APROBAT
Senatul Universității de Stat din Tiraspol
din 28.11.17

POLITICA
de asigurare a securității datelor cu caracter personal prelucrate de către Universitatea de Stat din Tiraspol (cu sediul la Chișinău)

I. Dispoziţiile generale

1. În vederea realizării prevederilor Legii nr.133 din 8 iulie 2011 privind protecţia datelor cu caracter personal şi în conformitate cu Hotărârea Guvernului nr.1123 din 14 decembrie 2010 „Privind aprobarea Cerinţelor faţă de asigurarea securităţii datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaţionale de date cu caracter personal", Universitatea de Stat din Tiraspol (în continuare UST), reieşind din necesitatea asigurării securităţii patrimoniului instituției, a elaborat şi organizează implementarea prevederilor documentului respectiv, care stabileşte **Politica de securitate a datelor cu caracter personal prelucrate de către UST**.

2. Prezentul Regulament se revizuieşte cel puţin o dată în an şi, după caz, amendamentele vor fi aprobate prin ordin al Rectorului Universității.

3. Pentru ca politica de securitate a datelor cu caracter personal să fie cunoscută tuturor, acest document este adus la cunoştinţă utilizatorilor şi altor angajaţi ai UST, în limitele competenţelor funcţionale şi nivelului de acces acordat.

4. În sensul prezentului document, UST are calitatea de ***OPERATOR***, iar persoanele care vor monitoriza sau vor avea acces la date au calitatea de ***PERSOANĂ ÎMPUTERNICITĂ DE OPERATOR***.

5. Prin ordin al Rectorului UST se desemnează o persoană, denumită ***ADMINISTRATOR***, responsabilă de elaborarea, implementarea şi monitorizarea respectării prevederilor politicii de securitate a datelor cu caracter personal, care nu va avea atribuţii/sarcini/responsabilităţi incompatibile cu sarcinile funcţiei de implementare a politicii.

6. Administratorul va dispune de resurse suficiente (timp, resurse umane, echipament şi buget) şi va avea acces liber la informaţia necesară pentru îndeplinirea funcţiilor sale în măsura în care aceasta nu operează în afara cadrului acestei politici. Acesta asigură definirea clară a diferitelor responsabilităţi cu privire la securitatea prelucrării datelor cu caracter personal (prevenire, supraveghere, detectare şi

prelucrare), precum şi operarea cu ele, în afara presiunilor ca rezultat al intereselor personale sau alte împrejurări.

II. Scopul

7. Prezentul Regulament stabileşte măsurile de asigurare a securităţii datelor cu caracter personal prelucrate de către operator.

8. Scopul documentului este descrierea politicii de securitate privind protecția datelor cu caracter personal dar și a patrimoniului instituției precum și protecția altor drepturi fundamentale şi interese legitime ale studenților, cursanților și angajaților UST.

III. Categorii de date cu caracter personal

9. În contextul prezentei politici, datele cu caracter personal pot fi clasificate după următoarele categorii:

- Date personale pe **suport fizic** (hârtie) – informațiile din cadrul serviciului personal privind activitatea cadrelor didactice, studenților și cursanților UST colectate și stocate de persoanele responsabile în procesul activității profesionale.
- Date personale în format **text digital** – date cu caracter personal, stocate cu acordul proprietarului pe suporturi digitale în cadrul sistemelor informaționale instituționale
- Date personale în format **video digital** – date cu caracter personal în format video preluate și stocate de pe sistemele de supraveghere video din cadrul Instituției

10. Modul de protecție și utilizare a fiecărei categorii de date este stabilit de actul reglementar respectiv, aprobat de Senatul UST.

IV. Asigurarea securității datelor cu caracter personal

11. Procedurile de asigurare a securității pentru fiecare categorie a datelor cu caracter personal sunt stabilite prezentul act privind asigurarea securității datelor, aprobate de Senatul UST.

12. securitatea datelor pe suport fizic (documente tipărite) va fi asigurată prin:

a) Spațiu (încăpere) special amenajat, cu acces restricționat doar pentru personalul autorizat; în cazul amplasării încăperii la parter şi/sau la ultimul etaj al clădirii, precum şi în cazul existenţei balcoanelor, scărilor antiincendiare, ferestrele încăperilor respective trebuie să aibă gratii.

b) Instalații și echipamente pentru protecția fizică a informației în caz de calamități naturale sau accidente tehnogene;
c) Accesul permis doar pentru personal instruit, care a semnat prealabil acordul de confidențialitate (Anexa 1).

13. securitatea datelor pe suport digital (baze de date etc.) va fi asigurată prin:

a) Spațiu (încăpere) special amenajat, cu acces restricționat doar pentru personalul autorizat; În cazul amplasării încăperii la parter şi/sau la ultimul etaj al clădirii, precum şi în cazul existenţei balcoanelor, scărilor antiincendiare, ferestrele încăperilor respective trebuie să aibă gratii.
b) Purtători de informaţii şi mijloace de stocare şi prelucrare a înregistrărilor video sub control permanent şi cu acces doar pentru personalul autorizat.
c) Sisteme informatice cu acces restricționat în funcție de rolul utilizatorului concret în sistem.
d) Canale de comunicație protejate, separate de rețeaua utilitară pentru transfer date.
e) Accesul permis doar pentru personal instruit, care a semnat prealabil acordul de confidențialitate (Anexa 1)

V. Stocarea datelor cu caracter personal

14. Perioada de stocare pentru fiecare categorie de date cu caracter personal este stabilit de actul normativ respectiv, aprobat de Senatul UST, ținând cont de prevederile actelor normative și legislative pentru această categorie de date.

15. Pentru perioada de stocare datele în format digital vor fi stocate concomitent pe două suporturi digitale, copia de siguranță fiind păstrată separat, în spații securizate.

16. Lichidarea datelor după expirarea perioadei de stocare este realizată automat pentru datele pe suport digital și cu confirmare prin act de lichidare pentru datele pe suport fizic.

VI. Controlul accesului și auditul securității datelor cu caracter personal

17. Orice operație de acces la datele cu caracter personal este înregistrată în Registrul de monitorizare, conform următorilor parametri:

a) data şi timpul tentativei intrării/ieşirii;
b) ID-ul utilizatorului;
c) descrierea operației efectuate.

18. Orice operație de acces la sistemele digitale informatice care gestionează datele cu caracter personal este înregistrată în Registrul de monitorizare, conform următorilor parametri:

a) data şi timpul tentativei intrării/ieşirii;
b) ID-ul utilizatorului;
c) descrierea operației efectuate.

19. Orice operație de eliberare a datelor cu caracter personal este înregistrată în Registrul de monitorizare, conform următorilor parametri:
a) data şi timpul tentativei intrării/ieşirii;
b) documentul în baza căruia au fost eliberate datele;
c) instituția căreia i-au fost transmise datele;
c) condițiile de eliberare a datelor.

ANEXA nr.1
la Politica de asigurare a securităţii datelor cu caracter personal
prelucrate de către Universitatea de Stat Tiraspol

ANGAJAMENT

Subsemnatul/a _____, angajat/ă în cadrul _____, în funcţia de _____, în conformitate cu prevederile Legii nr.133 din 8 iulie 2011 privind protecţia datelor cu caracter personal şi a Hotărîrii Guvernului nr.1123 din 14 decembrie 2010 „Privind aprobarea Cerinţelor faţă de asigurarea securităţii datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaţionale de date cu caracter personal", mă oblig să respect drepturile şi libertăţile fundamentale ale persoanelor cu privire la prelucrarea, confidenţialitatea şi securitatea datelor şi imaginilor cu caracter personal.

Data _____ Semnătura _____