamentul / Personalul IT&C. Aceste programe trebuie să includă toate patch-urile de securitate puse la dispoziţie de către producător.

Toate informaţiile accesate în reţeaua Internet trebuie să se conformeze acestei politici.

Toate fişierele care provin din reţeaua Internet trebuie să fie scanate cu un program antivirus care să fie actualizat cel puţin o dată la 24 ore.

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

Orice activitate a utilizatorilor folosind sistemul informatic poate fi înregistrată şi ulterior examinată, cu respectarea dreptului la protecţia datelor cu caracter personal

Nu este permisă utilizarea sistemelor informatice ale ***UNIVERSITATEA "DIMITRIE CANTEMIR" DIN TÂRGU MUREŞ*** în scop personal sau pentru solicitări personale ce nu au legătură cu ***UNIVERSITATEA "DIMITRIE CANTEMIR" DIN TÂRGU MUREŞ.***

Angajaţilor ce utilizează Internetul nu le este permis să copieze, transfere, redenumească, adauge sau să şteargă informaţii sau programe ce aparţin altor persoane exceptând situaţia când li s-a permis acest lucru, încălcarea drepturilor de autor sau a contractelor de licenţe vor duce la sancţiuni disciplinare din partea ***UNIVERSITATEA "DIMITRIE CANTEMIR" DIN TÂRGU MUREŞ*** şi/sau acţiuni în instanţă ale deţinătorului dreptului de autor.

4.18. Site-uri web ale ***UNIVERSITATEA "DIMITRIE CANTEMIR" DIN TÂRGU MUREŞ***

Toate site-urilor web aparţinând ***UNIVERSITATEA "DIMITRIE CANTEMIR" DIN TÂRGU MUREŞ*** trebuie să se supună regulilor stabilite la nivelul ***UNIVERSITATEA "DIMITRIE CANTEMIR" DIN TÂRGU MUREŞ*** din punct de vedere al aspectului şi al securităţii. Publicaţiile de pe site-urile web ale ***UNIVERSITATEA "DIMITRIE CANTEMIR" DIN TÂRGU MUREŞ*** nu vor conţine materiale care să îndemne la defăimarea ţării şi a naţiunii, la război, la ură naţională, rasială, de clasă sau religioasă; care să incite la discriminare, la separatism teritorial sau la violenţă publică, la fel cum nu vor conţine nici manifestări obscene, contrare bunelor moravuri.

Orice material confidenţial al ***UNIVERSITATEA "DIMITRIE CANTEMIR" DIN TÂRGU MUREŞ*** transmis prin reţeaua Internet trebuie criptat.

4.19. Mijloace de comunicaţie

Adresa de e-mail furnizată de ***UNIVERSITATEA "DIMITRIE CANTEMIR" DIN TÂRGU MUREŞ*** şi mailbox-ul asociat acesteia, adresa IP şi, după caz, numărul de telefon fix, telefon mobil şi conexiunea de date mobile sunt resurse puse la dispoziţia utilizatorilor de ***UNIVERSITATEA "DIMITRIE CANTEMIR" DIN TÂRGU MUREŞ*** pentru a fi folosite la îndeplinirea sarcinilor de serviciu. Utilizarea ocazională în scop personal a acestora este permisă numai dacă nu afectează într-o măsură perceptibilă consumul de resurse al ***UNIVERSITATEA "DIMITRIE CANTEMIR" DIN TÂRGU MUREŞ*** şi nu introduce riscuri suplimentare pentru ***UNIVERSITATEA "DIMITRIE CANTEMIR" DIN TÂRGU MUREŞ***.

Următoarele acţiuni sunt strict interzise utilizatorilor:

- utilizarea necorespunzătoare a mijloacelor de comunicare, inclusiv, dar fără a se limita la: sprijinirea activităţilor ilegale, procurarea şi distribuirea de materiale sau mesaje cu caracter ofensator, rasist, obscen, discriminator sau în scop de hărţuire, defăimare sau ameninţare, procurarea şi distribuirea neautorizată de materiale protejate de drepturile de autor (imagini, muzică, filme, mărci şi logo-uri ale altor companii preluate din reviste, ziare, cărţi sau de pe Internet),
- transmiterea de materiale cu încălcarea drepturilor de proprietate intelectuală , utilizarea mijloacelor de comunicare pentru publicitate neautorizată, relaţii de afaceri care nu implică sau sunt contrare intereselor ***UNIVERSITATEA "DIMITRIE CANTEMIR" DIN TÂRGU MUREȘ***, campanii politice, utilizarea în scop de amuzament sau orice alte scopuri care nu au legătură cu activitatea ***UNIVERSITATEA "DIMITRIE CANTEMIR" DIN TÂRGU MUREȘ***, trimiterea de spam sau bombe e-mail prin intermediul sistemului de e-mail, mesajelor text, mesageriei instant, mesageriei vocale sau altor forme de comunicare electronică utilizate, falsificarea, denaturarea, ascunderea, suprimarea sau înlocuirea unei identităţi de utilizator, pe orice mijloc de comunicare electronică, cu scopul de a induce în eroare destinatarul cu privire la identitatea expeditorului,
- postarea sau transmiterea de mesaje non-business identice sau similare către un număr mare de destinatari (news-group spam),
- transmiterea de informaţii confidenţiale sau secrete de serviciu altor destinatari decât cei autorizaţi să primească aceste informaţii,
- utilizarea adresei de e-mail sau a adresei IP pentru a se angaja în activităţi care încalcă politicile sau orientările ***UNIVERSITATEA "DIMITRIE CANTEMIR" DIN TÂRGU MUREȘ***; postarea pe grupuri publice de ştiri, forumuri sau reţele sociale folosind adresa de e-mail sau adresa IP ale ***UNIVERSITATEA "DIMITRIE CANTEMIR" DIN TÂRGU MUREȘ***, reprezintă compania în faţa publicului şi prin urmare trebuie efectuată cu discernământ pentru a evita reprezentarea greşită sau depăşirea autorităţii de a reprezenta poziţia ***UNIVERSITATEA "DIMITRIE CANTEMIR" DIN TÂRGU MUREȘ.***

Orice mesaj şi/sau informaţie trimisă prin intermediul reţelelor publice pot fi identificate şi atribuite ***UNIVERSITATEA "DIMITRIE CANTEMIR" DIN TÂRGU MUREȘ***. Din acest motiv, postarea pe forumuri sau alte site-uri de informaţii care implică numele sau adrese de e-mail ale ***UNIVERSITATEA "DIMITRIE CANTEMIR" DIN TÂRGU MUREȘ*** se va face fără furnizarea de informaţii confidenţiale sau care pot afecta reputaţia ***UNIVERSITATEA "DIMITRIE CANTEMIR" DIN TÂRGU MUREȘ.***

4.20. Utilizarea resurselor informatice în scop personal

Mijloacele de procesare a informaţiei puse la dispoziţie de ***UNIVERSITATEA "DIMITRIE CANTEMIR" DIN TÂRGU MUREȘ*** sunt destinate în primul rând îndeplinirii sarcinilor de serviciu.

Utilizarea limitată în scopuri personale, ocazională sau accidentală, a mijloacelor de procesare a informaţiei este de înţeles şi acceptabilă, cu condiţia ca ea să se facă într-o manieră care să nu afecteze negativ utilizarea acestora pentru scopul principal. Utilizatorii trebuie să demonstreze simţ de responsabilitate şi să nu abuzeze de acest drept.

Stocarea e-mail-urilor, documentelor şi altor fişiere personale nu este încurajată. În cazul în care acestea sunt totuşi păstrate, vor fi stocate local şi nu pe serverele ***UNIVERSITATEA "DIMITRIE CANTEMIR" DIN TÂRGU MUREȘ***, în locaţii separate de cele care conţin

informații ce aparțin ***UNIVERSITATEA "DIMITRIE CANTEMIR" DIN TÂRGU MUREȘ***. Toate mesajele și fișierele personale aflate în sistemul informatic pot fi supuse verificării de conformitate cu Politicile IT&C a ***UNIVERSITATEA "DIMITRIE CANTEMIR" DIN TÂRGU MUREȘ.***
UNIVERSITATEA "DIMITRIE CANTEMIR" DIN TÂRGU MUREȘ nu își asumă nicio responsabilitate cu privire la securitatea acestor informații, întreaga responsabilitate (inclusiv realizarea copiilor de siguranță) revenind utilizatorului.

4.21. Detectarea virușilor

Toate stațiile de lucru de sine stătătoare sau conectate la rețeaua de comunicații a ***UNIVERSITATEA "DIMITRIE CANTEMIR" DIN TÂRGU MUREȘ***, trebuie să utilizeze programe antivirus aprobate de către Departamentul / Personalul IT&C.
Programele antivirus nu trebuie dezactivate.
Configurația programului antivirus trebuie să nu fie modificată într-un mod care să reducă eficacitatea programului.
Frecvența actualizărilor automate a programului antivirus trebuie asigurată de către utilizator.
Orice server de fișiere conectat la rețeaua ***UNIVERSITATEA "DIMITRIE CANTEMIR" DIN TÂRGU MUREȘ*** trebuie să utilizeze un program antivirus aprobat în scopul detectării și curățirii virușilor care pot infecta fișierele puse la dispoziție.
Orice server sau gateway pentru e-mail trebuie să folosească un program antivirus pentru e-mail aprobat și trebuie să respecte regulile de instalare și utilizare a acestui program.
Orice virus care nu a putut fi înlăturat automat de către programul antivirus constituie un incident de securitate și trebuie raportat imediat Departamentului / Personalului IT&C.

4.22. Returnarea resurselor la terminarea contractului

Utilizatorul va returna ***UNIVERSITATEA "DIMITRIE CANTEMIR" DIN TÂRGU MUREȘ***, la încetarea contractului de muncă sau de servicii, orice informații și orice mijloace de procesare a informațiilor puse la dispoziția sa în scopul îndeplinirii atribuțiilor de serviciu sau obligațiilor contractuale. Acestea includ și nu se limitează la: credențialele de acces la sisteme critice, primite sau modificate pe perioada contractului ș.a.m.d.

4.23. Salvarea și restaurarea datelor

UNIVERSITATEA "DIMITRIE CANTEMIR" DIN TÂRGU MUREȘ realizează salvări periodice a sistemelor și datelor. Toate mediile de stocare (casete, discuri etc.) trebuie să fie clar etichetate. Datele salvate sunt depozitate în clădirea ***UNIVERSITATEA "DIMITRIE CANTEMIR" DIN TÂRGU MUREȘ*** și / sau într-o locație alternativă. Ambele locații, cea primară și cea alternativă, au controale de securitate încorporate pentru a proteja datele împotriva accesului neautorizat. Locația alternativă trebuie să fie localizată departe de locația primară pentru a nu fi afectată în cazul în care locația primară a fost serios avariată (ex. incendiu, inundație, cutremur sau explozie).
Mediile de stocare trebuie testate periodic pentru a asigura posibilitatea recuperării datelor în caz de urgență.

4.24. Excepții

Excepţiile de la regulile definite în această politică vor fi puse în aplicare numai după autorizarea prealabilă a Departamentului / Personalului IT&C, care va fi solicitată în scris şi va include obligatoriu motivul excepţiei.
Toate excepţiile vor fi considerate evenimente de securitate, vor fi comunicate Departamentului / Personalului IT&C şi vor fi înregistrate de acesta în Registrul incidentelor de securitate, specificând data şi ora, descrierea, motivul şi modul de gestionare a riscurilor.
Nicio excepţie nu poate fi pusă în aplicare dacă aceasta presupune o încălcare prevederilor legale, a politicilor şi procedurilor operaţionale ale ***UNIVERSITATEA "DIMITRIE CANTEMIR" DIN TÂRGU MUREŞ*** precum şi a drepturilor şi libertăţilor altor persoane.

5. Responsabilităţi

6.

Forurile decizionale ale ***UNIVERSITATEA "DIMITRIE CANTEMIR" DIN TÂRGU MUREŞ*** au următoarele responsabilităţi:

- stabilesc şi aprobă Politica IT&C. procedurile subsecvente precum şi obiectivele de securitate a informaţiilor;
- asigură disponibilitatea resurselor necesare pentru aplicarea politicilor şi procedurilor IT&C;
- comunică importanţa unei gestionări eficiente a sistemelor informatice şi de comunicaţii.

Conducerea Departamentelor / Serviciilor

- se asigură că sistemele informatice şi de comunicaţii sunt gestionate eficient;
- îndrumă şi sprijină personalul să contribuie la eficacitatea sistemele informatice şi de comunicaţii.

Departamentul / Personalul IT&C are următoarele responsabilităţi:

- propune modificări ale Politicii IT&C;
- elaborează şi propune pentru aprobare politici şi proceduri de gestionare şi de securitate a resurselor informatice şi de comunicaţii în conformitate cu Politica IT&C;
- tratează incidentele de securitate în scopul minimizării efectului distructiv al acestora asupra resurselor informatice şi de comunicaţii;
- informează conducerea în caz de incidente, intervenţie şi rezolvarea incidentelor de securitate a informaţiilor;
- asigură existenţa jurnalelor şi a traseelor auditării pentru orice tip de acces în sistem conform procedurilor asociate;
- planifică, implementează şi verifică zilnic soluţiile de securitate a informaţiilor: server antivirus, firewall, server de actualizări de securitate, backup, acces securizat la camera tehnică, asigurare aer condiţionat, asigurare alimentare cu energie electrică/UPS;
- menţine înregistrări privind configuraţia, aplicaţiile şi serviciile instalate (fişa de server), pentru a se putea reface sistemul în caz de dezastru;
- inventariază periodic aplicaţiile şi serviciile instalate şi verifică dacă sunt autorizate;
- administrează sistemele IT şi aplică măsurile de securitate şi alte cerinţe ale programului de securitate a informaţiilor pentru sistemele informatice pentru care are atribuită responsabilitatea.

Şefii entităţilor organizatorice sunt responsabili pentru:

- implementarea de zi cu zi a Politicii IT&C şi a procedurilor aferente acesteia;
- asigurarea că măsurile de securitate tehnice, fizice şi procedurale adecvate sunt

implementate în conformitate cu Politica IT&C şi sunt aplicate în mod corespunzător şi de către tot personalul, asigurarea resurselor şi efectuarea analizelor necesare pentru a se asigura că informaţiile şi activele sunt protejate în mod corespunzător în zona lor de responsabilitate, informarea persoanei desemnate cu managementul incidentelor de securitate despre încălcările reale sau presupuse ale Politicii IT&C care afectează securitatea informaţiilor din zona lor de responsabilitate (incidentele de securitate a informaţiilor), identificarea şi clasificarea informaţiilor şi echipamentelor din zona lor de responsabilitate şi desemnarea deţinătorilor (responsabililor) pentru acestea;

- informarea Departamentului / Personalului IT&C la schimbarea responsabililor de active.

Utilizatorii datelor / sistemelor (angajaţi şi terţi care acţionează într-o modalitate similară, cum ar fi furnizori de servicii etc.):

- cunosc şi respectă Politica IT&C şi procedurile aferente acesteia aplicabile pentru locurile lor de muncă,
- răspund direct de resursele informatice şi de comunicaţii încredinţate direct sau indirect.

7. Formular evidenţă modificări

Nr. crt.	Ediția	Data ediției	Revizia	Data reviziei	Nr. pag.	Descriere modificare	Semnătura conducătorului compartimentului
1	2	4	5	6	7	8	9
1	I		0	-	19	-Elaborare conf. Regulamentului UE679/2016 şi a ghidurilor emise de EDPB -Elaborare conform OSGG 600/2018	
2							
3							
4							
5							

8. Formular analiză politică

Nr. crt.	Departament	Nume și prenume conducător departament	Înlocuitor de drept sau delegat	Aviz favorabil		Aviz nefavorabil		
				Semnătura	Data	Obs.	Semnătura	Data
1	2	3	4	5	6	7	8	9
1								
2								
3								
4								
5								

9. Lista de distribuire a politicii

Nr. ex.	Compartiment	Nume și prenume	Data primirii politicii	Semnătura	Data retragerii politicii	Semnătura
1	2	3	4	5	6	7
1 copie						
1 copie						
1 copie						
1 copie						
1 copie						
1 copie						
1 copie						
1 copie						
1 copie						
1 copie						