Președinte Consiliu de Administrație
Prof. Univ. Dr. Mircea Dumitru

Nr. de înregistrare: 19515, din 04.09.2019

POLITICA IT&C

Ediția 1, Revizia 0, Data 12.08.2019

Avizat,

Secretariat Comisie de Monitorizare

Silvia Pădure

Elaborat,

Director Direcția IT&C

Anca Ileana

Administrator Patrimoniu și

Responsabil Proceduri IT&C

Camelia Mucică

Cuprins

1. Scop

Politica IT&C are ca scop asigurarea integrităţii, confidenţialităţii şi disponibilităţii sistemelor informatice din cadrul Universităţii din București.

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

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

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

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

2. Domeniu aplicare

Politica IT&C se aplică tuturor angajaților Universităţii din Bucureşti și persoanelor împuternicite care accesează resursele informatice și de comunicație ale Universităţii.

3. Documente de referinţă (reglementări), politici și proceduri asociate

3.1.Documente de referinţă

- SR ISO/CEI 27001: 2013 – Tehnologia informaţiei. Tehnici de securitate. Sisteme de management a securităţii informaţiei;
- SR ISO/CEI 27002: 2018 - Tehnologia informaţiei. Tehnici de securitate. Cod de bună practică pentru managementul securităţii informaţiei;
- Ghidul de securitate informatică pentru funcționarii publici, CERT-RO;
- OSSG 600/2018 – privind aprobarea Codului controlului intern managerial al entităţilor publice;

3.2. Politici și proceduri IT&C asociate

Angajații Universităţii din Bucureşti, subcontractanții și persoanele împuternicite care accesează resursele informatice și de comunicație ale Universității din București trebuie să respecte următoarele politici și proceduri IT&C identificate la momentul dezvoltării Politicii IT&C:

- Politica privind rolurile și responsabilitățile personalului legate de securitatea datelor,
- Politica privind dispozitivele mobile și lucrul de la distanța,
- Politica privind managementul resurselor informatice,
- Procedura privind controlul accesului logic,
- Procedura privind gestionarea dispozitivelor criptografice,
- Procedura privind backup-ul și arhivarea,
- Procedura privind stocarea și transmiterea de informații,
- Procedura privind utilizarea serviciilor cloud,
- Procedura privind managementul parolelor,
- Politica utilizării sistemelor informatice și comunicațiilor,
- Politica privind utilizarea echipamentelor proprietate personală,
- Procedura instalare echipamente,
- Procedura acces angajaţi,
- Procedura acces studenți sau terța parte (studenți, vizitatori, profesori alte facultăți),
- Politica management incidente de securitate,
- Politica privind site-urile web.

4. Definiţii și abrevieri ale termenilor utilizați în politica de securitate

4.1. Definiţii ale termenilor

Nr. crt.	Termenul	Definiția și/sau, dacă este cazul, actul care definește termenul
1.	Resurse informatice și de comunicaţii	Toate dispozitivele de tipărire/imprimare, dispozitive de afișare, unităţi de stocare și toate activităţile asociate calculatorului care implică utilizarea oricărui dispozitiv capabil să recepţioneze email-uri, să navigheze pe site-uri web, capabil să transmită, stocheze, administreze date electronice, incluzând, dar fără a se limită la: servere, calculatoare personale, laptop-uri, smartphone-uri, sisteme de procesare distribuită, echipament de laborator şi medical conectat la reţea şi controlat prin calculator (tehnologie încapsulată), resurse de telecomunicaţii, medii de reţea, telefoane, faxuri, imprimante și alte accesorii. La acestea se adaugă procedurile, echipamentele, facilităţile, programele și datele care sunt proiectate, construite, puse în funcţiune (operaţionale) și menţinute pentru a crea, colecta, înregistra, procesa, stoca, primi, afișa și transmite informaţia.

Nr. crt.	Termenul	Definiția și/sau, dacă este cazul, actul care definește termenul
2.	Abuz de privilegii	Orice acţiune întreprinsă în mod voit de un utilizator, care vine în contradicţie cu regulamentele Universității din Bucureşti şi/sau legile în vigoare, inclusiv cazul în care, din punct de vedere tehnic, nu se poate preveni înfăptuirea de către utilizator a acţiunii respective.
3.	Subcontractant	Persoană fizică/juridică care oferă bunuri sau servicii Universității din Bucureşti în baza unui contract comercial sau de colaborare.
4.	Persoană împuternicită	Persoană fizică/juridică care oferă bunuri sau servicii Universității din Bucureşti în baza unui contract comercial sau de colaborare și poate avea acces la date cu caracter personal.
5.	Securitatea fizică	Domeniul securităţii care prezintă atât măsuri pentru prevenire cât şi pentru împiedicarea atacatorilor să aibă acces la obiective, resurse sau informaţii şi recomandări privind proiectarea infrastructurii pentru a opune rezistenţă la actele ostile.
6.	Securitatea informaţiei	Păstrarea confidenţialităţii, integrităţii şi a disponibilităţii informaţiei.
7.	Confidenţialitate	Proprietatea ca informaţia să nu fie făcută disponibilă sau divulgată unor persoane, entităţi, sau procese neautorizate.
8.	Integritate	Proprietatea de a proteja acurateţea şi completitudinea resurselor.
9.	Disponibilitate	Proprietatea de a fi accesibil şi utilizabil la cerere de către o entitate autorizată.
10.	Atac	Încercare de a distruge, a expune, a modifica, a dezactiva, a fura sau a obţine accesul neautorizat sau a utiliza în mod neautorizat o resursă.
11.	Ameninţare	Cauză potenţială a unui incident nedorit care poate produce daune unui sistem sau organizaţii.
12.	Vulnerabilitate	Slăbiciune a unei resurse sau a unui mijloc de control care poate fi exploatată de o ameninţare.
13.	Eveniment privind securitatea informaţiei	Fapt identificat în legătură cu starea unui sistem, a unui serviciu, sau a unei reţele indicând o posibilă încălcare a politicii de securitate a informaţiei, un eşec al mijloacelor de control sau o situaţie ignorată anterior dar care poate fi relevantă din punct de vedere al securităţii.
14.	Incident privind securitatea informaţiei	Unul sau o serie de evenimente privind securitatea informaţiei nedorite sau neprevăzute care au o probabilitate semnificativă de compromitere a operaţiunilor de business şi de ameninţare a securităţii informaţiei.

4.2. Abrevieri ale termenilor

Nr. crt.	Abrevierea	Termenul abreviat
1.	DTIC	Direcţia Tehnologia Informaţiei şi comunicaţiei
2.	IT&C	Tehnologia Informaţiei şi comunicaţiei
3.	CERT-RO	Centrul naţional de răspuns la incidente de securitate cibernetica
4.	PLT	Politică
5.	UB	Universitatea din Bucureşti

5. Politică

5.1. Declarație

Resursele informatice și de comunicații ale Universității din Bucureşti sunt bunuri strategice ale Universității din Bucureşti și sunt parte integrantă a acesteia. Universitatea din Bucureşti a investit substanţial în resurse financiare și umane pentru a putea crea acest sistem și de aceea trebuie administrat ca atare.

Compromiterea securității acestor resurse poate afecta capacitatea Universității din Bucureşti de a oferi servicii informatice și de comunicații și poate conduce la fraude, incidente legate de confidenţialitatea datelor cu caracter personal, la distrugerea datelor, la violarea clauzelor contractuale, divulgarea secretelor, la afectarea credibilității Universității în faţa partenerilor săi.

Această politică este stabilită astfel încât:

- să fie în conformitate cu statutul, regulamentele, legile și alte documente oficiale în vigoare privind administrarea resurselor informatice și de comunicaţii;
- să stabilească practici prudente şi acceptabile privind utilizarea resurselor informatice şi de comunicații ale Universității din Bucureşti;
- să instruiască utilizatorii care au dreptul de folosire a acestor resurse privind responsabilităţile asociate utilizării acestora;
- să protejeze această investiţie;
- să protejeze informaţiile conținute în aceste sisteme;
- să reducă riscurile legale;
- să protejeze renumele Universității din Bucureşti.

5.2. Confidenţialitate

În scopul administrării Resurselor Informatice și de Comunicații şi pentru asigurarea securității acestora, personalul autorizat poate revizui sau utiliza orice informaţie stocată pe/sau transportată prin sistemele Resurselor Informatice și de Comunicații în conformitate cu legile în vigoare.

Utilizatorii vor avea grijă să nu încalce drepturile de confidențialitate ale altor persoane atunci când utilizează echipamentele (de exemplu, când fac înregistrări audio-video la locul de muncă).
Utilizatorii trebuie să raporteze orice slăbiciune în sistemul de securitate al calculatoarelor din cadrul Universității din Bucureşti, orice incident de posibilă întrebuinţare greşită sau încălcare a acestui regulament.

Utilizatorul trebuie să se asigure prin mijloace legale sau tehnice că informațiile aparținând sau aflate în custodia Universității din Bucureşti rămân sub controlul Universității în orice moment.

Utilizatorii nu trebuie să încerce să acceseze informații sau programe de pe sistemele Universității din Bucureşti pentru care nu au autorizaţie sau consimţământ explicit.

Nici un utilizator al Resurselor informatice și de comunicații ale Universității din Bucureşti 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 și de comunicaţii. Această regulă se extinde şi după ce utilizatorul a încheiat relaţiile cu Universitatea din Bucureşti.

Stocarea de informații în interes de serviciu pe dispozitive aflate în afara controlului Universității, inclusiv pe dispozitive administrate de terți cu care Universității nu are un acord contractual, este interzisă. Aceasta interzice în mod expres utilizarea în interes de serviciu a unui cont de e-mail care nu este furnizat de Universitate.

Confidenţialitatea informaţiilor transmise prin intermediul resurselor de comunicaţii ale terţilor nu poate fi garantată. Pentru aceste situaţii, confidenţialitatea şi integritatea informaţiilor se poate asigura folosind tehnici de criptare. Utilizatorii sunt obligaţi să se asigure că toate informaţiile confidenţiale ale Universității din Bucureşti se transmit în aşa fel încât să se asigure confidenţialitatea şi integritatea acestora.

5.3. Administrarea conturilor

Toate conturile create trebuie să aibă asociată o cerere şi o aprobare corespunzătoare.

Toate conturile de acces se vor crea în formatul standard cont utilizator prenume.nume.

Prin contractul de muncă şi/sau alte documente toţi utilizatorii acceptă prevederile regulamentelor 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 și folosite în conformitate cu politica privind parolele de acces.

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.

Responsabilul IT trebuie să aibă o documentaţie de modificare a conturilor de utilizator pentru situații precum schimbări ale numelor de familie, modificări privind contul (numele contului), modificări ale drepturilor de utilizator.

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

Acordarea accesului pentru angajaţi se va face de către Responsabilul IT în urma transmiterii de către Direcţia Resurse Umane a unui formular care va conţine 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 studenţi se va face de către Responsabilul IT în urma transmiterii de către Direcţia Generală Secretariat, la începutul fiecărui an școlar, a unui formular care va conţine detalii legate de utilizator și drepturile acestuia.

Acordarea accesului pentru studenții și profesorii vizitatori, pentru furnizori sau alte categorii de utilizatori, se va face de către Responsabilul IT în urma transmiterii de către Departamentele / Facultăţile interesate a unui formular ce va conţine detalii legate de utilizator precum și legate de durata activării contului de utilizator și drepturile acestuia.

Accesul la sistemele informatice și site-urile web utilizate de Universitatea din Bucureşti se va face conform procedurilor de acces ale acestor sisteme informatice și site-uri web.

Mai multe detalii în procedurile: Procedura privind accesul angajaţilor și Procedura acces studenți sau terța parte (studenți, vizitatori, profesori alte facultăți).

5.5. Identificare și autentificare

Utilizatorul este responsabil pentru securitatea datelor, a informațiilor de autentificare și a sistemelor aflate sub controlul său.
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.
Asigurarea accesului altei persoane, fie în mod deliberat, fie prin incapacitatea de a păstra în siguranță informațiile de autentificare, reprezintă o încălcare a acestei politici.
Nu trebuie, sub nici o formă, să acceseze neautorizat fişierele, calculatoarele sau alte dispozitive din reţeaua Universităţii din Bucureşti. Acesta este considerat caz de fraudă majoră.
La părăsirea calculatorului trebuie ca utilizatorul să iasă din reţea (log off).

De asemenea sunt interzise:

- încercarea utilizatorilor de a vizualiza și deduce parolele altora în timpul introducerii acestora,
- transmiterea de parole în clar prin intermediul sistemelor de comunicații (e-mail, mesagerie instant, SMS etc.).

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.

5.6. Acces administrativ

Facultăţile și Departamentele Universității din Bucureşti trebuie să prezinte Responsabilului IT o listă cu persoanele de contact cu drept de administrator pentru toate sistemele informatice conectate la reţeaua de comunicații a Universității din București. Această listă trebuie refăcută și prezentată Responsabilului IT de fiecare dată când apar modificări de orice natură.

Utilizatorii trebuie să cunoască şi să accepte toate regulamentele 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 și 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 investigații numai sub îndrumarea sefului 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 sefului direct şi trebuie să fie schimbată atunci când persoana care utilizează acest cont îşi schimbă locul de muncă în cadrul Universității din Bucureşti, sau în cazul unei modificări a listei de personal care furnizează servicii din partea terţilor având contracte cu Universitatea.

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

5.7. Accesul la reţeaua de comunicaţii

Utilizatorilor le este permis să utilizeze numai parametrii pentru conectare la reţea specificaţi de către Responsabilul IT.

Șefii entităților organizatorice trebuie să aprobe, în scris, conectarea dispozitivelor de calcul la rețeaua de comunicații a Universității din Bucureşti. Pentru fiecare sistem conectat trebuie să existe o persoană care să răspundă de acesta, numele și datele de identificare ale acesteia se vor comunica către Responsabilul IT.

Conectarea sistemelor de calcul care nu sunt proprietatea Universității din Bucureşti se face numai cu aprobarea în scris a șefului direct al solicitantului.

Accesul de la distanţă la reţeaua Universității din Bucureşti se va realiza numai prin echipamente aprobate, folosind protocoale aprobate de către Responsabilul IT și managementul Universității din Bucureşti.

Utilizatorii din interiorul rețelei de comunicație a Universității din Bucureşti nu se pot conecta la altă reţea.

Utilizatorii nu trebuie să extindă sau să retransmită serviciile de reţea în nici un fel (pe nici o 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 Responsabilului IT.

Sistemele computerizate din afara Universității din Bucureşti care necesită conectare la reţea trebuie să se conformeze cu standardele reţelei interne ale Universității din Bucureşti.

Utilizatorii nu au dreptul să descarce, să instaleze sau să ruleze programe de securitate care pot dezvălui slăbiciuni în securitatea unui sistem. De exemplu, utilizatorii Universității din Bucureşti nu au dreptul să ruleze programe de spargere a parolei, sustragere de pachete, scanare a porturilor, în timp ce sunt conectaţi la reţeaua Universității din Bucureşti.

Utilizatorii nu au dreptul să modifice, reconfigureze, instaleze, dezinstaleze echipamente de reţea, cabluri, prize de conexiuni.

Serviciul de administrare a numelor și adreselor IP este deservit exclusiv de către Responsabilul IT.

Serviciile de interconectare a reţelei Universității din Bucureşti cu alte reţele sunt realizate exclusiv de către Responsabilul IT.

Nu este permisă instalarea şi/sau modificarea echipamentelor utilizate pentru conectare la reţea (inclusiv plăci de reţea) fără aprobarea Responsabilului IT. Tipul şi modelul plăcilor de reţea şi tuturor echipamentelor care se pot conecta în reţea trebuie să fie aprobate de către Responsabilul IT.

5.8. Configurarea sistemelor informatice pentru accesul la reţeaua de comunicaţii

Infrastructura de comunicaţii și reţeaua de comunicații digitale a Universității din Bucureşti este administrată de către Responsabilul IT, 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 Responsabilul IT sau de către un furnizor avizat explicit de către Responsabilul IT.

Toate echipamentele, fără excepţie, conectate la reţeaua de comunicații trebuie configurate conform specificaţiilor Responsabilului IT.

Toate dispozitivele hardware, inclusiv plăcile de reţea, care se vor conecta la reţeaua Universității din Bucureşti, trebuie să fie însoţite de o aprobare tip (producător, model etc.) din partea Responsabilului IT.

Modificarea configuraţiei oricărui dispozitiv activ conectat la reţeaua de comunicații se face numai cu aprobarea Responsabilului IT.

Infrastructura de comunicaţii de date a Universității din Bucureşti 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 Responsabilul IT.

Adresele de reţea sunt alocate dinamic sau static numai de către Responsabilul IT.

Toate conectările în reţeaua de comunicaţii a Universității din Bucureşti reprezintă sarcină a Responsabilului IT, conectarea se va face numai în baza unei cereri standard aprobată de către șeful direct.

Toate conectările dintre reţeaua de comunicații a Universității din Bucureşti şi alte reţele de comunicaţii, publice sau private, sunt responsabilitatea exclusivă a Responsabilului IT.

Echipamentele de protecţie a reţelei de comunicaţie a Universității din Bucureşti (firewall) se vor instala de către Responsabilul IT.

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 Universității din Bucureşti) fără aprobare din partea Responsabilului IT.

Utilizatorilor li se interzice instalarea de dispozitive hardware de reţea sau de programe care furnizează servicii de reţea fără aprobarea Responsabilului IT.

Utilizatorilor nu le este permis accesul la dispozitivele hardware ale reţelei.

5.9. Utilizarea echipamentelor

Utilizatorul este responsabil de păstrarea în siguranță și folosirea corectă în scopurile destinate și autorizate a echipamentelor care i-au fost puse la dispoziție de Universitate. Acestea includ stații de lucru fixe și mobile, imprimante, telefoane mobile și fixe și alte mijloace de procesare a informațiilor, inclusiv software-ul asociat.

Toate stațiile de lucru trebuie să fie asigurate împotriva accesului neautorizat atunci când sunt lăsate nesupravegheate. Aceasta se poate face prin blocarea calculatorului, log off sau cu un screensaver protejat cu parolă, cu funcția de activare automată setată la 5 minute sau mai puțin. La sfârșitul programului de lucru acestea, precum și orice aparatură electrică și electronică, trebuie să fie oprite.

De asemenea:

- CD-urile, DVD-urile, alte medii de stocare nu trebuiesc lăsate la vedere atunci când nu sunt folosite.
- Daca ele conţin date de maximă confidenţialitate, trebuie să fie ţinute sub cheie.
- CD-urile, DVD-urile, mediile de stocare mobile trebuie păstrate departe de acţiunile mediului înconjurător cum ar fi: surse de căldura, lumina directă a soarelui şi câmpuri magnetice.

Dispozitivele care nu aparțin Universității din Bucureşti și care se conectează la rețeaua Universității trebuie să se conformeze *Procedurii privind utilizarea echipamentelor de proprietate personală*. Echipamentele conectate fără autorizare sunt expuse monitorizării și vor fi blocate fără avertisment de îndată ce sunt detectate.

Următoarele acțiuni 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,
- interferența cu procedurile Universității 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 configurației hardware a echipamentului,
- scoaterea echipamentului în afara locației fără autorizare prealabilă,
- introducerea şi utilizarea de produse care pun în pericol securitatea informațiilor (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 componență medii de stocare.

5.10. Securitatea echipamentelor și resurselor în afara locației Universității

Folosirea echipamentelor în afara locației Universității creşte riscurile de securitate ale acestora, echipamentele fiind în special vulnerabile la daune fizice, pierdere și furt. În acest caz, se vor aplica următoarele măsuri de securitate:

1. Echipamentul va fi instalat conform *Procedură instalare echipamente* ;
2. În momentul părăsirii Universității, echipamentul poate fi utilizat pentru resursele online (ex. e-mail) şi va exista acces la informaţiile statice;
3. Update-urile aplicaţiilor (de exemplu: sistem de operare, antivirus, Suita Office etc.) se vor face doar la revenirea cu echipamentul în reţeaua Universităţii din București. Utilizatorul are obligaţia ca la un interval de maximum 2 săptămâni să introducă echipamentul în reţeaua internă a Universităţii din București pentru actualizări ;
4. Accesul la aplicaţiile de pe serverele Universităţii din București (ex. Emsys, SAL, UMS) se va face prin VPN cu aprobarea șefului direct, aprobarea pentru utilizarea VPN-ului fiind comunicată Direcției IT&C;
5. Documentele personale (valabil pentru toate echipamentele) se vor ţine într-un folder "Personal".

Furtul sau pierderea unui echipament scos în afara Universităţii din București vor fi raportate imediat șefului ierarhic și Direcției IT&C.

Detalii suplimentare în *Politica privind dispozitivele mobile și lucrul de la distanța*.

5.11. Utilizarea echipamentelor proprietate personală

Universitatea din Bucureşti poate permite angajaților sau persoanelor terțe să folosească echipamente proprietate personală (EPP) pentru îndeplinirea sarcinilor de serviciu.

Următoarele echipamente proprietate personală sunt permise:

a) dispozitive de tip smartphone având sisteme de operare: iOS, Android, Blackberry sau Windows;
b) tablete având sisteme de operare: iOS, Android, Windows;
c) laptop-uri;
d) 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 informațiilor, cum ar fi:

- pierderea, dezvăluirea sau alterarea informațiilor Universității din Bucureşti stocate pe EPP;
- incidente care implică amenințări la adresa infrastructurii informatice a Universității sau compromiterea acestei infrastructuri (de exemplu: viruși, malware, hacking);
- nerespectarea legilor, reglementărilor și obligațiilor contractuale (de exemplu, protecția datelor cu caracter personal, legislația anti-piraterie etc.);
- nerespectarea drepturilor de proprietate intelectuală pentru informațiile universității create, stocate, procesate sau transmise pe EPP.

Angajații care folosesc EPP pentru îndeplinirea sarcinilor de serviciu trebuie să fie autorizați în mod explicit să facă acest lucru. Autorizarea va fi dată de Responsabilul IT la cererea șefului direct ca răspuns la o solicitare în care este explicat motivul solicitării. Pentru autorizare, Responsabilul IT va putea cere informații despre EPP care va fi utilizat.

Utilizatorii trebuie să asigure aceleași măsuri de protecție a informațiilor ca și cele aplicate pentru echipamentele Universității din Bucureşti și nu trebuie să introducă riscuri inacceptabile (exemplu: malware) în rețeaua universității prin utilizarea de echipamente nesigure.

Universitatea din Bucureşti își rezervă dreptul de a refuza sau de a retrage autorizarea în cazul în care consideră că echipamentul nu este adecvat și/sau nu este folosit în interesul universității.

În timp ce utilizatorii au o așteptare rezonabilă de intimitate asupra informațiilor lor personale pe propriul echipament, dreptul Universității de a controla propriile date și de a gestiona EPP poate duce ocazional la accesul neintenționat al personalului de asistență la informațiile lor personale. Pentru a reduce posibilitatea unui astfel de acces, utilizatorii trebuie să păstreze datele lor personale separat de datele Universității, în directoare separate, denumite în mod sugestiv.

5.12. Securizarea serverelor

Un server nu trebuie conectat la reţeaua Universității din Bucureşti până când nu se află într-o stare sigură, acreditată de către Responsabil IT.

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 și a driver-lor care nu sunt necesare;
- Setarea/activarea parametrilor de securitate, a protecţiilor pentru fişiere și activarea jurnalelor de monitorizare;
- Dezactivarea sau schimbarea parolelor conturilor predefinite;
- Securizarea accesului fizic la aceste echipamente.

Responsabilul IT va monitoriza obligatoriu pentru serverele principale, procesul de instalare şi aplicarea regulată a patch-urilor de securitate.

5.13. Detectarea accesului neautorizat

Procesele de înregistrare şi verificare a activității sistemelor de operare, conturilor utilizator şi programelor trebuie să fie funcţionale pe toate sistemele active (host, server, echipamente de reţea).

Trebuie activate funcţiile de anunţare a persoanelor responsabile oferite de firewall-uri și sistemele de control al accesului la reţea.

Trebuie activate funcţiile de înregistrare a evenimentelor pe dispozitivele firewall şi pe toate sistemele de control al accesului.

Înregistrările de verificare ale dispozitivelor de control al accesului trebuie monitorizate/revizuite (examinate) zilnic de către Responsabilul IT.

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 Responsabilul IT.

Utilizatorii sunt obligaţi să raporteze orice anomalii în performanţa sistemelor utilizate cât şi orice semne ale unor posibile infracţiuni la Responsabilul IT.

5.14. Modificări ale configuraţiei sistemului

Orice modificare asupra unei componente a configuraţiei sistemului din cadrul Universității din Bucureşti, cum ar fi: sisteme de operare, componente hardware, echipamente şi componente de reţea, aplicaţii, este supusă prezentului regulament și trebuie să urmeze procedurile în vigoare.

Toate modificările care afectează mediul de funcţionare a sistemelor componente ale sistemului informatic (ex: aparate de aer condiţionat, instalații de apă, încălzire, instalații electrice și 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 Responsabilul IT. 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 și aprobate de către conducerea departamentului sau de către managementul universității.

Modificările planificate trebuie anunţate cu cel puțin 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 Universității 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;
- informații de contact pentru utilizator;
- natura modificării;
- indicarea succesului sau nereuşitei modificări.

5.15. Utilizarea reţelei Internet şi Intranet

Programele pentru acces la reţeaua Internet sunt destinate utilizatorilor autorizaţi pentru a fi folosite în scopul desfășurării activității specificate în fișa postului.
Utilizatorul care folosește Internetul, e-mail-ul sau resurse de pe Internet este obligat:

1. să se asigure că toate comunicaţiile se fac în scopuri profesionale şi nu interferează cu productivitatea personală.
2. să fie responsabili pentru conţinutul materialelor – text, imagine, audio sau de altă natură care plasează sau trimite pe Internet. Toate comunicaţiile vor avea ataşate numele angajatului.
3. Angajatul este obligat să cunoască şi să respecte toate politicile IT&C și procedurile asociate ale Universităţii din București 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 Responsabilul IT. 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.

Nu este permisă utilizarea sistemelor informatice ale Universității din Bucureşti în scop personal sau pentru solicitări personale ce nu au legătură cu universitatea.
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 Universităţii din București şi/sau acţiuni în instanţă ale deţinătorului dreptului de autor.

5.16. Site-uri web facultăți și Universitatea din Bucureşti

Toate site-urilor web aparținând facultăților și Universității din Bucureşti trebuie să se supună regulilor stabilite la nivelul Universității din punct de vedere al aspectului și al securității.
Nu se vor publica pe site-urile web ale Universității din Bucureşti materiale cu caracter ofensiv sau de hărţuire.
Orice material confidenţial al Universității din Bucureşti transmis prin reţeaua Internet trebuie criptat.

5.17. Mijloace de comunicaţie

Adresa de e-mail furnizată de Universitatea din Bucureşti și mailbox-ul asociat acesteia, adresa IP și, după caz, numărul de telefon fix, telefon mobil și conexiunea de date mobile sunt resurse puse la dispoziția utilizatorilor de Universitate 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 Universității și nu introduce riscuri suplimentare pentru universitate.

Următoarele acțiuni sunt strict interzise utilizatorilor:

- utilizarea necorespunzătoare a mijloacelor de comunicare, inclusiv, dar fără a se limita la: sprijinirea activităților ilegale, procurarea și distribuirea de materiale sau mesaje cu caracter ofensator, rasist, obscen, discriminator sau în scop de hărțuire, defăimare sau amenințare,
- procurarea și 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 protejate prin legea dreptului de autor fără permisiunea expresă,
- utilizarea mijloacelor de comunicare pentru publicitate neautorizată, relații de afaceri care nu implică sau sunt contrare intereselor Universității din Bucureşti, campanii politice, utilizarea în scop distractiv sau orice alte scopuri care nu au legătură cu activitatea Universității,
- 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 identități 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 informații confidențiale sau secrete de serviciu altor destinatari decât cei autorizați să primească aceste informații,
- utilizarea adresei de e-mail sau a adresei IP pentru a se angaja în activități care încalcă politicile sau orientările Universității; postarea pe grupuri publice de știri, forumuri sau rețele sociale folosind adresa de e-mail sau adresa IP ale Universității, reprezintă compania în fața publicului și prin urmare trebuie efectuată cu discernământ pentru a evita reprezentarea greșită sau depășirea autorității de a reprezenta poziția universității.

Orice mesaj și/sau informaţie trimisă prin intermediul rețelelor publice pot fi identificate și atribuite Universității din Bucureşti. Din acest motiv, postarea pe forumuri sau alte site-uri de informații care implică numele sau adrese de e-mail ale Universității din Bucureşti se va face fără furnizarea de informații

confidenţiale sau care pot afecta reputația universității. Părerile personale exprimate pe astfel de site-uri sau forumuri vor fi însoțite de nota: "Părerile exprimate sunt personale şi nu reprezintă poziția oficială a Universității din Bucureşti. "

5.18. Utilizarea resurselor informatice în scop personal

Mijloacele de procesare a informației puse la dispoziţie de Universitatea din Bucureşti sunt destinate în primul rând îndeplinirii sarcinilor de serviciu.

Utilizarea limitată în scopuri personale, ocazională sau accidentală, a mijloacelor de procesare a informației 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 universității, în locații separate de cele care conţin informații ce aparţin universității. Toate mesajele şi fişierele personale aflate în sistemul informatic pot fi supuse verificării de conformitate cu Politicile IT&C a Universității din Bucureşti.

Universitatea din Bucureşti nu își asumă nicio responsabilitate cu privire la securitatea acestor informații, întreaga responsabilitate (inclusiv realizarea copiilor de siguranță) revenind utilizatorului.

5.19. Detectarea viruşilor

Toate staţiile de lucru de sine stătătoare sau conectate la reţeaua de comunicații a Universității din Bucureşti, trebuie să utilizeze programe antivirus aprobate de către Responsabilul IT.

Programele antivirus nu trebuie dezactivate.

Configuraţia programului antivirus trebuie să nu fie modificată într-un mod care să reducă eficacitatea programului.

Frecvenţa actualizărilor automate a programului antivirus trebuie asigurată de către utilizator.

Orice server de fişiere conectat la reţeaua Universității trebuie să utilizeze un program antivirus aprobat în scopul detectării şi curăţirii viruşilor care pot infecta fişierele puse la dispoziţie.

Orice server sau gateway pentru e-mail trebuie să folosească un program antivirus pentru e-mail aprobat și trebuie să respecte regulile de instalare şi utilizare a acestui program.

Orice virus care nu a putut fi înlăturat automat de către programul antivirus constituie un incident de securitate şi trebuie raportat imediat Responsabilului IT.

5.20. Returnarea resurselor la terminarea contractului

Utilizatorul va returna Universității, 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 ş.a.m.d.

5.21. Excepții

Excepțiile de la regulile definite în această politică vor fi puse în aplicare numai după autorizarea prealabilă a Responsabilului IT, care va fi solicitată în scris și va include obligatoriu motivul excepției.
Toate excepțiile vor fi considerate evenimente de securitate și vor fi comunicate Responsabilului IT și vor fi înregistrate de acesta în Registrul incidentelor de securitate, specificând data și ora, descrierea, motivul și modul de gestionare a riscurilor.

6. Responsabilități

Forurile decizionale ale Universității din Bucureşti au următoarele responsabilități:

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

Conducerea Facultăților / Instituțiilor:

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

Direcția IT&C (prin angajații săi) are următoarele responsabilități:

- propune modificări ale Politicii IT&C;
- elaborează și propune pentru aprobare politici și proceduri de gestionare și de securitate a resurselor informatice și de comunicații în conformitate cu Politica IT&C;
- tratează incidentele de securitate în scopul minimizării efectului distructiv al acestora asupra resurselor informatice și de comunicaţii;
- informează conducerea în caz de incidente, intervenție și rezolvarea incidentelor de securitate a informațiilor;
- asigură existenţa jurnalelor şi a traseelor auditării pentru orice tip de acces în sistem conform procedurilor asociate;
- planifică, implementează și verifică zilnic soluțiile de securitate a informațiilor: server antivirus, firewall, server de actualizări de securitate, backup, acces securizat la camera tehnică, asigurare aer condiționat, asigurare alimentare cu energie electrică/UPS;
- menține înregistrări privind configurația, aplicațiile și serviciile instalate (fișa de server), pentru a se putea reface sistemul în caz de dezastru;
- inventariază periodic aplicațiile și serviciile instalate și verifică dacă sunt autorizate;

- administrează sistemele IT și aplică măsurile de securitate și alte cerințe ale programului de securitate a informațiilor pentru sistemele informatice pentru care are atribuită responsabilitatea.

Șefii entităților organizatorice sunt responsabili pentru:

- implementarea de zi cu zi a Politicii IT&C și a procedurilor aferente acesteia;
- asigurarea că măsurile de securitate tehnice, fizice și procedurale adecvate sunt implementate în conformitate cu Politica IT&C și sunt aplicate în mod corespunzător și de către tot personalul, asigurarea resurselor și efectuarea analizelor necesare pentru a se asigura că informațiile și 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 informațiilor din zona lor de responsabilitate (incidentele de securitate a informațiilor), identificarea și clasificarea informațiilor și echipamentelor din zona lor de responsabilitate și desemnarea deținătorilor (responsabililor) pentru acestea;
- informarea Direcției IT&C la schimbarea responsabililor de active.

Utilizatorii datelor / sistemelor (angajați, studenți și terți care acționează într-o modalitate similară, cum ar fi furnizori de servicii, studenți ai altor facultăți, profesori ai altor facultăți etc.):

- cunosc și respectă Politica IT&C și procedurile aferente acesteia aplicabile pentru locurile lor de muncă,
- răspund direct de resursele informatice și de comunicații încredințate 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	1		-		20	-Elaborare conf. ISO 27001 -Elaborare conform OSGG 600/2010	