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

Nr. de înregistrare: 19516, din 04.09.2019

POLITICĂ PRIVIND SECURITATEA INFORMAȚIILOR

Ediția 1, Revizia 0, Data 12.08.2019

Avizat,

Secretariat Comisie de Monitorizare

Silvia Pădure

Elaborat,

Responsabil protecţia datelor

Dan Iordache, Total Data Management S.R.L.

Cuprins

1. Introducere

În activitățile desfășurate în cadrul Universității din București se creează, colectează, stochează şi prelucrează cantităţi mari de date. Informaţiile şi procesele, sistemele şi reţelele asociate, precum şi personalul implicat în exploatarea, manipularea şi protecţia acestora sunt resurse importante pentru Universitatea din București şi, în consecinţă, merită sau necesită protecţie împotriva diverselor pericole.

Resursele sunt expuse atât ameninţărilor intenţionate, cât şi celor accidentale, iar procesele, sistemele şi reţelele asociate, precum şi personalul pot prezenta vulnerabilităţi inerente. Schimbările intervenite în modul de desfășurare a activităților, în cadrul sistemelor utilizate sau alte schimbări externe (cum ar fi, legi şi reglementări noi) pot crea noi riscuri de securitate a informaţiei. Prin urmare, dată fiind multitudinea de moduri în care ameninţările pot profita de vulnerabilităţi pentru a dăuna organizaţiei, riscurile de securitate a informaţiei sunt întotdeauna prezente. O securitate a informaţiei eficace reduce aceste riscuri prin protejarea organizaţiei împotriva ameninţărilor şi vulnerabilităţilor şi apoi reduce impactul asupra resurselor ei.

Securitatea informaţiilor este obţinută prin implementarea unui set adecvat de mijloace de control, incluzând politici, procese, proceduri, structuri organizatorice şi funcţii software şi hardware. Aceste mijloace de control necesită să fie stabilite, implementate, supravegheate, revizuite şi îmbunătăţite, dacă este necesar, pentru a se asigura atingerea obiectivelor de securitate ale organizaţiei.

Pe lângă bunele practici stabilite la nivelul organizației, anumite categorii de date sunt supuse şi reglementărilor legislației naţionale și este vital ca personalul să recunoască toate detaliile legate de manipularea informațiilor Universității din București.

2. Scop

Politica de securitate a informațiilor are ca scop asigurarea integrității, confidenţialității şi disponibilităţii informaţiei.

Confidenţialitatea se referă la protejarea informațiilor împotriva accesului neautorizat. Fiecare utilizator răspunde personal de confidenţialitatea informațiilor încredinţate sau create.

Integritatea se referă la măsurile şi procedurile utilizate împotriva modificărilor sau distrugerii neautorizatea tuturor informațiilor în format letric sau electronic necesare desfășurării activităților din cadrul organizației.

Disponibilitatea se realizează prin asigurarea accesului la informațiile necesare desfășurării activităţilor din cadrul organizației.

De asemenea, Politica de securitate are ca scop stabilirea cadrului necesar pentru elaborarea politicilor și procedurilor de securitate a informațiilor.

3. Domeniu de aplicare

Politica se aplică tuturor angajaților Universităţii din Bucureşti, colaboratorilor și angajaţilor furnizorilor de servicii care accesează resursele informaţionale ale Universităţii din Bucureşti.

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

4.1.Documente de referinţă

- OSSG 600/2018 – privind aprobarea Codului controlului intern managerial al entităţilor publice;
- 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;
- Regulamentul (UE) 679/ 2016 al Parlamentului European și al Consiliului (GDPR);
- Carta Universității din București

4.2.Politici și proceduri asociate

Următoarele politici și proceduri ar trebui să fie consultate împreună cu Politica privind securitatea informațiilor:

Politici şi proceduri asociate **Politicii privind securitatea informațiilor a Universității din Bucureşti**:
- Procedura privind securitatea resursele umane,
- Politica privind securitatea fizică şi securitatea mediului de lucru,
- Politici privind biroul curat, protejarea ecranului și tipărirea documentelor,
- Politică privind relațiile cu furnizorii.

Politici şi proceduri asociate **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.

Politica Universității din București privind protecția datelor și procedurile asociate acesteia:
• Procedura desemnare Responsabil protecţia datelor, PO-DPO-01;
• Procedura Evidența prelucrărilor de date cu caracter personal, PO-DPO-02;
• Procedura de evaluare a impactului privind protecția datelor, PO-DPO-03;
• Procedura de evaluare a interesului legitim, PO-DPO-04;
• Procedura privind acordarea și retragerea consimțământului, PO-DPO-05;
• Procedura privind managementul persoanelor împuternicite, PO-DPO-06;
• Procedura privind informarea persoanelor vizate, PO-DPO-07;
• Procedura de organizare a evenimentelor, PO-DPO-08;
• Procedura utilizare colaboratori, PO-DPO-09;
• Procedura privind instruirea GDPR, PO-DPO-10;
• Procedura privind supravegherea video, PO-DPO-11;
• Procedura solicitare persoană vizată, PO-DPO-12;
• Procedura privind managementul încălcărilor securităţii datelor cu caracter personal, PO-DPO-13;
• Procedura de notificare a încălcării confidenţialităţii datelor, PO-DPO-14;
• Procedura privind eliminarea înregistrărilor, PO-DPO-15.

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

5.1.Definiţii ale termenilor

Nr. crt.	Termenul	Definiția și/sau, dacă este cazul, actul care definește termenul
1.	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.
2.	Securitatea informaţiei	Păstrarea confidenţialităţii, integrităţii şi a disponibilităţii informaţiei.
3.	Confidenţialitate	Proprietatea ca informaţia să nu fie făcută disponibilă sau divulgată unor persoane, entităţi, sau procese neautorizate.
4.	Integritate	Proprietatea de a proteja acurateţea şi completitudinea resurselor.
5.	Disponibilitate	Proprietatea de a fi accesibil şi utilizabil la cerere de către o entitate autorizată.
6.	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.
7.	Ameninţare	Cauză potenţială a unui incident nedorit care poate produce daune unui sistem sau organizaţii.
8.	Vulnerabilitate	Slăbiciune a unei resurse sau a unui mijloc de control care poate fi exploatată de o ameninţare.

Nr. crt.	Termenul	Definiția și/sau, dacă este cazul, actul care definește termenul
9.	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.
10.	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.

5.2.Abrevieri ale termenilor

Nr. crt.	Abrevierea	Termenul abreviat
1.	GDPR	Regulamentul General pentru Protecția Datelor personale
2.	CERT-RO	Centrul naţional de răspuns la incidente de securitate cibernetica
3.	PLT	Politică
4.	SEC	Securitatea informaţiei
5.	UB	Universitatea din Bucureşti

6. Politică

6.1. Declarație

Informațiile în format olografic, letric sau electronic utilizate în activitățile desfășurate în cadrul Universității din Bucureşti sunt proprietatea acesteia și reprezintă bunuri strategice care trebuiesc administrate ca atare.

Compromiterea securității acestor resurse poate afecta capacitatea Universității din Bucureşti de a oferi servicii de calitate și poate conduce la fraude, incidente legate de confidenţialitatea informațiilor, distrugerea informațiilor, violarea unor clauze contractuale sau afectarea credibilității organizației 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 informaționale;
- să stabilească practici prudente şi acceptabile privind utilizarea resursele informaționale ale Universității din Bucureşti;
- să instruiască utilizatorii care au dreptul de folosire a acestor resurse privind responsabilităţile asociate unei astfel de utilizări.

Politica de securitate a informațiilor se aplică nediscriminatoriu tuturor angajaților, colaboratorilor și angajaților furnizorilor de servicii cărora li s-a permis accesul la orice resursă informațională a

Universității din Bucureşti. Fiecare angajat, colaborator sau angajat al furnizorilor de servicii este răspunzător pentru aplicarea întocmai în activitatea sa a politicilor şi procedurilor de securitate interne în vigoare, elaborate şi aprobate, conform cu legislaţia specifică şi reglementările interne de funcţionare.
De asemenea, fiecare angajat, colaborator sau angajat al furnizorilor de servicii are obligaţia raportării oricărui incident de securitate sesizat.

6.2.Clasificarea informaţiilor

Clasificarea informaţiilor este necesară pentru a permite atât alocarea resurselor necesare protejării acestora, cât și pentru a determina pierderile potenţiale ca urmare a modificărilor, pierderii/ distrugerii sau divulgării acestora.
Managementul Universității din Bucureşti răspunde de evaluarea periodică a schemei de clasificare a informaţiilor.
Toate informaţiile din Universitătea din Bucureşti trebuie să se regăsească în una din următoarele categorii:

- Publice: Acestea sunt informații accesibile oricărui utilizator din interiorul sau exteriorul Universității din Bucureşti. Divulgarea, utilizarea neautorizată a acestora nu produce efecte asupra organizației sau aceste efecte sunt nesemnificative. Utilizatorii care furnizează aceste informații sunt responsabili de asigurarea integrității şi disponibilității acestora în raport cu cerinţele Universității din Bucureşti. Exemple: Informaţiile de pe aviziere, informațiile de pe site-ul web, comunicate de presă ș.a.m.d.

- Confidenţiale: Accesul la aceste informații va fi restricţionat la persoanele care trebuie să le cunoască pentru îndeplinirea unor activități prevăzute în fișa postului sau în diferite contracte încheiate de către Universitatea din București cu terți (din sectorul public sau privat). Datele confidențiale nu pot fi copiate, distribuite sau şterse fără acordul șefului entității organizatorice, conducerii Facultății sau a managementului Universității din Bucureşti. Exemple: informații privind studenții, informații legate de angajați, chei criptografice, conturi administrative de pe serverele de gestiune a informațiilor ș.a.m.d.

- Secrete: Informaţiile pe care Universitatea din Bucureşti trebuie să le protejeze conform legislaţiei în vigoare (Legea nr.182/2002, H.G. nr.585/2002 și H.G. nr.781/2002). Aceste date vor fi copiate şi distribuite în cadrul Universității din Bucureşti doar utilizatorilor autorizaţi.

6.3.Securitatea fizică şi a mediului de lucru

Prelucrările de date și echipamentele de prelucrare a informaţiilor importante sau sensibile trebuie desfășurate sau amplasate în zone sigure, protejate de un perimetru de securitate definit. Ele trebuie protejate fizic împotriva accesului neautorizat, deteriorărilor și intervenţiilor.

Protecţia fizică este realizată prin crearea uneia sau mai multor bariere fizice în jurul incintelor Universității din Bucureşti și a sistemelor de prelucrare a informaţiilor. Folosirea barierelor multiple oferă o protecţie suplimentară, în sensul că eşecul unei singure bariere nu înseamnă compromiterea imediată a securităţii.

Universitatea din Bucureşti aplică măsuri de protecţie fizică şi împotriva incendiilor, inundaţiilor şi a oricăror alte forme de dezastre naturale sau produse de oameni.

Toate utilităţile suport, precum electricitatea, încălzirea/ ventilaţia sau aerul condiţionat sunt dimensionate corespunzător sistemelor pe care le servesc. Utilităţile suport sunt verificate cu regularitate şi testate pentru a se asigura buna lor funcţionare şi pentru a se reduce riscul funcţionărilor incorecte sau al defectărilor.

Informații suplimentare despre securitatea fizică și a mediului de lucru pot fi găsite în **Politica privind securitatea fizică şi a mediului de lucru**.

6.4. Securitatea resurselor umane

Universitatea din București trebuie să aplice măsuri astfel încât angajații, colaboratorii și angajații furnizorilor de servicii:

- să înţeleagă responsabilităţile care le revin și să fie corespunzători pentru rolurile alocate;
- să reducă riscul de furt, fraudă sau de folosire necorespunzătoare a activelor folosite la prelucrarea datelor;
- să fie pregătiţi să susţină și să aplice politica de securitate a Universității din București pe durata contractului de muncă sau a contractului în baza căruia au acces la informații;
- să părăsească Universitatea din Bucureşti sau să-și schimbe locul de muncă într-o manieră reglementată.

Detalii despre măsurile adoptate în cazul resurselor umane pot fi găsite în **Politica privind securitatea resurselor umane**.

6.5. Securitatea documentelor utilizate

Angajații, colaboratorii și angajații furnizorilor de servicii care utilizează documente în format olograf, letric sau pe suport electronic conținând informații confidențiale (inclusiv date cu caracter personal) sau secrete aparţinând Universității din București, trebuie să le protejeze în mod adecvat împotriva accesului neautorizat atunci când nu le utilizează sau le lăsă nesupravegheate.
Detalii despre măsurile de securitate aplicate în cazul documentelor utilizate pot fi găsite în **Politica privind biroul curat, protejarea ecranului și tipărirea documentelor**.

6.6. Securitatea IT&C

O mare parte din datele create, colectate sau stocate se bazează pe utilizarea resurselor informatice și de comunicații ale Universității din Bucureşti. Organizația investește substanţial în resurse financiare și umane pentru a putea asigura integritatea, confidenţialitatea şi disponibilitatea acestor sisteme și de aceea aceste resurse trebuie utilizate și administrate corespunzător.

Integritatea, confidenţialitatea şi disponibilitatea acestor resurse este obţinută prin implementarea unui set adecvat de mijloace de control, incluzând politici, proceduri, procese, aplicații software şi echipamente hardware. Astfel, sunt aplicate măsuri în vederea:

- administrării conturilor de acces la date, sisteme informatice și site-uri web;
- administrării accesului administrativ la sistemele informatice și la reţeaua de comunicaţii;

- gestionării aplicaţiilor ce se pot utiliza în cadrul organizaţiei;
- configurării sistemelor informatice ce accesează reţeaua de comunicaţii;
- securizării serverelor și a dispozitivelor de stocare a datelor;
- gestionării back-up-urilor şi arhivelor;
- utilizării corespunzătoare a echipamentelor;
- detectării accesului neautorizat;
- gestionării modificărilor efectuate echipamentelor;
- asigurării securităţii echipamentelor și resurselor scoase în afara organizaţiei;
- utilizării echipamentelor proprietate personală;
- utilizării corespunzătoare a reţelelor Intranet și Internet;
- gestionării mijloacelor de comunicaţie puse la dispoziţia angajaţilor și colaboratorilor;
- gestionării site-urilor web aparţinând Universităţii din București;
- detectării virușilor;
- asigurării securităţii în cazul accesului de la distanță;
- managementului incidentelor de securitate.

Detalii despre măsurile de securitate aplicate în resurselor IT&C pot fi găsite în **Politica IT&C** și în procedurile aferente acesteia.

6.7. Protecția datelor cu caracter personal

În activitățile din cadrul Universității din București se creează, colectează, stochează și prelucrează cantități mari de date din diverse categorii de date cu caracter personal, aparţinând unor tipuri diferite de persoane vizate, cum ar fi angajați, studenţi, alumni, candidaţi posturi vacante, clienți/ furnizori sau alte categorii de persoane.

Protecția datelor personale este o componentă importantă a oricărei activități, astfel că toate informațiile trebuie să fie prelucrate în siguranță și în conformitate cu politica stabilită. Pe lângă bunele practici stabilite la nivelul instituției, anumite categorii de date sunt supuse şi reglementărilor legislației naţionale și este vital ca personalul să recunoască toate detaliile legate de manipularea informațiilor și datelor Universității din București.

Respectarea cerințelor legate de protecția datelor cu caracter personal este responsabilitatea tuturor membrilor Universității din București. Orice încălcare deliberată a acestei politici poate conduce la măsuri disciplinare, la retragerea accesului la facilitățile Universității din București sau chiar la urmărirea penală.

Informații suplimentare despre protecția datelor cu caracter personal pot fi găsite în **Politica privind protecția datelor și în procedurile aferente acesteia**.

6.8.Conștientizare și instruire cu privire la securitatea informației

Toți angajații Universității din București, colaboratorii sau angajații furnizorilor de servicii trebuie să fie conștientizați sau instruiți cu privire a politicile și procedurile organizaționale corespunzătoare fiecarui loc de muncă sau activități desfășurate.

În acest scop, șefii entităților organizatorice trebuie să stabilească un program de instruire a personalului din subordine cu privire la cerințele legate de securitatea informațiilor aplicabile pentru fiecare loc de muncă sau activități desfășurate.

6.9. Relațiile cu furnizorii

Unele din activităţile desfășurate în cadrul Universității din București sunt realizate de către furnizori de servicii. În acest caz, Universitatea din Bucureşti recurge doar la furnizori de servicii care oferă garanții suficiente pentru punerea în aplicare a măsurilor tehnice şi organizatorice prevăzute de politica de securitate și de politicile și procedurile asociate acesteia.

Activitatea desfășurată de către un furnizor de servicii trebuie reglementată printr-un contract sau alt act juridic care are caracter obligatoriu pentru furnizorul de servicii şi care trebuie să stabilească cel puţin durata desfășurării activităţilor, natura activităţilor desfășurate şi măsurile tehnice şi organizatorice ce trebuie implementate de furnizor sau respectate de către angajaţii furnizorului de servicii.

În cazul în care o prelucrare de date cu caracter personal urmează să fie realizată în asociere între doi sau mai mulţi operatori, trebuie încheiat un acord, contract sau alt act juridic care să precizeze responsabilităţile fiecărei părţi în ceea ce priveşte îndeplinirea obligaţiilor care le revin în temeiul regulamentului GDPR, în special cu privire la modul de exercitare a drepturilor persoanelor vizate şi îndatoririle fiecărei parti de furnizare a informaţiilor către persoanele vizate de prelucrări.

Detalii despre măsurile de securitate aplicate în cazul relaţiilor cu furnizorii pot fi găsite în **Politica privind relațiile cu furnizorii**.

6.10. Măsuri disciplinare

Toți angajații Universității din București, colaboratorii sau angajații furnizorilor de servicii sunt obligați să respecte această politică de securitate a informațiilor precum și politicile și procedurile asociate acesteia.

Încălcarea prevederilor politicii de securitate a informațiilor sau a politicilor și procedurile asociate acesteia poate face obiectul unor măsuri disciplinare, civile, contravenţionale ori penale, în raport cu gravitatea faptei săvârșite.

7. Responsabilități

7.1. Managementul Universității

Managementul Universității din Bucureşti are următoarele responsabilități:

- stabileşte și aprobă politica generală, politicile subsecvente și obiectivele de securitate a informațiilor;
- asigură disponibilitatea resurselor necesare pentru managementul securității informațiilor;
- comunică importanța unei gestionări eficiente a securității informației și a respectării cerințelor sistemului de management al securității informațiilor.

7.2. Direcția IT&C

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

- propune modificări ale Politicii IT&C și ale politicilor și procedurilor aferente acesteia;
- propune proceduri de gestionare și de securitate a resurselor informatice și de comunicații în conformitate cu Politica IT&C.

7.3. Management Facultăţi / Șefi entități organizatorice

Managementul Facultăților/ Instituțiilor:

- se asigură că sistemul de management al securității informațiilor atinge rezultatele dorite;
- îndrumă și sprijină personalul să contribuie la eficacitatea sistemului de management al securității informațiilor;
- promovează îmbunătățirea continuă a sistemului de management al securității informațiilor.

Șefii entităților organizatorice sunt responsabili pentru:

- implementarea de zi cu zi a politicilor si procedurile de securitate a informațiilor;
- instruirea personalului din subordine cu privire la cerințele legate de securitatea informațiilor aplicabile pentru fiecare loc de muncă;
- asigurarea că măsurile de securitate tehnice, fizice și procedurale adecvate sunt implementate în conformitate cu politicile și procedurile de securitate 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 informaționale sunt protejate în mod corespunzător în zona lor de responsabilitate;
- informarea persoanei desemnate cu managementul incidentelor de securitate despre încălcările reale sau presupuse ale politicilor de securitate care afectează securitatea informațiilor din zona lor de responsabilitate (incidentele de securitate a informațiilor);
- identificarea și clasificarea informațiilor și activelor informaționale semnificative din zona lor de responsabilitate și desemnarea deținătorilor (responsabililor) pentru acestea;
- informarea Direcției IT&C la schimbarea responsabililor de active informaționale.

7.4. Angajații Universității din Bucureşti

Angajații Universității au următoarele responsabilități:

- respectă toate politicile și procedurile privind securitatea informațiilor aplicabile pentru locurile lor de muncă ;
- participă la instruirile legate de securitatea informațiilor;

- sunt responsabili pentru menținerea securității si confidenţialităţii tuturor informațiilor încredințate;
- informează șefii entităților organizatorice despre încălcările reale sau presupuse ale politicilor de securitate și confidenţialitate a datelor din zona lor de responsabilitate (incidente privind securitatea și confidenţialitatea datelor).

7.5. Colaboratorii și angajații furnizorilor de servicii

Colaboratorii (studenți, studenți ai altor universități, profesori ai altor universități etc.) și angajații furnizorilor de servicii, au următoarele responsabilități:

- respectă toate politicile și procedurile privind securitatea informațiilor și de protecție a datelor aplicabile pentru informațiile la care au acces;
- răspund direct de securitatea și conţinutul informaţiilor şi resursele informatice și de comunicații încredinţate direct sau indirect;
- returnează informațiile încredințate în momentul încheierii relației contractuale sau în momentul solicitării returnării acestora de către Universitate.

8. 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		-		12	-Elaborare conf. ISO 27001 -Elaborare conform OSGG 600/2010	