



SISTEMUL DE MANAGEMENT AL CALITĂȚII

MOLDCOOP
UNIVERSITATEA COOPERATIST-COMERCIALĂ DIN
MOLDOVA (UCCM)

Ediția: 1

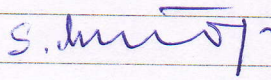
Revizia: 1

Data: 23.04.2015

Pagina 1 / 10

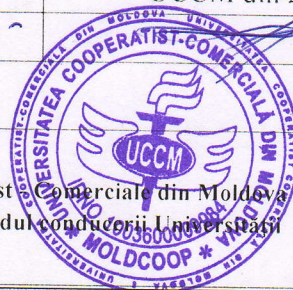
POLITICA DE SECURITATE

PRIVIND PROTECȚIA DATELOR CU CARACTER PERSONAL ȘI PRELUCRAREA ACESTORA ÎN CADRUL UNIVERSITĂȚII COOPERATIST-COMERCIALE DIN MOLDOVA

	ELABORAT	COORDONAT și VERIFICAT	APROBAT
Responsabil	Pavel PAVALACHI, Șef CTIC	Simion MUSTEATĂ Prorector	Larisa ȘAVGA Rector UCCM
Data	7.04.2015	7.04.2015	Proces-verbal nr. 7 al Senatului UCCM din 23.04.2015
Semnătura			



Prezenta politică este proprietatea Universității Cooperatist-Comerciale din Moldova.
Este interzisă multiplicarea și difuzarea acesteia fără acordul conducerii Universității.





I. DISPOZIȚII GENERALE

Prezenta Politică de securitate privind protecția datelor cu caracter personal și prelucrarea acestora în cadrul UCCM este elaborată în conformitate cu prevederile Legii nr. 133 din 08.07.2011 privind protecția datelor cu caracter personal și reglementează modul de colectare și utilizare acestor date, precum și condițiile de utilizare a informației în cadrul UCCM.

Reglementările prezentei Politici reprezintă un standard minim pentru UCCM, inclusiv toți angajații UCCM. Pornind de la această reglementare, toți angajații UCCM urmează să respecte strict prevederile Politicii și regulilor interne ale UCCM privind protecția datelor cu caracter personal și sistemelor IT.

II. OBIECTIVE MAJORE

Politica de securitate are ca scop primordial asigurarea integrității, disponibilității și confidențialității informației.

Integritatea se referă la măsurile și procedurile utilizate pentru protecția datelor împotriva modificărilor sau distrugerii neautorizate.

Disponibilitatea se asigură prin funcționarea continuă a tuturor componentelor sistemului informațional (SI). Diverse aplicații au nevoie de nivele diferite de disponibilitate în funcție de impactul sau daunele produse ca urmare a nefuncționării corespunzătoare a SI.

Confidențialitatea se referă la protecția datelor împotriva accesului neautorizat. Utilizatorul răspunde personal de asigurarea confidențialității datelor încredințate prin procedurile de acces la SI.

Prezenta Politică de securitate are ca scop, de asemenea, stabilirea cadrului normativ necesar pentru elaborarea regulamentelor și procedurilor de securitate în cadrul UCCM. Acestea sînt obligatorii pentru toți utilizatorii SI.

III. PRINCIPIILE PRELUCRĂRII DATELOR CU CARACTER PERSONAL

1. Datele cu caracter personal sunt prelucrate cu buna-credință și în conformitate cu dispozițiile legale în vigoare.
2. Datele cu caracter personal sunt colectate numai în scopuri determinate, explicite și legitime, iar prelucrarea ulterioară nu va fi incompatibilă cu aceste scopuri.
3. Datele cu caracter personal care fac obiectul prelucrării sunt adecvate, pertinente și neexcesive prin raportare la scopul în care sunt colectate.
4. Datele cu caracter personal care fac obiectul prelucrării sunt exacte și, dacă este cazul, actualizate.
5. Datele cu caracter personal nu se stochează pentru o perioadă mai lungă decît este necesar pentru realizarea scopurilor în care au fost colectate.
6. Datele cu caracter personal se prelucrează în conformitate cu drepturile persoanei vizate prevăzute de Legea privind protecția datelor cu caracter personal Nr. 133 din 8 iulie 2011.
7. Asigurarea și păstrarea confidențialității datelor cu caracter personal se efectuează în conformitate cu prevederile legislației în vigoare și ale părților semnatare în contracte.
8. Datele inexacte sau incomplete din punct de vedere al scopului în care sunt colectate și pentru care vor fi prelucrate vor fi șterse sau rectificate.
9. Asigurarea măsurilor tehnice și organizatorice (procedurale) adecvate pentru protejarea datelor cu caracter personal împotriva distrugerii accidentale sau ilegale, pierderii, modificării, dezvăluirii sau accesului neautorizat.

	SISTEMUL DE MANAGEMENT AL CALITĂȚII	Ediția: 1
		Revizia: 1
	MOLDCOOP UNIVERSITATEA COOPERATIST-COMERCIALĂ DIN MOLDOVA (UCCM)	Data: 23.04.2015
		Pagina 3 / 10

IV. METODE DE PROTECȚIE A DATELOR CU CARACTER PERSONAL

Protecția datelor cu caracter personal prelucrate în sistemele informaționale se efectuează prin următoarele metode:

- preîntâmpinarea conexiunilor neautorizate la rețelele telecomunicaționale și interceptării cu ajutorul mijloacelor tehnice a datelor cu caracter personal transmise prin aceste rețele;
- excluderea accesului neautorizat la datele cu caracter personal prelucrate;
- preîntâmpinarea acțiunilor speciale tehnice și de program, care condiționează distrugerea, modificarea datelor cu caracter personal sau defecțiuni în lucrul complexului tehnic și de program,
- preîntâmpinarea acțiunilor intenționate și/sau neintenționate a utilizatorilor interni și/sau externi, precum și a altor membri ai operatorului/persoanelor împuternicite de către operator, care condiționează distrugerea, modificarea datelor cu caracter personal sau defecțiuni în lucrul complexului tehnic și de program,
- preîntâmpinarea scurgerii de informații care conțin date cu caracter personal, transmise prin canalele de legătură, este asigurată prin folosirea metodelor de cifrare a acestei informații, precum și utilizarea canalelor VPN,
- preîntâmpinarea distrugerii, modificării datelor cu caracter personal sau defecțiunilor în funcționarea soft-ului destinat prelucrării datelor cu caracter personal este asigurată prin metoda folosirii mijloacelor de protecție speciale tehnice și de program, inclusiv a programelor licențiate, programelor antivirus, organizării sistemului de control al securității soft-ului și efectuarea periodică a copiilor de siguranță,
- preîntâmpinarea scurgerii de informații care conțin date cu caracter personal, este asigurată prin auditul intern al sistemelor informaționale, care se efectuează permanent.
- stabilirea exactă a ordinii de acces la informația care conține date cu caracter personal, prelucrate în cadrul sistemelor informaționale și de evidență instituite atât pentru utilizatorii interni cât și pentru cei externi.

V. PROCEDURI ORGANIZATORICE ȘI TEHNICE CARE URMEAZĂ A FI RESPECTATE ÎN CADRUL UCCM LA PRELUCRAREA DATELOR CU CARACTER PERSONAL

1. Proceduri generale de administrare a securității informaționale

- a) În cazul neutilizării temporare a purtătorilor de informație pe suport de hârtie sau electronici (digitali) care conțin date cu caracter personal, aceștia se păstrează în safeuri sau dulapuri metalice care se încuie.
- b) Computerele, terminalele de acces și imprimantele sînt deconectate la terminarea sesiunilor de lucru.
- c) Este asigurată securitatea punctelor de primire/expediere a corespondenței, precum și securitatea contra accesului neautorizat la aparatele fax și de copiere.
- d) Este asigurată securitatea și accesul fizic la mijloacele de reprezentare a informației care conține date cu caracter personal, în scopul împiedicării vizualizării acesteia de către persoane neautorizate.



Prezenta politică este proprietatea Universității Cooperatist - Comerciale din Moldova
Este interzisă multiplicarea și difuzarea acesteia fără acordul conducerii Universității





UCCM

SISTEMUL DE MANAGEMENT AL CALITĂȚII

MOLDCOOP
UNIVERSITATEA COOPERATIST-COMERCIALĂ DIN
MOLDOVA (UCCM)

Ediția: 1

Revizia: 1

Data: 23.04.2015

Pagina 4 / 10

e) Mijloacele de prelucrare a datelor cu caracter personal, informația care conține date cu caracter personal sau soft-urile destinate prelucrării datelor cu caracter personal sînt scoase din perimetrul de securitate doar în temeiul unei permisiuni scrise a conducerii.

2. Securitatea mediului fizic și a tehnologiilor informaționale folosite în procesul prelucrării datelor cu caracter personal

- a) Accesul în sediile/oficiile/birourile ori spațiile unde sînt amplasate sistemele informaționale de date cu caracter personal este restricționat, fiind permis doar persoanelor care au autorizația necesară, conform listei autorizate de conducerea UCCM.
- b) Se asigură administrarea și monitorizarea accesului fizic în toate punctele de acces la sistemele informaționale de date cu caracter personal.
- c) Perimetrul de securitate al UCCM reprezintă spațiile oficiilor în care se prelucrează/stochează date cu caracter personal.
- d) Perimetrul clădirii sau încăperilor în care sînt amplasate mijloacele de prelucrare a datelor cu caracter personal este integru din punct de vedere fizic, pereții exteriori ai încăperilor sînt rezistenți, intrările sunt echipate cu lacăte și semnalizare.
- e) Amplasarea mijloacelor de prelucrare a datelor cu caracter personal corespunde necesității asigurării securității acestora contra accesului nesancționat, furturilor, incendiilor, inundațiilor și altor posibile riscuri.
- f) Ușile și ferestrele se încuie în cazul în care în încăpere lipsesc membrii.
- g) Computerele, serverele, alte terminale de acces sunt amplasate în locuri cu acces limitat pentru persoane străine.
- h) Accesul cu utilaje foto/video neautorizate este interzis în perimetrul de securitate a clădirii UCCM unde se prelucrează/stochează date cu caracter personal, ținînd cont de necesitatea asigurării regimului de confidențialitate și securitate a prelucrării datelor cu caracter personal, prevăzut de art.29 și art. 30 ale Legii privind protecția datelor cu caracter personal, precum și pct. 26 din Cerințe.
- i) 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 UCCM.

3. Identificarea și autentificarea utilizatorilor

- a) Este efectuată identificarea și autentificarea utilizatorilor sistemelor informaționale de date cu caracter personal și a proceselor executate în numele acestor utilizatori.
- b) Toți utilizatorii (inclusiv personalul care asigură susținerea tehnică, administratorii de rețea, personalul CTIC) au un identificator personal (ID-ul utilizatorului), care nu conține semnalmentele nivelului de accesibilitate al utilizatorului.
- c) Pentru confirmarea ID-ului utilizatorului sînt utilizate parole.
- d) 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 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 sau se suspendă de către CTIC din cadrul UCCM.



Prezenta politică este proprietatea Universității Cooperatist - Comerciale din Moldova
Este interzisă multiplicarea și difuzarea acesteia fără acordul conducerii Universității



	SISTEMUL DE MANAGEMENT AL CALITĂȚII	Ediția: 1
		Revizia: 1
	MOLDCOOP UNIVERSITATEA COOPERATIST-COMERCIALĂ DIN MOLDOVA (UCCM)	Data: 23.04.2015
		Pagina 5 / 10

4. Identificarea și autentificarea echipamentului

Echipamentele tehnice, inclusiv cele folosite în operațiunile de prelucrare a datelor cu caracter personal sînt identificate și autentificate prin număr de inventariere.

5. Administrarea identificatorilor utilizatorilor include

- identificarea univocă a fiecărui utilizator,
- verificarea autenticității fiecărui utilizator.

6. Utilizarea parolelor în procesul asigurării securității informaționale

Sunt respectate regulile de asigurare a securității informaționale în cazul alegerii și folosirii parolelor care includ:

- păstrarea confidențialității parolelor;
- interzicerea înscrierii parolelor pe suport de hîrtie, în cazul în care nu se asigură securitatea păstrării acestuia;
- modificarea parolelor de fiecare dată cînd sînt prezente indiciile eventualei compromiteri a sistemului sau parolei;
- alegerea parolelor calitative cu o mărime de minimum 5-8 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;
- dezactivarea procesului automatizat de înregistrare (cu folosirea parolelor salvate).

7. Controlul administrării accesului

Controlul sistematic al acțiunilor utilizatorilor în vederea evaluării corectitudinii și conformării operațiunilor și acțiunilor efectuate prin intermediul sistemelor informaționale de date cu caracter personal este efectuat de către personalul CTIC.

8. Accesul de la distanță

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

9. Securitatea electroenergetică

- Echipamentul electric utilizat pentru menținerea funcționalității sistemelor informaționale de date cu caracter personal, a cablurilor electrice, este asigurat contra deteriorărilor și conectărilor nesancționate, prin montarea lor în nișe speciale.



Prezenta politică este proprietatea Universității Cooperatist - Comerciale din Moldova
Este interzisă multiplicarea și difuzarea acesteia fără acordul conducerii Universității



 UCCM	SISTEMUL DE MANAGEMENT AL CALITĂȚII	Ediția: 1
		Revizia: 1
	MOLDCOOP UNIVERSITATEA COOPERATIST-COMERCIALĂ DIN MOLDOVA (UCCM)	Data: 23.04.2015
		Pagina 6 / 10

- b) În cazul apariției situațiilor excepționale, de avarie sau de forță majoră, este asigurată posibilitatea deconectării electricității la sistemele informaționale de date cu caracter personal, inclusiv posibilitatea deconectării oricărui component TI.

10. Controlul instalării și scoaterii componentelor T.I.

- a) Controlul și evidența instalării și scoaterii mijloacelor de program, mijloacelor tehnice și celor tehnice de program, utilizate în cadrul sistemelor informaționale de date cu caracter personal este exercitat de către CTIC.
- b) La expirarea perioadei de valabilitate, informațiile, care conțin date cu caracter personal și care se conțin pe purtătorii de informații, se distrug fizic sau se transcriu și se nimicesc prin metode sigure, evitându-se folosirea funcțiilor standarde de nimicire.

11. Dezvăluirea datelor cu caracter personal

- a) Fiecare caz de solicitare a dezvăluirii prin transmitere a datelor cu caracter personal pe cale electronică va fi examinat separat, reieșind din posibilitățile tehnice asigurate de destinatar și operator, precum și în corespundere cu măsurile organizatorice și tehnice implementate de părți. În cazul în care rețelele comunicaționale prezintă riscuri pentru confidențialitatea și securitatea datelor cu caracter personal, vor fi utilizate metode tradiționale de transmitere (*expediere poștală cu aviz recomandat, înmînarea personală, etc.*).
- b) Este interzisă dezvăluirea prin transmitere a datelor cu caracter personal prin rețele comunicaționale ce nu corespund Cerințelor (*spre exemplu: expedierea informației prin intermediul e-mail-urilor personale de tipul @gmail.com, @mail.ru, @yahoo.com, etc.*).
- c) Volumul și categoriile datelor cu caracter personal colectate în scopul ținerii evidenței UCCM, este limitat la strictul necesar pentru realizarea scopurilor declarate.
- d) Acces la sistemele informaționale gestionate în cadrul UCCM, din partea Procuraturii Generale (*după caz procuraturile teritoriale/specializate*), Ministerului Afacerilor Interne, Centrului Național Anticorupție etc., va fi permis doar în cazul în care solicitarea va corespunde prevederilor art. 15 și art. 212 Cod de procedură penală.

12. Drepturile subiecților de date cu caracter personal

- a) În cazul în care datele cu caracter personal sînt colectate direct de la subiectul acestor date, în conformitate cu prevederile art.12 al Legii privind protecția datelor cu caracter personal, persoanei necesită a-i fi furnizate următoarele informații, exceptînd cazul în care el deține deja informațiile respective:
- privind identitatea operatorului sau, după caz, a persoanei împuternicite de către operator (*denumirea, adresa juridică, IDNO-ul, numărul de înregistrare în Registrul de evidență al operatorilor de date cu caracter personal*);
 - privind scopul concret al prelucrării datelor cu caracter personal colectate;
 - privind destinatarii sau categoriile de destinatari ai datelor cu caracter personal;
 - existența drepturilor la informare și de acces la datele colectate; de intervenție asupra datelor (*în special de a rectifica, actualiza, bloca sau șterge datele cu caracter personal a căror prelucrare contravine legii datorită caracterului incomplet sau inexact al acestora*) și de opoziție, precum și condițiile în care aceste drepturi pot fi exercitate;



Prezenta politică este proprietatea Universității Cooperatist - Comerciale din Moldova
Este interzisă multiplicarea și difuzarea acesteia fără acordul conducerii Universității



 UCCM	SISTEMUL DE MANAGEMENT AL CALITĂȚII	Ediția: 1
		Revizia: 1
	MOLDCOOP UNIVERSITATEA COOPERATIST-COMERCIALĂ DIN MOLDOVA (UCCM)	Data: 23.04.2015
		Pagina 7 / 10

- b) Subiecților de date cu caracter personal le este asigurat dreptul de acces și posibilitatea de a lua cunoștință cu actele întocmite în scopul verificării corectitudinii întocmirii lor, contestării împotriva neincluserii sau includerii incorecte a unor date, precum și împotriva altor erori comise la înscrierea datelor despre sine.
- c) Dreptul de informare este asigurat de către operatorul datelor cu caracter personal (*sau entitățile ce asigură mentenanța sistemului și sau prestează servicii externalizate ale operatorului*) tuturor persoanelor supuse prelucrării.
- d) În cazul realizării de către subiectul de date cu caracter personal a dreptului de intervenție, datele inexacte vor fi actualizate prin rectificare sau ștergere, ca bază servind doar surse legale (*acte de identitate, de stare civilă, resurse informaționale principale de stat etc.*), modificarea urmînd a fi efectuată în toate sistemele informaționale și de evidență gestionate.

13. Stocarea, păstrarea și distrugerea datelor cu caracter personal prelucrate

- a) Accesul în spațiile/perimetrul unde sînt amplasate sistemele informaționale și de evidență a datelor cu caracter personal este restricționat, fiind permis doar persoanelor care au autorizația necesară conform politicii de securitate respective, ordinului și alte acte aprobate de conducerea UCCM cu privire la reglementarea protecției datelor cu caracter personal.
- b) Este interzisă stocarea și păstrarea formatului electronic al datelor cu caracter personal în computere care sînt conectate la internet și nu sînt echipate cu mijloace de protecție speciale tehnice și de program, precum și nu au instalate programe antivirus licențiate, sisteme de control al securității soft-ului.
- c) Este interzisă introducerea în perimetrul de securitate instituțional și utilizarea calculatoarelor personale ori a purtătorilor de informații în scopuri de serviciu. Mai mult, accesul la computerele din dotare sunt protejate/restricționate prin crearea profilurilor de utilizatori, iar drepturile de administrator sînt încredințate doar persoanelor din cadrul CTIC.
- d) Stocarea datelor cu caracter personal pe suport magnetic, optic, laser, de hîrtie sau alt suport al informației, pe care se creează, se fixează, se transmite, se recepționează, se păstrează sau, în alt mod, se utilizează documentul și care permite reproducerea acestuia, este asigurată prin plasarea acestora în safeuri sau dulapuri care se încuie. Scoaterea, fără autorizare, a purtătorilor de date cu caracter personal din perimetrul de securitate al operatorului este interzisă.

14. Auditul sistemelor informaționale gestionate

- a) Înregistrarea tentativelor de intrare/ieșire a utilizatorului în sistem, conform următorilor parametri se efectuează astfel:
- data și timpul tentativei intrării/ieșirii;
 - ID-ul utilizatorului;
 - rezultatul tentativei de intrare/ieșire - pozitivă sau negativă.
- b) Înregistrarea tentativelor de obținere a accesului (de executare a operațiunilor) pentru aplicații și procese destinate prelucrării datelor cu caracter personal, se efectuează conform următorilor parametri:
- data și timpul tentativei de obținere a accesului (executate a operațiunii),
 - denumirea (identificatorul) aplicației sau procesului, ID-ul utilizatorului,
 - specificațiile resursei protejate (identificator, nume logic, nume fișier, număr etc.),
 - tipul operațiunii solicitate (citire, înregistrare, ștergere etc.),



Prezenta politică este proprietatea Universității Cooperatist - Comerciale din Moldova
Este interzisă multiplicarea și difuzarea acesteia fără acordul conducerii Universității



	SISTEMUL DE MANAGEMENT AL CALITĂȚII	Ediția: 1
		Revizia: 1
	MOLDCOOP UNIVERSITATEA COOPERATIST-COMERCIALĂ DIN MOLDOVA (UCCM)	Data: 23.04.2015
		Pagina 8 / 10

-rezultatul tentativei de obținere a accesului (executare a operațiunii) – pozitivă sau negativă.

c) Înregistrarea modificărilor drepturilor de acces (competențelor) utilizatorului și statutului obiectelor de acces, este efectuată conform următorilor parametri:

- data și timpul modificării competențelor,
- ID-ul administratorului care a efectuat modificările,
- ID-ul utilizatorului și competențele acestuia sau specificarea obiectelor de acces și statutul nou al acestora.

d) 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, se efectuează conform următorilor parametri:

- data și timpul eliberării;
- denumirea informației și căile de acces la aceasta;
- specificarea echipamentului (dispozitivului) care a eliberat informația (numele logic);
- ID-ul utilizatorului, care a solicitat informația.

15. Asigurarea protecției contra programelor dăunătoare (virusurilor)

Protecția contra infiltrării programelor dăunătoare în soft-urile destinate prelucrării datelor cu caracter personal este asigurată prin existența programelor licențiate anti-virus.

16. Testarea posibilităților funcționale de asigurare a securității sistemelor informaționale de date cu caracter personal

Testarea funcționării corecte a funcțiilor de securitate a sistemelor informaționale de date cu caracter personal se asigură de către personalul CTIC.

17. Gestionarea incidentelor de securitate

- a) Personalul care asigură exploatarea sistemelor informaționale de date cu caracter personal trece, minimum o dată în an, instruirea referitor la responsabilitățile și obligațiile în cazul executării acțiunilor de gestionare și reacționare la incidentele de securitate.
- b) Personalul UCCM informează neîntârziat conducerea despre incidentele privind securitatea sistemelor informaționale de date cu caracter personal.
- c) Prelucrarea incidentelor include depistarea, analiza, preîntâmpinarea dezvoltării, înlăturarea lor și restabilirea securității.
- d) Până la 31 ianuarie a fiecărui an, UCCM va informa în scris Autoritatea națională pentru protecția datelor cu caracter personal despre incidentele de securitate constatate.

18. Marcarea documentelor

Toată informația care se intenționează a fi dezvăluită, și care conține date cu caracter personal, urmează a fi marcată prin includerea numărului de înregistrare din Registrul de evidență al operatorilor de date cu caracter personal.

	Prezenta politică este proprietatea Universității Cooperatist - Comerciale din Moldova Este interzisă multiplicarea și difuzarea acesteia fără acordul conducerii Universității	
---	--	---

 UCCM	SISTEMUL DE MANAGEMENT AL CALITĂȚII	Ediția: 1
		Revizia: 1
	MOLDCOOP UNIVERSITATEA COOPERATIST-COMERCIALĂ DIN MOLDOVA (UCCM)	Data: 23.04.2015
		Pagina 9 / 10

19. Responsabilitatea pentru asigurarea securității datelor cu caracter personal precum și a informațiilor cu accesibilitate limitată

Operatorul de date cu caracter personal, persoana împuternicită de către operator, persoanele terțe după caz, semnatarii a anexei nr. 1, pentru nerespectarea dispozițiilor prezentei Politici de securitate - poartă răspundere civilă (Codul civil), contravențională (art. 74¹ Cod contravențional) și penală (art.art. 177, 178, 180 Cod penal).

VI. MIJLOACE DE PROTECȚIE A DATELOR CU CARACTER PERSONAL

Protecția datelor cu caracter personal în cadrul UCCM este asigurată printr-un complex de măsuri tehnice și organizatorice de preîntâmpinare a prelucrării ilicite a datelor cu caracter personal.

Sînt supuse protecției prin mijloace/procedee specifice, toate resursele informaționale ale operatorului de date cu caracter personal gestionate, care conțin date cu caracter personal, păstrate:

- pe suporturi magnetice, optice, laser sau alte suporturi ale informației electronice, masive informaționale și baze de date;
- în sistemele informaționale, rețelele, sistemele operaționale, sistemele de gestionare a bazelor de date și alte aplicații, sistemele de telecomunicații, inclusiv mijloacele de confecționare și multiplicare a documentelor și alte mijloace tehnice de prelucrare a informației.

V. Pășe

[Signature]



Prezenta politică este proprietatea Universității Cooperatist - Comerciale din Moldova
Este interzisă multiplicarea și difuzarea acesteia fără acordul conducerii Universității



 UCCM	SISTEMUL DE MANAGEMENT AL CALITĂȚII	Ediția: 1
		Revizia: 1
	MOLDCOOP UNIVERSITATEA COOPERATIST-COMERCIALĂ DIN MOLDOVA (UCCM)	Data: 23.04.2015
		Pagina 10 / 10

ANEXA 1

Subsemnat (ul/a), _____ ,
născut (ă) la data de _____ ,
cu domiciliul în _____ ,
angajat (ă) al(a) _____ ,
în funcția de _____ ,

declar pe propria răspundere că am luat cunoștință de prevederile legale referitoare la protecția datelor cu caracter personal și consimt să păstrez confidențialitatea datelor cu caracter personal a căror prelucrare o efectuez în condițiile legii, în virtutea atribuțiilor de serviciu, inclusiv și după încetarea activităților de prelucrare a acestor date.

Cunosc faptul că încălcarea normelor legale privind protecția datelor cu caracter personal atrage răspundere administrativă, disciplinară, materială, civilă ori penală, în raport cu gravitatea faptei, potrivit legii.

Data _____

Numele, Prenumele, Patronimicul _____

Semnătura _____



Prezenta politică este proprietatea Universității Cooperatist - Comerciale din Moldova
Este interzisă multiplicarea și difuzarea acesteia fără acordul conducerii Universității

