





<b>REG</b> <i>38/20</i>	<b>POLITICA</b> <b>de asigurare a securității datelor cu caracter personal</b> <b>în cadrul Universității de Stat „Dimitrie Cantemir”</b>	Ediția II
----------------------------	---	-----------

**1. Lista responsabililor de elaborarea, verificarea și aprobarea ediției în cadrul procedurii de sistem**

Elemente privind responsabilii/ operațiunea	Nume, prenume	Funcție	Data	Semnătura
Elaborat	Plevan Natalia	Specialist principal RU	<i>22.01.2020</i>	
Verificat	Chilari Rodica	Șef secție PL	<i>23.01.2020</i>	
Avizat	Erhan Ana	Prorector	<i>24.01.2020</i>	
Aprobat	Hanganu Aurelia	Rector	<i>31.01.2020</i>	

**I. DISPOZIȚII GENERALE**

Cerințele față de asigurarea securității datelor cu caracter personal au drept scop stabilirea regulilor de implementare de către **Universitatea de Stat “Dimitrie Cantemir”** (în continuare USDC) a măsurilor tehnice și organizatorice necesare pentru asigurarea securității, confidențialității și integrității datelor cu caracter personal, prelucrate în cadrul sistemelor informaționale și mecanice de date cu caracter personal și/sau registrelor ținute manual, în conformitate cu prevederile Legii RM nr.133 din 8 iulie 2011 privind protecția datelor cu caracter personal și Hotărârii Guvernului RM nr.1123 din 14.12.2010 privind Cerințele față de asigurarea securității datelor cu caracter personal.

**II. CERINȚE GENERALE**

1. Măsurile de protecție a datelor cu caracter personal reprezintă o parte componentă a lucrărilor de creare, dezvoltare și exploatare a sistemului informațional de date cu caracter personal și vor fi efectuate neîntrerupt de către persoanele responsabile, angajate la USDC.
2. Protecția datelor cu caracter personal este asigurată printr-un complex de măsuri tehnice și organizatorice de preîntâmpinare a prelucrării ilicite a datelor cu caracter personal.
3. Sunt supuse protecției toate resursele informaționale ale USDC, care conțin date cu caracter personal inclusiv :
  - a) suporturile magnetice, optice, laser sau alte suporturi ale informației electronice, masive informaționale și baze de date;
  - b) sistemele informaționale, rețelele, sistemele operaționale, sistemele de gestionare a bazelor de date și alte aplicații, sistemele de telecomunicații, inclusiv mijloacele de confecționare și spațiu multiplicare a documentelor și alte mijloace tehnice de prelucrare a informației;
  - c) carnetele de muncă, dosarele personale ce conțin acte ale persoanelor, suporturi de hârtie etc.
4. Protecția datelor cu caracter personal este asigurată în scopul:
  - a) preîntâmpinării distrugerii, modificării, copierii, blocării neautorizate a datelor cu caracter personal în rețelele telecomunicaționale și resursele informaționale;
  - b) respectării cadrului normativ de folosire a sistemelor informaționale și a programelor de prelucrare a datelor cu caracter personal;
  - c) păstrării posibilităților de gestionare a procesului de prelucrare și păstrare a datelor cu caracter personal;
  - d) recunoașterii și respectării dreptului la viață intimă, familială și privată, prelucrarea datelor cu caracter personal desfășurându-se în conformitate cu prevederile legale în vigoare.

**III. POLITICA DE SECURITATE A DATELOR CU CARACTER PERSONAL**

5. Prin Ordinul USDC este nominalizată persoana responsabilă de întocmirea, menținerea, modificarea și actualizarea politicii de securitate a USDC.
6. Măsurile de securitate emise sunt stabilite conform regulamentelor de securitate ale fiecărui sistem care

- Secția Studii și managementul calității;
- Secția doctorat și cercetare;
- Contabilitate;
- Sistemul informațional(rețeaua de calculatoare).

7. Mecanismul de punere în aplicare a măsurilor de securitate este prevăzut de prezenta Politică de Securitate , prin Regulamentele interne privind prelucrarea și asigurarea securității informațiilor ce conțin date cu caracter personal ale celor 5 subdiviziuni și Nomenclatorul datelor cu caracter personal ,prelucrate în cadrul USDC.
8. Lista nominală a utilizatorilor, autorizați să acceseze datele cu caracter personal este stabilită prin Ordinul intern al USDC.
9. Documentația tehnică cu privire la controalele de securitate este ținută sub formă de registru de către persoana responsabilă, numită prin ordinul USDC pentru fiecare sistem informațional în parte.
10. Orarul controalelor de securitate este stabilit de către persoana numită responsabilă, în conformitate cu regulamentul de securitate al fiecărui sistem care prelucrează date cu caracter personal.
11. Rapoartele despre incidentele de securitate sunt înregistrate în registrele respective de către persoanele responsabile. Fiecare incident urmează a fi adus la cunoștința conducerii Universității în mod de urgență, pentru a putea fi identificată procedura de soluționare a incidentului.

#### **IV. SECURITATEA MEDIULUI FIZIC ȘI A TENOLOGILOR INFORMAȚIONALE FOLOSITE ÎN PROCESUL PRELUCRĂRII DATELOR CU CARACTER PERSONAL**

##### **Secțiunea 1**

12. Accesul în sediile/oficiile/birourile ori spațiile unde sunt amplasate sistemele informaționale de date cu caracter personal este restricționat, fiind permis doar persoanelor care îndeplinesc funcțiile stipulate în Regulamentele interne privind prelucrarea și asigurarea securității informațiilor ce conțin date cu caracter personal ale celor 5 subdiviziuni și doar în timpul orelor de program și însemnelor corespunzătoare (ecusoane).

Accesul în camera de servere este permisă doar personalului IT, administratorului care este numit prin ordin. Personalul străin are acces în această încăpere doar sub stricta supraveghere a unui specialist IT. Toate operațiunile de acces la servere sau alte mijloace tehnice sau software se fac de către personalul IT al USDC.

##### **Secțiunea 2**

13. **Administrarea și monitorizarea accesului fizic.** Se efectuează administrarea și monitorizarea accesului fizic în toate punctele de acces la sistemele informaționale de date cu caracter personal, inclusive se reacționează ca încălcarea regimului de acces.
14. **Camera de servere** este echipată cu ușă metalică și gratii metalice la ferestre.
15. Perimetrul sediilor și încăperii în care sînt amplasate mijloacele de prelucrare a datelor cu carcter personal sunt păstrate integri din punct de vedere fizic, toți pereții sunt întregi, ușile se încuie, iar ferestrele se închid.
16. Pereții exterior ai încăperilor sînt rezistenți, înrările echipate cu lacăte. Birourile amplasate la parter au au ferestrele echipate cu gratii. Ușile și ferestrele se încuie în cazul în care în încăpere lipsesc angajații.
17. Înainte de acordarea accesului fizic la sistemele informaționale de date cu carcter personal se verifică **competențele de acces**. Persoanele noi angajate sunt instruite în domeniul prelucrării datelor cu carcter personal și semnează declarația de confidențialitate emisă în acest sens.
18. Toate fișele personale ale fiecărui angajat, inclusiv carnetele de muncă, sunt păstrate în safeu metallic fiind ocrotit împotriva incendiilor ,în secția resurse umane a USDC.
19. Amplasarea mijloacelor de prelucrare a datelor cu caracter personal corespunde necesității asigurării securității acestora contra accesului nesancționat, furturilor, incendiilor, inundațiilor și altor posibile riscuri.
20. Folosirea tehnicii foto, video, audio sau altor mijloace de înregistrare în perimetrul de securitate este admisă doar în cazul prezenței unei permisiuni speciale a conducerii deținătorului de date cu caracter personal

##### **. Secțiunea 3**

21. Persoanele care accesează sediile UnAȘM sunt **supravegheate de camerele video** . În birourile cu acces interzis pot intra doar sub supravegherea personalului autorizat. În cazul depistării persoanelor cu acces interzis în birourile cu acces limitat, aceștia vor fi rugați să părăsească încăperea în mod cât mai urgent. Incidentul va fi adus la cunoștința conducerii USDC.

##### **Secțiunea 4**

22. Se asigură **securitatea echipamentului electric** utilizat pentru menținerea funcționalității sistemelor informaționale de date cu caracter personal, a cablurilor electrice, inclusiv protecția acestora contra deteriorărilor și conectărilor nesancționate. Cablurile de tensiune sunt separate de cele comunicaționale pentru a exclude bruiatul. Specialiștii IT a USDC efectuează controale, nu mai rar decît o dată în lună în scopul verificării cazurilor de conectare neautorizate la cablurile de rețea.

##### **Secțiunea 5**

23. USDC dispune de mijloace de asigurare a securității antiincendiere a sediilor /oficiilor/ birourilor unde sunt amplasate sistemele informaționale de date cu caracter personal și mijloacele de prelucrare a datelor cu caracter personal.

### **Secțiunea 6**

24. Pentru asigurarea securității informaționale în cazul neutilizării temporare a purtătorilor de informație pe suport de hârtie sau electronică (digitală) care conțin date cu caracter personal, acestea se păstrează în safeuri sau dulapuri metalice care se încuie. Computerele, terminalele de acces și imprimantele sunt deconectate la terminarea sesiunilor de lucru. Este asigurată securitatea punctelor de primire/expediere a corespondenței, precum și securitatea contra accesului neautorizat la aparatele fax și cele de copiere. Accesul fizic la mijloacele de reprezentare a informației care conține date cu caracter personal, în scopul împiedicării vizualizării acesteia de către persoane neautorizate este interzis și controlat. Mijloacele de prelucrare a datelor cu caracter personal, informația care conține date cu caracter personal sau soft-urile destinate prelucrării datelor cu caracter personal sunt scoase din perimetrul de securitate doar în temeiul unei permisiuni scrise a Rectorului USDC .

## **V. IDENTIFICAREA ȘI AUTETIFICAREA UTILIZATORULUI SISTEMULUI INFORMAȚIONAL DE DATE CU CARACTER PERSONAL**

### **Secțiunea 1**

25. Toți utilizatorii (inclusiv personalul care asigură susținerea tehnică, administratorii de rețea, programatorii și administratorii bazelor de date) vor avea un identificator personal (ID-ul utilizatorului), care nu trebuie să conțină semnalmamentele nivelului de accesibilitate al utilizatorului. Pentru confirmarea ID-ului utilizatorului sunt folosite parole. În cazul în care contractul de muncă/raporturile de serviciu ale utilizatorului au fost încetate, suspendate sau modificate și noile sarcini nu necesită accesul la date cu caracter personal ori drepturile de acces ale utilizatorului au fost încetate, suspendate sau modificate și noile sarcini nu necesită accesul la date cu caracter personal ori drepturile de acces ale utilizatorului au fost modificate, ori utilizatorul a abuzat de codurile primite în scopul comiterii unei fapte prejudiciabile, a absentat o perioadă îndelungată, codurile de identificare și autentificare se revocă în mod automat în decursul a două săptămîni de la ultimul acces sau în mod individual imediat, la momentul introducerii modificării în raportul de muncă.
26. Se respectă regulile de asigurare a securității informaționale în cazul alegerii și folosirii parolelor ce includ:
- 1) păstrarea confidențialității parole;
  - 2) interzicerea înscrierii parole pe suport de hârtie, în cazul în care nu se asigură securitatea păstrării acestora;
  - 3) modificarea parolelor de fiecare dată când sunt prezente indiciile eventualei compromiteri a sistemului ;
  - 4) alegerea parolelor calitative cu o mărime de minimum 8 simboluri, care nu sînt legate de informația cu caracter personal a utilizatorului, nu conțin simboluri identice consecutive și nu sînt compuse integral din grupuri de cifre sau litere;
  - 5) modificarea parolelor peste intervale de maximum 3 luni;
  - 6) dezactivarea procesului automatizat de înregistrare (cu folosirea parolelor salvate
27. Se utilizează autentificarea multifactorială, care include parole complexe, cu includerea simbolurilor, literelor, cifrelor în combinație complexă. În mod obligatoriu fiecare parolă conține una sau mai multe litere scrise cu majuscule (sa fie tot cu litera mare ). Parola nu va conține inițialele sau date care pot caracteriza o anumită persoană (data de naștere, adresa, poreclă,etc.)

## **VI. ADMINISTRAREA ACCESULUI UTILIZATORILOR**

### **Secțiunea 1**

28. Înainte de acordarea accesului în sistem, utilizatorii sunt informați despre faptul că folosirea sistemelor informaționale de date cu caracter personal este controlată și că folosirea neautorizată a acestora se urmărește în conformitate cu legislația.

### **Secțiunea 2**

29. **Drepturile de acces ale utilizatorilor** la sistemele informaționale de date cu caracter personal sînt revizuite cu regularitate pentru asigurarea faptului că nu au fost acordate drepturi de acces neautorizate (maximum peste fiecare șase luni) și după oricare schimbare de statut al utilizatorului.

### **Secțiunea 3**

30. **Repartizarea obligațiilor** subiecților care asigură funcționarea sistemelor informaționale de date cu caracter personal este efectuată prin intermediul investiției cu drepturi/competențe corespunzătoare de acces, prin ordinul USDC . Utilizatorii sistemelor informaționale de date cu caracter personal se investesc doar cu acele drepturi/competente, care sunt necesare pentru realizarea de către ei a obiectivelor stabilite .
31. Sesiunea de lucru în sistemul informațional, destinat prelucrării datelor cu caracter personal, se blochează (la solicitarea utilizatorului sau automat, după maximum 15 minute de perioadă inactivă a utilizatorului), fapt care face imposibil accesul de mai departe pînă în momentul când utilizatorul nu deblochează

#### **Secțiunea 4**

32. Toate metodele de acces de la distanță la sistemele informaționale de date cu caracter personal trebuie securizate (utilizându-se VPN, criptarea, cifrarea etc.), precum și sunt documentate, supuse monitorizării și controlului. Fiecare metodă de acces de la distanță la sistemele informaționale de date cu caracter personal se autorizează de persoanele responsabile ale deținătorilor de date cu caracter personal și este permisă doar utilizatorilor, cărora aceasta le este necesar pentru îndeplinirea obiectivelor stabilite.

#### **Secțiunea 5**

33. Accesul fără fir la sistemele informaționale de date cu caracter personal este documentat, supus monitorizării și controlului și este permis doar în cazul utilizării mijloacelor criptografice de protecție a informației. Folosirea tehnologiilor fără fir se autorizează de personalul IT al USDC.

#### **Secțiunea 6**

34. Se stabilesc limitări și se elaborează reguli de folosire a echipamentului portativ și mobil care permit accesul la sistemele informaționale de date cu caracter personal. Accesul la sistemele informaționale de date cu caracter personal cu folosirea echipamentului portativ și mobil se documentează, fiind monitorizat și controlat. Folosirea echipamentului portativ și mobil este autorizată de Serviciul Tehnologii Informaționale al USDC.

### **VII. PROTECȚIA SISTEMELOR INFORMAȚIONALE ȘI A COMUNICAȚIILOR ÎN CARE SUNT PRELUCRATE DATE CU CARACTER PERSONAL**

#### **Secțiunea 1**

35. Se asigură izolarea funcțiilor de securitate de funcțiile care nu se atribuie la securitatea sistemelor informaționale de date cu caracter personal.

Trebuie preîntâmpinate tentativele dezvăluirii neautorizate sau neintenționate a informației restante care conține date cu caracter personal, prin intermediul resurselor informaționale general accesibile .

#### **Secțiunea 2**

36. Se asigură protecția sistemelor informaționale de date cu caracter personal sau sunt limitate posibilitățile de realizare a atacurilor de diferite tipuri, inclusiv DOS (denial of service) - „refuz în serviciu”.
37. Se efectuează monitorizarea permanentă și controlul comunicațiilor la perimetrul exterior al sistemelor informaționale de date cu caracter personal, inclusiv la cele mai importante puncte de contact în interiorul perimetrului acestor sisteme informaționale. Amplasarea resurselor general accesibile se asigură în spațiile special destinate a rețelei de calcul cu interfețele fizice de rețea.  
Este asigurată imposibilitatea accesului din exterior al utilizatorilor la rețeaua internă în care se prelucrează date cu caracter personal.
38. Pentru toate categoriile sistemelor informaționale de date cu caracter personal se asigură confidențialitatea datelor cu caracter personal transmise, utilizându-se mijloace de protecție criptografică a informației.

### **VIII. AUDITUL SECURITĂȚII ÎN SISTEMELE INFORMAȚIONALE DE DATE CU CARACTER PERSONAL**

39. Responsabilul fiecărui sistem informațional este obligat să întocmească următoarele proceduri obligatorii de audit al sistemului :
- 1) Se efectuează înregistrarea tentativelor de intrare/ieșire a utilizatorului în sistem, conform următorilor parametri:
    - a) data și timpul tentativei intrării/ieșirii;
    - b) ID-ul utilizatorului;
    - c) rezultatul tentativei de intrare/ieșire – pozitivă sau negativă
  - 2) Este efectuată înregistrarea tentativelor de pornire/finisare a sesiunii de lucru a programelor aplicative și a proceselor, destinate prelucrării datelor cu caracter personal, înregistrarea modificărilor drepturilor de acces ale utilizatorilor și statutul obiectelor de acces conform următorilor parametri:
    - a) data și timpul tentativei de pornire;
    - b) denumirea/identificatorul programului aplicativ sau al procesului;
    - c) ID-ul utilizatorului;
    - d) rezultatul tentativei de pornire – pozitivă sau negativă.
  - 3) Se efectuează înregistrarea tentativelor de obținere a accesului (de executare a operațiunilor) pentru aplicații și procese destinate prelucrării datelor cu caracter personal, conform următorilor parametri:
    - a) data și timpul tentativei de obținere a accesului (executare a operațiunii);
    - b) denumirea (identificatorul) aplicației sau procesului;
    - c) ID-ul utilizatorului;
    - d) specificațiile resursei protejate (identificator, nume logic, nume fișier, număr etc.);
    - e) tipul operațiunii solicitate (citire, înregistrare, ștergere etc.);
    - f) rezultatul tentativei de obținere a accesului (executare a operațiunii) – pozitivă sau negativă

- 4) Este efectuată înregistrarea modificărilor drepturilor de acces ale utilizatorului și statutului obiectelor de acces, conform următorilor parametri :
- a) data și timpul modificării competențelor;
  - b) ID-ul administratorului care a efectuat modificările;
  - c) ID-ul utilizatorului și competențele acestuia sau specificarea obiectelor de acces și statutul nou al acestora.
- 5) Se efectuează înregistrarea ieșirii din sistem a informației care conține date cu caracter personal (documente electronice, date etc.), înregistrarea modificărilor drepturilor de acces ale subiecților și statutul obiectelor de acces, conform următorilor parametri :
- a) data și timpul eliberării;
  - b) denumirea informației și căile de acces la aceasta;
  - c) specificarea echipamentului (dispozitivului) care a eliberat informația (numele logic);
  - d) ID-ul utilizatorului, care a solicitat informația;
  - e) volumul documentului eliberat (numărul paginilor, a filelor, copiilor) și rezultatul eliberării.
40. În caz de deranjament al auditului securității în sistemele informaționale de date cu caracter personal sau completării întregului volum de memorie repartizat pentru păstrarea rezultatelor auditului, este informată persoana responsabilă de politica de securitate a datelor cu caracter personal și întreprinse măsuri în vederea restabilirii capacității de lucru a sistemului de audit.
41. Se efectuează monitorizarea permanentă și analiza înregistrărilor de audit a securității în sistemele informaționale de date cu caracter personal, în scopul depistării activităților neobișnuite sau suspecte de utilizare a acestor sisteme informaționale, cu întocmirea raportului referitor la cazurile depistării acestor activități, stocate în mijloacele electronice de calcul.
42. Rezultatele auditului securității în sistemele informaționale de date cu caracter personal, care reprezintă operațiuni de prelucrare a datelor cu caracter personal și mijloacele de efectuare a auditului, se protejează contra accesului neautorizat prin instituirea măsurilor de securitate adecvate, inclusiv prin asigurarea confidențialității și integrității acestora.
43. Durata stocării rezultatelor auditului securității în sistemele informaționale de date cu caracter personal se justifică în politica de securitate a datelor cu caracter personal, acest termen nu este mai mic de 2 ani, pentru a fi posibil folosirea acestora în calitate de probe în cazul incidentelor de securitate, unor eventuale investigații sau procese judiciare

## **IX. ASIGURAREA INTEGRITĂȚII INFORMAȚIEI CARE CONȚINE DATE CU CARACTER PERSONAL ȘI A TEHNOLOGIILOR INFORMAȚIONALE**

### **Secțiunea 1**

44. Se asigură identificarea, protocolarea și înlăturarea deficiențelor de soft-uri destinate prelucrării datelor cu caracter personal, inclusiv instalarea corecțiilor și pachetelor de reînnoire a acestor soft-uri.

### **Secțiunea 2**

45. Se utilizează tehnologii și mijloace de constatare a intruziunilor, care permit monitorizarea evenimentelor în sistemele informaționale de date cu caracter personal și constatarea atacurilor, inclusiv a altora care asigură identificarea tentativelor folosirii neautorizate a sistemelor informaționale.

### **Secțiunea 3**

46. Se asigură protecția și posibilitatea depistării modificării neautorizate a soft-urilor destinate prelucrării datelor cu caracter personal și a informației care conține date cu caracter personal.

### **Secțiunea 4**

47. Pentru toate categoriile sistemelor informaționale de date cu caracter personal se asigură testarea funcționării corecte a funcțiilor de securitate a sistemelor informaționale de date cu caracter personal (automat, la pornirea sistemului, și lunar, la solicitarea utilizatorului autorizat în acest scop).

## **X. COPIILE DE REZERVĂ ȘI RESTABILIREA INFORMAȚIEI CARE CONȚINE DATE CU CARACTER PERSONAL ȘI IT**

### **Secțiunea 1**

48. Reieșind din volumul prelucrărilor efectuate, individual, se stabilește de către deținătorul de date cu caracter personal intervalul de timp în care se execută copiile de siguranță a informațiilor care conțin date cu caracter personal și soft-urile folosite pentru prelucrarea automatizată a datelor cu caracter personal, dar în orice caz acest termen este mai mic de un an, care se păstrează în locuri protejate, în afara zonei de amplasare a acestei informații și soft-urile de bază.

Copiile de siguranță se testează în scopul verificării siguranței purtătorilor de informații și integrității informației care conține date cu caracter personal.

Procedurile de restabilire a copiilor de siguranță se actualizează și se testează cu regularitate, în scopul asigurării eficacității acestora.

## **XI. CONTROALELE DE SECURITATE A SISTEMELOR INFORMAȚIONALE DE DATE CU CARACTER PERSONAL**

### **Secțiunea 1**

- 49.** Deținătorii de date cu caracter personal verifică cu regularitate, cel puțin o dată pe an, îndeplinirea măsurilor tehnice și/sau organizaționale luate pentru detectarea unor disfuncționalități în ceea ce privește folosirea în procesul prelucrării datelor cu caracter personal asistemelor de telecomunicații și/sau efectuarea îmbunătățirilor, în caz de necesitate.
- 50.** Controalele de securitate sunt actualizate de fiecare dată când deținătorul de date cu caracter personal este reorganizat sau își schimbă infrastructura.

### **Secțiunea 2**

- 51.** În scopul verificării nivelului de protecție a sistemelor informaționale de date cu caracter personal, precum și în scopul prevențării unor eventuale cazuri de acces ilicit sau întâmplător asupra acestor sisteme informaționale, depistării locurilor slabe în mecanismele de protejare a acestora, Centrul întreprinde periodic controale de securitate, inclusiv cu efectuarea unor măsuri tehnice speciale pentru simularea unui model de accesare a sistemelor informaționale de date cu caracter personal.

### **Secțiunea 3**

- 52.** Rezultatele controalelor efectuate de Centru sunt puse imediat la dispoziția deținătorului de date cu caracter personal, nivelul de protecție a sistemelor informaționale de date cu caracter personal a căruia a servit obiect al controlului, cu prescrierea, în caz de necesitate, a acțiunilor necesare de a fi întreprinse în vederea asigurării securității prelucrării datelor cu caracter personal

