UNIVERSITATEA BABEȘ-BOLYAI
BABEȘ-BOLYAI TUDOMÁNYEGYETEM
BABEȘ-BOLYAI UNIVERSITÄT
BABEȘ-BOLYAI UNIVERSITY
TRADITIO ET EXCELLENTIA

RECTORAT

Str. M. Kogălniceanu nr. 1
Cluj-Napoca, RO-400084
Tel.: 0264-40.53.00
Fax: 0264-59.19.06
contact@ubbcluj.ro
www.ubbcluj.ro

Ghid de utilizare în siguranță a serviciului de mesagerie electronică al Universității Babeș-Bolyai

1. De ce trebuie să folosim serviciul de mesagerie electronică al UBB?

Asigurarea securității datelor și informațiilor presupune îndeplinirea următoarelor condiționalități: confidențialitatea, integritatea, disponibilitatea, și non-repudierea informațiilor transmise. Serviciul de mesagerie electronică al UBB (e-mail în continuare) asigură aceste condiționalități în conformitate cu HCA 16772 din 09.11.2020 privind Politica utilizării serviciului de mesagerie electronică (e-mail) instituțional.

Hotărârea Consiliului de Administrație al UBB nr. 16772 din 09.11.2020 privind Politica utilizării serviciului de mesagerie electronică (e-mail instituțional) prevede ca pentru respectarea regulilor de securitate pe timpul transmiterii informațiilor prin intermediul mesageriei electronice, atât inter-instituțional, cât și extra-instituțional se va folosi exclusiv serviciul de mesagerie electronică (e-mail) al UBB.

Varianta web a serviciului de mesagerie electronică (e-mail) al UBB (https://mail.ubbcluj.ro sau https://outlook.office.com/mail/) este una modernă, care încorporează cele mai noi tehnologii de nivel internațional furnizate de una dintre cele mai mari companii din domeniu: Microsoft. Compania Microsoft pune la dispoziția utilizatorilor serviciului de e-mail al UBB și servicii de protecție anti-spam și anti-phishing de calitate.

Serverele pe care funcționează serviciul de e-mail al UBB sunt dispuse geografic în Uniunea Europeană și respectă Regulamentul General European 2016/679 privind protecția datelor cu caracter personal (GDPR).

Prin folosirea e-mailului în comunicarea intra și extra-instituțională, UBB s-a conformat cerințelor privind securitatea informațiilor din sistemele informatice și de comunicații, precum și GDPR.

Utilizarea serviciului de e-mail instituțional reduce riscurile interceptării, pierderii, degradării informației, deoarece aceste mesaje nu ies din spațiul digital al UBB, informațiile netrecând prin alte servere aflate „undeva” în Internet.

2. Care sunt bazele legale care reglementează folosirea mesageriei electronice a UBB?

- **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

Str. M. Kogălniceanu nr. 1
Cluj-Napoca, RO-400084
Tel.: 0264-40.53.00
Fax: 0264-59.19.06
contact@ubbcluj.ro
www.ubbcluj.ro

personal și privind libera circulație a acestor date și de abrogare a Directivei95/46/CE (Regulamentul general privind protecția datelor), denumită în continuare **GDPR**, Art. 35 GDPR (Motivarea 89);

- **Legea nr. 190/2018 privind măsuri de punere în aplicare a Regulamentului (UE) 2016/679 (GDPR)** al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor);
- **Directiva 2002/58/CE** a Parlamentului European și a Consiliului din 12 iulie 2002 privind prelucrarea datelor personale și protejarea confidențialității în sectorul comunicațiilor publice (Directiva asupra confidențialității și comunicațiilor electronice);
- **Legea nr. 506 din 17 noiembrie 2004** privind prelucrarea datelor cu caracter personal și protecția vieții private în sectorul comunicațiilor electronice;
- **SR ISO/CEI 27000:2015**, Tehnologia informației. Tehnici de securitate. Sisteme de management al securității informației;
- **Standardul ISO/CEI 17799**: se referă la implementarea politicii de securitate (SMSI) și la managementul acestuia;
- **Strategia de Securitate Cibernetică a României 2.0 (2021-2026);**
- **Baze legale a UBB:**
    - Dispoziția conducerii UBB de achiziționare a unui pachet de mesagerie electronică de la Microsoft prin S.C. NetBrinel S.A
    - HCA 16772 din 09.11.2020 privind Politica utilizării serviciului de mesagerie electronică (e-mail) instituțional

3. Prezentarea pe scurt al sistemul de mesagerie electronică al UBB

Un mesaj electronic (e-mail) din sistemul de e-mail al UBB este alcătuit din două părți: antetul (header) și conținutul mesajului (body).

a. Antetul este format din mai multe secțiuni:
    - Expeditor (from) - adresa de e-mail a expeditorului;
    - Destinatar (to) - adresa de e-mail a destinatarului;
    - Subiectul (Subject) - un text scurt ce descrie conținutul sau tematica e-mail-ului;
    - Data (Date) - data și ora când s-a efectuat trimiterea e-mail-ului.

Notă: *Se pot defini mai mulți destinatari folosind următoarele secțiuni:*

- *Copie la indigo (Carbon Copy, CC) – toate adresele specificate vor primi mesajul respectiv, destinatarul poate vedea inclusiv celelalte adrese cărora li s-a trimis e-mail-ul;*

Str. M. Kogălniceanu nr. 1
Cluj-Napoca, RO-400084
Tel.: 0264-40.53.00
Fax: 0264-59.19.06
contact@ubbcluj.ro
www.ubbcluj.ro

- *Copie la indigo oarbă (Blind Carbon Copy, BCC) – destinatarii vor primi e-mail-ul, dar nu pot vedea dacă acesta a fost trimis și altor persoane.*

b. corpul e-mail-ului: zona în care se scrie mesajul propriu-zis de către expeditor;

c. attachment: zona în care se pot atașa diferite tipuri de fișiere, de exemplu: .doc, .docx, .pdf, .xlsx, .xls, jpeg, png, gif, .pptx, .ppt, .ppsx, .txt, .pub, .rar, .zip. etc.

Notă: *dimensiunea maximă a fișierelor este de 34 MB. Se pot atașa și fișiere din OneDrive, în cazul acestora dimensiunea maximă este de 2 GB.*

4. De ce trebuie să asigurăm securitatea serviciului de mesagerie electronică?

Aproximativ 91% dintre atacurile cibernetice sunt lansate prin intermediul e-mail-ului.

Prin accesarea unei legături (link) sau a unui atașament (attachment) infectat primit pe e-mail se poate declanșa un întreg lanț transparent de evenimente nefericite atât pentru calculatorul de pe care s-a accesat link-ul sau atașamentul, cât și pentru rețeaua de calculatoare și servere a instituției (rețeaua informatică a UBB).

Persoanele rău intenționate (atacatorii) folosesc tehnici de inginerie socială, care presupun manipularea persoanelor în vederea obținerii unor informații confidențiale din și prin intermediul sistemelor informatice.

Exemple:

- *Un exemplu de inginerie socială este acela în care atacatorul sună un angajat al instituției și încearcă să obțină informații confidențiale (date cu caracter personal ale unor angajați din instituție, parole de acces la sistemul informatic, etc), dându-se drept cineva din cadrul instituției (o persoană cu atribuții de conducere, un coleg de la un alt departament sau reprezentantul unui furnizor etc);*
- *Phishing-ul este o formă de activitate frauduloasă (inginerie socială) care constă în obținerea unor date confidențiale (inclusiv date cu caracter personal) prin trimiterea unui mesaj pe e-mail, mesaj ce conține un link către un site web fals al unei instituții sau organizații reale. Dacă persoana introduce date cu caracter personal sau alte informații confidențiale pe acel site web (parole, cod PIN etc.), acestea ajung la atacator. Atacatorul poate folosi în cadrul mesajului sigla unei instituții sau alte elemente vizuale (inclusiv o adresă de e-mail asemănătoare), pentru a oferi credibilitate în ochii utilizatorului. Mai departe, utilizatorul poate fi informat că din cauza unor defecțiuni tehnice ce au dus la pierderea unor date confidențiale/personale, este necesară retransmiterea acestor date;*
- *Infectarea rețelei informatice prin transmiterea unor link-uri spre un site fals care are rolul de a ataca sistemul informatic. Se folosesc adrese web (URL) sub forme de tipul http://172.148.25.100/edu/finantare-universitar/. Chiar dacă „edu" este parte a adresei afișate și ne poate trimite cu gândul la site-ul Ministerului Educației din România (edu.ro), prima parte conține caractere numerice aranjate sub forma unei adrese IP. Acesta este un indiciu că* ***link-ul nu este unul de încredere****. De asemenea, site-urile web securizate folosesc https:// în cadrul adreselor web, nu*

Str. M. Kogălniceanu nr. 1
Cluj-Napoca, RO-400084
Tel.: 0264-40.53.00
Fax: 0264-59.19.06
contact@ubbcluj.ro
www.ubbcluj.ro

http://. Unele link-uri suspecte pot include și https://, de aceea este important să analizați și denumirea domeniului din link-ul primit pe e-mail. Dacă în loc de domeniul .ro, veți observa un domeniu suspect, precum .xyz, înseamnă că site-ul web este rău intenționat.

5. Ce riscuri de securitate pot apărea pe timpul folosirii e-mailului?

Riscurile de securitate sunt direct proporționale cu nevoia de păstrare a confidențialității datelor și informațiilor transmise prin intermediul e-mail-ului. Securitatea UBB în ansamblu depinde de păstrarea confidențialității acestora. Mai jos este o listă cu riscuri identificate de responsabilii UBB în domeniu, dar, dat fiind faptul că tehnologiile informatice sunt în continuă dezvoltare, pot apărea și unele noi:

a. Folosirea incorectă a funcției CC atunci când se trimite un e-mail către un grup de persoane, prin sistem listă. Astfel, persoana care primește e-mailul are acces la o listă de adrese de e-mail care poate fi folosită ulterior în alte scopuri, contrar intereselor persoanelor din listă (încălcare a regulilor de protecție a datelor cu caracter personal). **Recomandare:** folosiți funcția BCC;

b. Completarea greșită a datelor (adresei) destinatarului. Astfel putem ajunge în situația de a trimite un e-mail care ar putea conține date confidențiale/sensibile la un alt destinatar. **Recomandare:** verificați cu atenție anterior transmiterii datele (adresa) destinatarului și folosiți confirmarea de primire;

c. Divulgarea informațiilor sensibile/confidențiale intenționat. Recomandare: se interzice cu desăvârșire transmiterea înspre terți a informațiilor sensibile fără acordul emitentului (UBB) ;

d. Divulgarea informațiilor sensibile/confidențiale accidental: atașarea greșită a unor documente care conțin date cu caracter personal sau alte date confidențiale/sensibile. **Recomandare:** verificarea antetului e-mail-ului, a corpului și a attachment-ului înaintea transmiterii;

e. Instalarea unui spyware. Programul de tip spyware poate fi instalat pe calculatoarele utilizatorilor fără consimțământul acestora, în momentul în care se deschid attachment-uri sau link-uri rău intenționate. Acest program monitorizează activitatea calculatorului și colectează informații din acesta, fără ca utilizatorul să știe. **Recomandare:** nu accesați link-uri și attachment-uri suspecte;

f. Păstrarea nejustificată a unor e-mail-uri care conțin informații sensibile sau date cu caracter personal. **Recomandare:** ștergeți mesajele/conversațiile care nu mai sunt necesare din Inbox, apoi accesați *Elemente șterse* (Trash)și ștergeți definitiv mesajele/conversațiile selectate;

Str. M. Kogălniceanu nr. 1
Cluj-Napoca, RO-400084
Tel.: 0264-40.53.00
Fax: 0264-59.19.06
contact@ubbcluj.ro
www.ubbcluj.ro

g. Nesecurizarea documentelor cu informații sensibile/confidențiale. Aceasta se face prin necriptarea sau neprotejarea cu o parolă a atașamentelor mesajului, acestea fiind ușor de accesat. **Recomandare:** Dacă trimiteți, pe e-mail, un document care conține informații sensibile și/sau date cu caracter personal, acesta trebuie să fie protejat cu o parolă (criptat). Parola se va trimite destinatarului e-mailului pe alt canal de comunicare (de exemplu: prin SMS) cu confirmare de primire.

h. Alegerea unei parole neadecvate pentru accesarea căsuței de e-mail: parola este prea simplă și prea previzibilă. **Recomandare:** Utilizați o parolă de minimum 8 caractere, care să conțină minimum o literă mică, o literă mare, o cifră, un simbol. Nu utilizați ca următoarele date și informații: data de naștere, numele de familie al părinților, numele străzii pe care locuiți, numele animalului de companie, numele instituției de învățământ absolvite, numele soțului/soției etc.

6. Care sunt măsurile de securitate care trebuie implementate de utilizatori?

- schimbați parola inițială/prestabilită de acces la adresa de e-mail instituțională la prima accesare a contului de e-mail. (Vezi tutorialul pentru schimbarea parolei)
- nu scrieți parolele de acces (la calculator sau la e-mailul de serviciu) pe bilețele sau pe hârtii și, ulterior, nu le lipiți pe birou, pe monitor, lângă tastatură sau în alte locuri accesibile;
- schimbați parola de acces la e-mailul instituțional o dată la 3 luni, chiar dacă sistemul nu o cere;
- nu utilizați aceeași parolă pentru e-mailul personal și e-mailul de serviciu;
- nu utilizați aceeași parolă pentru mai multe conturi;
- nu dezvăluiți niciodată și nimănui parola;
- nu trimiteți parole prin e-mail și nu le stocați într-o locație nesigură;
- utilizați un produs anti-malware/anti-virus pe dispozitivul informatic;
- actualizați periodic programul anti-malware/anti-virus;
- efectuați scanări periodice ale sistemului pentru a identifica posibile fișiere cu potențial malițios;
- nu desfășurați activități legate de locul de muncă (de exemplu: accesarea e-mail-ului de serviciu) atunci când utilizați o rețea WiFi publică sau nesecurizată;
- pentru a accesa e-mailul instituțional de pe smartphone sau tabletă utilizați o rețea WiFi sigură și securizată sau datele mobile. Evitați hotspot-urile wireless din cafenele, hoteluri, aeroporturi, mall-uri etc. atunci când vă accesați e-mailul instituțional sau cel personal;
- nu folosiți calculatoare publice pentru a accesa adresa de e-mail instituțională. Aceste calculatoare pot conține programe care înregistrează date cu caracter personal și/sau sensibile;

Str. M. Kogălniceanu nr. 1
Cluj-Napoca, RO-400084
Tel.: 0264-40.53.00
Fax: 0264-59.19.06
contact@ubbcluj.ro
www.ubbcluj.ro

- nu utilizați e-mailul instituțional în scopuri personale. Nu utilizați adresa de e-mail instituțională pentru înregistrarea pe diverse site-uri web sau pe platforme de comerț electronic;
- nu utilizați echipamentele informatice ale UBB (calculatoare, laptopuri, smartphone-uri, tablete) pentru activități personale (accesarea unor site-uri web care nu au legătură cu activitatea profesională/științifică, accesarea și înregistrarea pe platformele de comerț electronic, desfășurarea de activități financiar-bancare în scopuri personale);
- nu lăsați calculatorul/laptopul nesupravegheat, mai ales atunci când mesageria electronică este deschisă;
- închideți sesiunea de lucru (logout) atunci când părăsiți biroul unde se află calculatorul sau laptop-ul;
- nu utilizați date cu caracter personal în titlul/subiectul e-mail-ului;
- evitați divulgarea de date cu caracter personal și date sensibile prin e-mail, dacă nu puteți verifica identitatea celui cu care comunicați. Verificați identitatea persoanei care vă cere aceste date, o metodă eficientă fiind contactarea persoanei printr-un mijloc cunoscut (de exemplu: sunați persoana pe numărul de telefon mobil, contactați o persoană din apropierea acesteia);
- folosiți BCC (Blind Carbon Copy) atunci când trimiteți un e-mail către mai mulți destinatari sau către adrese de e-mail personale;
- dacă trimiteți pe e-mail date cu caracter personal sau alte informații sensibile, cereți destinatarului să confirme primirea e-mail-ului;
- nu deschideți mesajele e-mail venite de la surse nesigure (expeditor necunoscut, subiect și conținut suspect). Fiți atent/ă la calitatea textului primit, precum eventualele greșeli gramaticale, de redactare sau de exprimare. Verificați întotdeauna sursa mesajului;
- manifestați precauție la accesarea e-mailurilor. Uitați-vă cu atenție la adresa site-ului web (URL) și la link-urile care sunt incluse într-un e-mail înainte de a da click pe ele. Dacă bănuiți că link-ul este suspect, nu îl accesați;
- nu răspundeți niciodată la un mail de tip spam. Trebuie să trimiteți e-mailul spam structurii IT&C a UBB pentru a face ajustări la filtrul spam și a colecta, în viitor, e-mailurile de la acest expeditor;
- raportați întotdeauna e-mailurile suspecte DTIC sau solicitați îndrumare înainte de a acționa mai departe. Este important ca structura de securitate informatică să evalueze activitatea suspectă, astfel încât să poată stabili dacă un e-mail reprezintă o amenințare;
- în situația în care găsiți pe o masă în hol sau în biroul dumneavoastră un stick USB, iar acesta nu aparține niciunui coleg de serviciu (angajat al UBB), lăsați-l acolo.-Nu introduceți în nici un dispozitiv al instituției (inclusiv în cel pe care lucrați) acel stick USB.

Str. M. Kogălniceanu nr. 1
Cluj-Napoca, RO-400084
Tel.: 0264-40.53.00
Fax: 0264-59.19.06
contact@ubbcluj.ro
www.ubbcluj.ro

7. Alte recomandări

- fiți precauți atunci când introduceți credențialele (parolă sau PIN) de acces la calculator/laptop în prezența altor persoane, pentru a nu fi observate de acestea;
- dacă primiți pe e-mail un attachment cu o arhivă, este recomandat să dezarhivați conținutul arhivei și, ulterior, să accesați documentele. Procedând în acest fel, veți permite programului anti-malware/anti-virus să identifice un posibil software malițios;
- acordați foarte mare atenție virușilor informatici. Aceștia se pot transmite prin attachment-uri care au extensii neobișnuite (de exemplu: un fișier de tip imagine nu poate avea o extensie ca un program executabil). Nu deschideți fișierele atașate prin e-mail care se termină în .exe, .scr, .bat, .com sau alte fișiere executabile pe care nu le recunoașteți;
- evitați deschiderea de fișiere atașate necunoscute. Viermii informatici (worms) și programele rău intenționate (ransomware) se pot răspândi prin deschiderea unui e-mail infectat. Dacă nu sunteți sigur/ă în legătură cu un atașament, fie realizați o scanare de viruși pentru a vedea dacă fișierul este sigur sau malițios, fie ștergeți mesajul;
- remediați breșele de securitate și erorile software ale sistemului de operare folosit, prin aplicarea automată sau manuală a actualizărilor (up-date) disponibile;
- nu faceți publică adresa de e-mail instituțională pe platformele de socializare/cumpărături on-line, decât în scopuri profesionale și/sau științifice bine justificate. Dacă totuși faceți acest lucru, puteți primi mai multe e-mail-uri nesolicitate, unele cu potențial malițios.

8. Procedură de raportare a unui incident de securitate informatică

a. **Incident de securitate informatică**: eveniment produs în spațiul informatic virtual al cărui consecințe afectează securitatea informatică (ex.: virusarea stației de lucru, spargerea contului de e-mail, primirea de e-mail-uri-suspecte și/sau de tip spam etc.).

Incidentele de securitate informatică se semnalează responsabilului cu serviciile informatice (inginer de sistem, administrator de sistem, analist etc.) din unitatea administrativă și de cercetare în care a apărut incidentul.

Date de contact DTIC (Direcția Tehnologiei Informației și Comunicațiilor): https://helpdesk.ubbcluj.ro/.

b. **Incident de securitate care implică date cu caracter personal**: accesul neautorizat care duce la vizualizarea, modificarea, pierderea, distrugerea sau divulgarea datelor cu caracter personal sau la accesul neautorizat la acestea.

Semnalarea incidentului:

Str. M. Kogălniceanu nr. 1
Cluj-Napoca, RO-400084
Tel.: 0264-40.53.00
Fax: 0264-59.19.06
contact@ubbcluj.ro
www.ubbcluj.ro

Încălcarea securității datelor cu caracter personal sau a măsurilor organizatorice sau tehnice implementate la nivelul UBB se semnalează de către orice salariat sau unitate administrativă și de cercetare a UBB, respectiv o persoană vizată sau entitate terță, telefonic și în scris, Responsabilului cu protecția datelor cu caracter personal al UBB (DPO), (0744423188, dpo@ubbcluj.ro, 0264405300 - centrala UBB).

Sesizarea se va face în timpul cel mai scurt de la producerea incidentului în următoarea succesiune:

1. apel pe telefon mobil (sau telefon fix – centrala UBB – solicitându-se legătura cu DPO)
2. trimiterea unui e-mail (cu detalii) pe adresa DPO.

9. Procedura de alocare a unei adrese de e-mail și dezabonarea

a. Angajați titulari pe perioadă determinată/nedeterminată - pot fi atât cadre didactice, cât și personal didactic auxiliar/administrativ).

Aceștia primesc automat o adresă de e-mail, conform modului de administrare a adreselor de e-mail pentru angajați, pe toată durata contractului cu UBB și vor putea folosi contul de e-mail încă un an după încheierea relației contractuale cu UBB.

Prima accesare a adresei de e-mail se face conform procedurii de pe site-ul DTIC: https://dtic.ubbcluj.ro/tutorial/conectare-office365-angajati/.

După încetarea contractului de muncă, contul de e-mail va fi închis automat după un an, prin acțiuni informatice specifice.

Persoanele care mai derulează activități împreună cu UBB și după încetarea contractului de muncă pot solicita extinderea valabilității contului de e-mail în baza și pe durata perioadei valabilității formei justificate de derulare a activității (ex. convenție, acord, alt tip de contract decât cel de muncă etc.)

b. Cadre didactice asociate/colaboratori

Aceste persoane pot primi adresă de e-mail conform modului de administrare a adreselor de e-mail pentru angajați, la solicitarea conducătorului unității administrative și de cercetare și în urma aprobării acesteia de către superiorul ierarhic (rector, prorector, decan). Solicitarea se transmite prorectorului responsabil cu digitalizarea și se face anual. Adresele de e-mail sunt valabile un an, cu posibilitatea reînnoirii lor prin procedura de mai sus.

Str. M. Kogălniceanu nr. 1
Cluj-Napoca, RO-400084
Tel.: 0264-40.53.00
Fax: 0264-59.19.06
contact@ubbcluj.ro
www.ubbcluj.ro

c. Profesori emeriți sau profesori străini, pensionari, visiting professors/researchers care nu (mai) au relații contractuale cu Universitatea Babeș-Bolyai

Aceste persoane primesc adresă de e-mail conform modului de administrare a adreselor de e-mail pentru angajați, la solicitarea lor cu avizul decanului/ prorectorului/rectorului. Solicitarea trebuie să conțină perioada de valabilitate a contului de e-mail (data de început: ll/aaaa și data de sfârșit: ll/aaaa). Solicitarea trebuie aprobată și de prorectorul responsabil cu digitalizarea.

***d.* Doctoranzi**

Aceștia primesc automat o adresă de e-mail pe toată durata contractului de studii universitare de doctorat, încheiat cu Universitatea Babeș-Bolyai. Accesarea adresei de e-mail se face conform procedurii de pe site-ul DTIC (https://dtic.ubbcluj.ro/tutorial/conectare-office365-angajati/).

e. Studenții de la nivel licență și master

Studenții și masteranzii primesc automat o adresă de e-mail pe toată durata contractului de studii universitare, încheiat cu Universitatea Babeș-Bolyai. Contul de e-mail se închide automat la 3 luni după finalizarea studiilor. Accesarea adresei de e-mail se face conform procedurii de pe site-ul DTIC (https://dtic.ubbcluj.ro/tutorial/conectare-office365-studenti/).

Studentul care a absolvit studii universitare de nivel licență la UBB și își continuă studiile la un program de masterat din cadrul UBB sau care optează pentru un alt program de studii universitare de licență la UBB în anul universitar următor, își păstrează accesul la contul de e-mail pe care l-a avut în timpul ciclului de studii absolvit la UBB. Absolventul care se înscrie la un program de studii mai târziu decât anul universitar următor absolvirii, primește datele de conectare folosite pe perioada ciclului de studii absolvit (fără restabilirea conținutului contului).

Condiții în care se poate prelungi accesul la contul de e-mail instituțional:

- cadrul didactic asociat își prelungește contractual;
- angajatul a cărui contract de muncă pe perioadă determinată expiră și încheie un nou contract cu UBB;
- continuarea activității științifice (proiectului) începute anterior încetării contractului de muncă;
- studentul care a absolvit studii universitare de nivel licență și își continuă studiile la un program de masterat din cadrul UBB;
- doctorandul, după cei trei ani de studii doctorale, care își prelungește contractul cu încă un an sau care încheie un contract de muncă cu universitatea.

Str. M. Kogălniceanu nr. 1
Cluj-Napoca, RO-400084
Tel.: 0264-40.53.00
Fax: 0264-59.19.06
contact@ubbcluj.ro
www.ubbcluj.ro

Link către tutoriale utile pentru utilizarea serviciului de e-mail instituțional: https://dtic.ubbcluj.ro/categorie_tutoriale/tutoriale/.

GLOSAR DE TERMENI

Securitatea informatică	Ansamblul activităților necesare pentru protejarea sistemelor informatice, a datelor, informațiilor și a utilizatorilor acestor sisteme.
Spațiul informatic	Mediul virtual în care se găsesc informațiile.
Confidențialitatea	Ne asigură că datele și informațiile vor rămâne cunoscute doar persoanelor care au acest drept
Integritatea	Ne asigură că datele și informațiile nu vor fi modificate sau distruse decât de persoanele autorizate
Disponibilitatea	Ne asigură că datele, informațiile, echipamentele informatice și serviciile pot fi accesate și folosite de către persoanele autorizate în orice moment.
Non-repudierea	Confirmă destinatarului unui mesaj electronic faptul că respectivul mesaj este scris și/sau trimis de către utilizatorul care pretinde că la trimis.
Spam	Mesaj electronic nesolicitat.
Malware (software malițios)	Program creat pentru a se instala pe un dispozitiv informatic (calculator, laptop, smartphone, tabletă), fără consimțământul proprietarului, cu scopul de a distruge sau executa acțiuni nedorite pe acel sistem.
Vierme informatic (Worm)	Program care infectează un calculator, apoi se răspândește la alte calculatoare din rețea.
Program rău intenționat (Ransomware)	Program care criptează datele și informațiile de pe un calculator, cerând pentru decriptare o sumă de bani.
Spyware	Program malițios care monitorizează activitatea calculatorului și colectează informații personale.

Str. M. Kogălniceanu nr. 1
Cluj-Napoca, RO-400084
Tel.: 0264-40.53.00
Fax: 0264-59.19.06
contact@ubbcluj.ro
www.ubbcluj.ro

Date confidențiale/ sensibile	Date și informații care diseminate neautorizat pot produce prejudicii UBB (de imagine, patrimoniale, financiare, asupra membrilor comunității UBB, etc).
Date cu caracter personal	Orice informații privind o persoană fizică identificată sau identificabilă („persoana vizată”); o persoană fizică identificabilă este o persoană care poate fi identificată, direct sau indirect, în special prin referire la un element de identificare, cum ar fi un nume, un număr de identificare, date de localizare, un identificator online, sau la unul sau mai multe elemente specifice, proprii identității sale fizice, fiziologice, genetice, psihice, economice, culturale sau sociale.
Criptare	Procesul de mascare a informațiilor astfel încât doar persoanele autorizate să poată accesa informațiile respective.
Adresă IP (Internet protocol address)	Este un cod de identificare al dispozitivelor conectate la o rețea de calculatoare, care facilitează comunicarea între dispozitivele din aceeași rețea sau între dispozitivele aflate în rețele diferite.
Rețea de date	Un ansamblu de dispozitive (calculatoare, laptop-uri, routere, switch-uri etc) care sunt interconectate și schimbă informații între ele.
URL - Uniform Resource Locator	Secvență de caractere utilizată pentru localizarea unei resurse aflate în Internet.
Hotspot WiFi	Punct de acces la Internet care îi permite utilizatorului să se conecteze la o rețea WiFi folosind un echipament informatic (de exemplu: laptop, smartphone).

Colectivul redacțional

Direcția Tehnologiei Informației și Comunicațiilor	Protecția Datelor cu Caracter Personal
Colectivul DTIC	dr. Raul-Ciprian Dăncuță - Data Protection Officer UBB Cluj drd. Darius-Antoniu Ferenț - Asistent DPO UBB Cluj