APROB
Rector UnAŞM
Maria Duca
23 06 2015

REGULAMENTUL

privind supravegherea prin mijloace video şi asigurarea securităţii informaţiilor ce conţin date cu caracter personal din cadrul Universităţii Academiie de Ştiinţe a Moldovei

1.Dispoziţii generale

În contextul actual securitatea obiectivelor nu poate fi asigurată fără o supraveghere video eficientă, care să permită, atât monitorizarea în timp real a evenimentelor şi persoanelor suspecte, cât şi înregistrarea imaginilor video.

Aceste sisteme de supraveghere video se adresează, în principal spaţiilor în care se desfăşoară activităţi de vînzare, spaţii comerciale, dar şi birourilor de acces public.

Totodată utilizarea unui astfel de sistem include anumite responsabilităţi şi garanţii din partea proprietarului de sistem, referitor la prelucrarea şi protecţia datelor cu caracter personal ce se înregistrează în sistem, atribuţii şi reglementări descrise în legea nr. 133 din 18.07.2011 privind protecţia datelor cu caracter personal.

Din acest motiv este necesară stabilirea unui regulament de securitate privind supravegherea prin mijloace video şi prelucrarea datelor cu caracter personal preluate şi înregistrate în sistemul de monitorizare prin înregistrare video.

2. Scopul supravegherii prin mijloace video din cadrul UnAŞM

2.1 Stabilirea unui set unitar de reguli care reglementează implementarea şi utilizarea sistemului de supraveghere video, are scopul asigurării securităţii persoanelor şi bunurilor, pazei şi protecţiei bunurilor, imobilelor, valorilor şi a materialelor cu regim special, respectând în acelaşi timp obligaţiile ce revin UnAŞM , în calitate de operator de date, conform Legii nr. 133 din 18.07.2011 şi măsurile de securitate adoptate pentru protecţia datelor cu caracter personal, protejarea vieţii private, a intereselor legitime şi garantarea drepturilor fundamentale ale persoanelor vizate.

2.2 Stabilirea responsabilităţilor privind administrarea şi exploatarea sistemului de supraveghere prin mijloace video, precum şi cele privind întocmirea, avizarea şi aprobarea documentelor aferente acestor activităţi.

2.3 Scopul utilizării sistemului video este de a asigura buna administrare şi funcţionare a UnAŞM, în special în vederea controlului de securitate şi pază. De asemenea, sistemul video este necesar pentru a sprijini politicile de securitate instituite de actele normative care reglementează protecţia datelor cu caracter personal şi contribuie la îndeplinirea atribuţiilor structurii de securitate.

2.4 Prezentul Regulamentul descrie măsurile care necesită a fi luate de UnAŞM pentru a proteja datele cu caracter personal care sunt prelucrate prin metoda supravegherii video, a vieţii private şi alte drepturi fundamentale şi interese legitime ale subiecţilor.

3. Zonele supravegheate

3.1 Camerele de supraveghere video sunt amplasate în locuri vizibile. Orice utilizare ascunsă a acestora este strict interzisă, cu excepţia cazurilor reglementate de legislaţie.

3.2.1 Camerele de supraveghere video sunt amplasate conform anexei nr. 1 al prezentului Regulament.

3.3 Nu sânt monitorizate zonele în care persoanele pot conta, în mod rezonabil, pe intimitate, precum birourile de serviciu şi toaletele.

4.Datele cu caracter personal colectate prin intermediul sistemului de supraveghere video

4.1 Sistemul de supraveghere video este dotat cu detector de mişcare. Toate camerele funcţionează în regim 24/24 ore şi sunt fixate.

4.2 La darea în exploatare a sistemului de supraveghere video, persoana împuternicită va primi instructajul referitor la setările sistemului de monitorizare video, respectarea regimului de confidenţialitate şi dreptul de acces la informaţia prelucrată în sistemul de evidenţă.

5.Limitarea scopului

5.1 Sistemul de supraveghere video va fi utilizat numai în scopul în care este notificat, fără a se urmări în special obţinerea unor informaţii pentru anchetele interne sau procedurile disciplinare, cu excepţia situaţiilor în care se produce un incident de securitate sau se observă un comportament infracţional (în circumstanţe excepţionale imaginile pot fi transmise organelor competente în cadrul unor investigaţii disciplinare sau penale).

5.2 În vederea protejării vieţii private a altor subiecţi decât cei vizaţi nemijlocit, sistemul video este dotat cu mecanisme care prevăd estomparea imaginii (în caz de necesitate) pentru a face ca întreaga imagine sau o parte a ei, după caz, să fie anonimizată.

5.3 Persoana responsabilă va gestiona accesul la sistemul de supraveghere video numai cu acordul scris al conducerii UnAŞM.

6.Categorii speciale de date cu caracter personal

6.1 Sistemul de monitorizare video al UnAŞM nu are ca scop captarea (spre exemplu prin focalizare sau orientare selectivă) sau prelucrarea imaginilor (spre exemplu indexare, creare de profiluri) care constituie categoria specială de date cu caracter personal.

7.Accesul la datele cu caracter personal şi dezvăluirea acestora

7.1 Accesul la imaginile video înregistrate în timp real este limitat la un număr redus de angajaţi ai UnAŞM, care pot fi identificaţi individual, în conformitate cu lista aprobată de către conducerea Universităţii.

7.2 Accesul la imaginile video şi/ sau la arhiva în care sunt stocate imaginile în registrate este permis numai persoanei responsabile în conformitate cu Politica de securitate a UnAŞM şi numai cu acordul scris al conducerii.

7.3 Vizualizarea şi/sau efectuarea copiilor din fişierele temporare în care sunt stocate imagimle video, este permisă numai cu acordul scris al conducerii.

7.4 În cazul solicitării de către organele de drept ale Republicii Moldova, care îşi exercită atribuţiile conform legii, a unor copii din fişierele temporare în care sunt stocate imaginile video, este permis numai cu acordul scris al conducerii UnAŞM.

8. Protecţia sistemului informaţional de date cu caracter personal în care sînt stocate (prelucrate) imaginile video

8.1 În vederea securizării sistemului informaţional de date cu caracter personal în care sunt stocate (prelucrate) imaginile video, se aplică următoarele măsuri tehnice şi organizatorice:

a) sistemul informaţional de date cu caracter personal în care sînt stocate (prelucrate) imaginile video se păstrează într-o cameră special amenajată;

b) responsabilul de protecţie a datelor cu caracter personal şi responsabilii de securitate din cadrul UnAŞM vor fi consultaţi înainte de achiziţionarea sau instalarea oricărui nou sistem de supraveghere;

- toate sistemele trebuie să corespundă cerinţelor de securitate descrise în legislaţie (HG nr. 1123 privind aprobarea cerinţelor faţă de asigurarea securităţii datelor cu caracter personal);

c) accesul fizic la sistemul informaţional de date cu caracter personal în care sînt stocate (prelucrate) imaginile video are numai persoana responsabilă desemnată şi conducerea UnAŞM;

d) accesul la înregistrările video prelucrate este restricţionat prin introducerea unui şir de parole;

e) în cazul deconectării energiei electrice, sistemul informaţional de date cu caracter personal în

care sunt stocate (prelucrate) imaginile video este dotat cu sursă autonomă de alimentare cu energie electrică (UPS);

k) sistemul informațional de date cu caracter personal în care sunt stocate (prelucrate) imaginile video este dotat cu firewall care asigură protecția în rețea;

l) echipamentele sunt astfel instalate încît să se afle sub supraveghere doar acele spații identificate în analiza de risc ca având nevoie de protecție suplimentară;

m) utilizatorii sistemului de supraveghere video sunt instruiți să nu monitorizeze astfel de zone;

n) UnAȘM actualizează în permanență listă persoanelor care au acces la sistemul informațional de date cu caracter personal în care sunt stocate (prelucrate) imaginile video, care descrie în detaliu drepturile de acces ale acestora.

9. Măsurile tehnice și organizatorice pentru protecția și securitatea sistemului video și sporirea gradului de protecție a vieții private

9.1 Limitarea timpului de stocare a materialului filmat, în conformitate cu cerințele de securitate și legislația în vigoare privind conservarea datelor;

9.2 Mediile de stocare (serverele pe care se stochează imaginile înregistrate) se află în spații securizate și protejate de măsuri de securitate fizică;

9.3 Toți utilizatorii cu drept de acces la sistemul de supraveghere video au semnat acorduri de confidențialitate, prin care se obligă să respecte prevederile legale în domeniu;

9.4 Utilizatorilor se acordă dreptul de acces doar pentru acele resurse care sunt strict necesare pentru îndeplinirea atribuțiilor de serviciu;

9.5 Doar administratorii, de sistem numiți în acest sens de către operator și responsabilul de securitate, au dreptul de a accesa fișierele înregistrate în sistem, la cererea conducerii universității.

10. Camera de control

10.1 Imaginile captate de sistemul de supraveghere video sunt vizualizate în timp real pe monitoarele din camera de control acces, care reprezintă o încăpere securizată, iar monitoarele nu pot fi văzute din exterior.

10.2 Camera de control este amplasată în sediul central al UnAȘM.

10.3 Accesul neautorizat în Camera de control este interzis.

10.4 Accesul altor persoane în camera de control unde se află sistemul de supraveghere video, se acordă numai în bază de autorizare eliberată de responsabilul de securitate din cadrul universității.Aceste persoane nu vor avea acces la datele personale prelucrate, accesul fiind permis strict doar pentru executarea lucrărilor menționete în autorizație.

11.Drepturi de acces

11.1 Accesul la imaginile stocate și/sau la arhitectura tehnică a sistemului de supraveghere video este limitat la un număr redus de persoane și este determinat prin atribuțiile specificate în fișa postului, în care este indicat în ce scop și ce tip de acces este acordat.

11.2 UnAȘM impune limite stricte în privința persoanelor care au dreptul:

a) să vizioneze materialul filmat în timp real: imaginile care se derulează în timp real sunt accesibile responsabililor de securitate și agenților de pază desemnați să desfășoare activitatea de supraveghere;

b) să vizioneze înregistrarea materialului filmat care se va face în cazuri justificate, cum ar fi cele prevăzute de lege și incidentele de securitate, de către persoanele special desemnate;

c) să copieze, să descarce, să șteargă sau să modifice orice material filmat de sistemul de supraveghere video.

11.3 Instructaj :

a) toți membrii personalului cu drepturi de acces beneficiază de o instruire inițială în domeniul protecției datelor.

b) această procedură va fi integrată în programul de instruire și îndrumare, pentru toți utilizatorii cu drept de acces și atribuții în operarea sistemului de supraveghere video.

c) şeful subdiviziunii va asigura că întregul personal din subordine, implicat în operarea sistemului de supraveghere video, este instruit şi informat cu privire la toate aspectele funcţionale, operaţionale şi administrative ale acestei activităţi.

11.3 Măsuri de păstrare a confidenţialităţii. Imediat după instructaj, fiecare participant cu drept de acces la sistemul de supraveghere video semnează un acord de confidenţialitate.

12. Dezvăluirea datelor cu caracter personal

12.1 Orice activitate de dezvăluire a datelor personale către terţi va fi documentată şi supusă unei analize riguroase privind pe de-o parte necesitatea comunicării, şi pe de altă parte compatibilitatea dintre scopul în care se face comunicarea şi scopul în care aceste date au fost colectate iniţial pentru prelucrare.

12.2 Orice situaţie de dezvăluire va fi consemnată de administratorul sistemului într-un Registru de evidenţă a cazurilor de dezvăluire.

12.3 UnAŞM are obligaţia punerii la dispoziţia organelor judiciare, la solicitarea scrisă a acestora, înregistrările video în care este surprinsă săvârşirea unor fapte de natură contravenţională/penală.

12.4 Sistemul de supraveghere video nu este utilizat pentru verificarea prezenţei la program sau evaluarea performanţei la locul de muncă.

12.5 În cazuri excepţionale, dar cu respectarea garanţiilor descrise mai sus, se poate acorda acces altor servicii din cadrul universităţii(Protecţie Antiincendiară, Resurse Umane, Riscuri), în cadrul unei anchete disciplinare, de accidentare sau de securitate, cu condiţia ca informaţiile să ajute la investigarea unei infracţiuni, accident de muncă sau a unei abateri disciplinare de natură să prejudicieze drepturile şi libertăţile unei persoane fizice sau juridice.

13. Durata păstrării înregistrărilor video

13.1 Durata păstrării înregistrărilor video este de 30 zile calendaristice, după care acestea se nimicesc automat în ordinea în care au fost înregistrate.

13.2 În cazul producerii unui incident de securitate, durata de păstrare a înregistrărilor video poate depăşi limitele admisibile de program, în funcţie de timpul necesar investigării suplimentare a incidentului de securitate.

14.Informarea publicului referitor la supravegherea video

Informarea publicului referitor la supravegherea video din cadrul UnAŞM se efectuează prin pictograme. UnAŞM garantează că va asigura respectarea drepturilor ce revin persoanelor vizate, în conformitate cu legislaţia Republicii Moldova. Toate persoanele implicate în activitatea de supraveghere video şi cele responsabile de administrarea imaginilor filmate, vor respecta procedurile şi regulamentele de acces la date cu caracter personal ale universităţii.

15. Informarea persoanelor vizate

15.1 Informarea primară a persoanelor vizate se realizează în mod clar şi permanent, prin intermediul unui semn adecvat, cu vizibilitate suficientă şi localizat în zona supravegheată, astfel încât să semnaleze existenţa camerelor de supraveghere, dar şi pentru a comunica informaţiile esenţiale privind prelucrarea datelor cu caracter personal.

15.2 Persoanele vizate sunt atenţionate asupra existenţei sistemului de supraveghere video şi a proprietarului prin note de informare corespunzătoare, care cuprind scopul prelucrării şi identifică UnAŞM ca operator al datelor colectate prin intermediul supravegherii video.

16.Exercitarea drepturilor de acces, intervenţie şi opoziţie

16.1 Pe întreaga perioadă de stocare a datelor cu caracter personal, persoanele vizate au dreptul de acces la datele personale care deţinute de UnAŞM, de a solicita intervenţia (ştergere/actualizare/rectificare/anonimizare) sau de a se opune prelucrărilor, conform legii.

16.2 Orice cerere de a accesa, rectifica, bloca şi/sau şterge date cu caracter personal ca urmare a utilizării camerelor video ar trebui să fie adresată direct UnAŞM.

16.3 În cazul în care persoana vizată are alte întrebări privind prelucrarea de către UnAŞM a datelor personale care o privesc, se poate adresa conducerii UnAŞM .

16.4 Răspunsul la solicitarea de acces, intervenţie sau opoziţie se dă în termen de 15 zile calendaristice. Dacă nu se poate respecta acest termen, persoana vizată va fi informată asupra motivului de amânare a răspunsului, de asemenea i se va comunica şi procedura care va urma pentru soluţionarea cererii.

16.5 Dacă există solicitarea expresă a persoanei vizate, se poate acorda dreptul de a vizualiza imaginile înregistrate i se poate trimite o copie a acestora. Imaginile furnizate vor fi clare, în măsura posibilităţii, cu condiţia de a nu prejudicia drepturile terţilor (persoana vizată va putea vizualiza doar propria imagine, imaginile altor persoane care pot apărea în înregistrare vor fi editate astfel încît să nu fie posibilă recunoaşterea/identificarea lor). În cazul unei asemenea solicitări, persoana vizată este obligată:

a) să se identifice dincolo de orice suspiciune (să prezinte actul de identitate cînd participă la vizionare), să menţioneze data, ora, locaţia şi împrejurările în care a fost înregistrată de camerele de supraveghere.

b) de asemenea, persoana vizată va prezenta şi o fotografie recentă astfel încît utilizatorii desemnaţi să o poată identifica mai usor în imaginile filmate.

c) persoana va putea vizualiza doar propria imagine, imaginile persoanelor care pot apărea în înregistrare vor fi editate astfel încît să nu fie posibilă recunoaşterea/identificarea lor.

d) există posibilitatea refuzării dreptului de acces în situaţia în care se aplică excepţiile prevăzute de lege. Necesitatea de a restricţiona accesul se poate impune şi în cazul în care există obligaţia de a proteja drepturile şi libertăţile unor persoane terţe , de exemplu dacă în imagini apar şi alte persoane şi nu există posibilitatea de a obţine consimţământul lor sau nu se pot extrage, prin editarea imaginilor, datele personale nerelevante.

17.Auditul securităţii sistemului de monitorizare video

17.1 Auditul securităţii sistemului de monitorizare video menţine înscrieri de sistem despre evenimentele produse în activitatea sistemului sau a aplicaţiei, precum şi despre activitatea utilizatorului.

17.2 În conjuncţie cu instrumentele şi procedurile respective, auditul securităţii sistemului de monitorizare video permite promovarea mijloacelor de ajutor pentru a atinge obiective de securitate, cum ar fi evidenţa acţiunilor utilizatorului, definirea şi stabilirea responsabilităţii individuale, reconstrucţia evenimentelor, detectarea intruşilor şi problemelor de identificare a evenimentelor.

17.3 Auditul securităţii sistemului de monitorizare video este destinat să acorde suport la:

a) stabilirea consecutivităţii acţiunilor utilizatorului sau proceselor;

b) stabilirea când, cine sau ce a stopat funcţionarea normală a sistemului;

c) detectarea problemelor de funcţionare a sistemului informatic în regim on-line.

Anexa nr.1

Lista locaţiilor pentru amplasarea camerelor de supraveghere în cadrul UnAŞM

I. Locaţiile şi spaţiile de acces, destinate publicului de la parterul clădirilor;
   1. Camera Nr.2. Etaj I, coridor, aulele 8,9,10;
   2. Camera Nr.3. Etaj I, coridor, aulele 4,6,S, intrarea de rezervă;
   3. Camera Nr.4. Etaj II, coridor, aulele 22,19,18,17;
   4. Camera Nr.5. Etaj II, coridor, laboratorul CBM, aulele 28,29,30;
   5. Camera Nr.6. Etaj II, coridor, aulele 15,16,31,32;
   6. Camera Nr.7. Etaj I, coridor, aulele 11,12, locul de serviciu al portarului, intrarea centrală;

II. Locaţiile din împrejurimile clădirilor pentru a proteja spaţiile exterioare;
   1. Camera Nr.1. Etaj I, de asupra intrării centrale în blocul principal;

III. Locaţile critice de amplasare a echipamentelor şi sitemelor IT şi de telecomunicaţii:
   1. Aula 31/1 – server IT şi de reţea, sisemul de supraveghere video;
   2. Locul de serviciu al portarului, intrarea centrală – monitor sutraveghere video.