POLITICA
de asigurare a securităţii datelor cu caracter personal în cadrul Instituției Publice Centrul de Instruire și Inovații TIC-TEKWILL, IDNO 1017620001325

PREAMBUL

Cerinţele faţă de asigurarea securităţii datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaţionale şi mecanice de date cu caracter personal au drept scop stabilirea regulilor de implementare de către Instituția Publică Centrul de Instruire și Inovații TIC-TEKWILL a măsurilor tehnice și organizatorice necesare pentru asigurarea securităţii, confidenţialităţii şi integrităţii datelor cu caracter personal prelucrate în cadrul sistemelor informaţionale şi mecanice de date cu caracter personal şi/sau registrelor ţinute manual, în conformitate cu prevederile Legii nr.133 din 08.07.2011 privind protecţia datelor cu caracter personal; Legii nr.71-XVI din 22 martie 2007 cu privire la registre; Hotărârii Guvernului nr.1123 din 14.12.2010 „Privind aprobarea Cerinţelor faţă de asigurarea securităţii datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaţionale de date cu caracter personal"; Convenţiei pentru protecţia persoanelor referitor la prelucrarea automatizată a datelor cu caracter personal, încheiată la Strasbourg la 28.01.1981, publicată în European Treaty Series, nr.108, ratificată de Republica Moldova prin Hotărârea Parlamentului nr. 483-XIV din 02.07.1999.

DISPOZIŢII GENERALE

1. În sensul prezentei Politici, se definesc următoarele noţiuni:
autentificare - verificarea identificatorului atribuit subiectului de acces, confirmarea autenticităţii;
fişiere temporare – ansamblu de date sau informaţii pe suport digital creat pentru o perioadă de timp limitat până la iniţierea îndeplinirii sarcinilor pentru care au fost desemnate;
identificare – atribuirea unui identificator subiecţilor şi obiectelor de acces și/sau compararea identificatorului prezentat cu lista identificatoarelor atribuite;
integritate – certitudinea, necontradictorialitatea și actualitatea informaţiei care conţine date cu caracter personal, protecţia ei de distrugere și modificare neautorizată;
mijloace de protecţie criptografică a informaţiei care conţine date cu caracter personal – mijloace tehnice, de program și tehnico-aplicative, sisteme și complexe de sisteme ce realizează algoritmi de conversie criptografică a informaţiei care conţine date cu caracter personal, destinate să asigure integritatea și confidenţialitatea informaţiei în procesul de prelucrare, depozitare și transmitere a acesteia prin canalele de comunicaţii;
politica de securitate a datelor cu caracter personal – document, elaborat de către Instituția Publică Centrul de Instruire și Inovații TIC-TEKWILL care oferă o descriere generală a măsurilor de securitate și trăsăturilor de protecţie selectate pentru securitatea datelor, ţinându-se cont de potenţialele pericole pentru datele cu caracter personal prelucrate şi riscurile reale la care sunt expuse acestea;
perimetru de securitate – zona care reprezintă în sine o barieră de trecere asigurată cu mijloace de control tehnic al accesului;
control de securitate – acţiuni întreprinse de către deţinătorii de date cu caracter personal sau Centrul Naţional pentru Protecţia Datelor cu Caracter Personal (Centrul) în vederea verificării şi/sau asigurării nivelului adecvat de securitate a datelor cu caracter personal prelucrate în cadrul sistemelor informaţionale și/sau registrelor ţinute manual, în conformitate cu prezentele Cerinţe;
persoana responsabilă de politica de securitate a datelor cu caracter personal– persoana responsabilă de funcţionarea corespunzătoare a sistemului complex de protecţie a informaţiei care conţine date cu caracter personal, precum și de elaborarea, implementarea și monitorizarea respectării prevederilor politicii de securitate a deţinătorului de date cu caracter personal;

protecţia informaţiei contra acţiunilor neintenţionate – ansamblu de măsuri orientate spre prevenirea acţiunilor neintenţionate, provocate de erorile utilizatorului, defectele mijloacelor tehnico-aplicative, fenomenele naturii sau alte cauze ce nu au ca scop direct modificarea informaţiei, dar care conduc la distorsiunea, distrugerea, copierea, blocarea accesului la informaţie, precum și la pierderea, distrugerea acesteia sau la defectarea suportului material al informaţiei care conţine date cu caracter personal;
purtător de date cu caracter personal – suport magnetic, optic, laser, de hârtie sau alt suport al informaţiei, pe care se creează, se fixează, se transmite, se recepţionează, se păstrează sau, în alt mod, se utilizează documentul și care permite reproducerea acestuia;
restaurarea datelor – procedurile cu privire la reconstituirea datelor cu caracter personal în starea în care se aflau până la momentul pierderii sau distrugerii acestora;
tehnologie informaţională (TI) – totalitatea metodelor, procedeelor și mijloacelor de prelucrare și transmitere a informaţiei care conţine date cu caracter personal și regulile de aplicare a acesteia;
mijloace de protecţie criptografică a informaţiei care conţine date cu caracter personal – mijloace tehnice, de program și tehnico-aplicative, sisteme și complexe de sisteme ce realizează algoritmi de conversie criptografică a informaţiei care conţine date cu caracter personal, destinate să asigure integritatea și confidenţialitatea informaţiei în procesul de prelucrare, depozitare și transmitere a acesteia prin canalele de comunicaţii;
utilizator – persoana care acţionează sub autoritatea deţinătorului de date cu caracter personal, cu drept recunoscut de acces la sistemele informaţionale de date cu caracter personal;
sesiune de lucru – perioada care durează din momentul pornirii calculatorului și aplicaţiei de utilizare a resursei informaţionale sau din momentul pornirii resursei informaţionale și până la momentul opririi acestora;
sistem informaţional de date cu caracter personal – totalitatea resurselor și tehnologiilor informaţionale interdependente, de metode și de personal, destinată păstrării, prelucrării și furnizării de informaţie care conţine date cu caracter personal;
stocare – păstrarea pe orice fel de suport a datelor cu caracter personal;

CERINŢE GENERALE

2. Măsurile de protecţie a datelor cu caracter personal reprezintă o parte componentă a lucrărilor de creare, dezvoltare și exploatare a sistemelor informaţionale de date cu caracter personal și vor fi efectuate neîntrerupt de către persoanele responsabile angajate la Instituția Publică Centrul de Instruire și Inovații TIC-TEKWILL.
3. Protecţia datelor cu caracter personal este asigurată printr-un complex de măsuri tehnice și organizatorice de preîntâmpinare a prelucrării ilicite a datelor cu caracter personal.
4. Măsurile de protecţie a datelor cu caracter personal prelucrate în sistemele informaţionale și mecanice de date cu caracter personal ale Instituției Publice Centrul de Instruire și Inovații TIC-TEKWILL se înfăptuiesc ţinându-se cont de necesitatea asigurării confidenţialităţii acestor măsuri.
5. Sunt supuse protecţiei, toate resursele informaţionale ale Instituției Publice Centrul de Instruire și Inovații TIC-TEKWILL, care conţin date cu caracter personal, inclusiv:
1) Suporturile magnetice, optice, laser sau alte suporturi ale informaţiei electronice, masive informaţionale și baze de date;
2) Sistemele informaţionale, reţelele, sistemele operaţionale, sistemele de gestionare a bazelor de date și alte aplicaţii, sistemele de telecomunicaţii, inclusiv mijloacele de confecţionare și multiplicare a documentelor și alte mijloace tehnice de prelucrare a informaţiei.
6. Protecţia datelor cu caracter personal în sistemele informaţionale de date cu caracter personal este asigurată în scopul:
a) Preîntâmpinării scurgerii informaţiei care conţine date cu caracter personal prin metoda excluderii accesului neautorizat la aceasta;
b) Preîntâmpinării distrugerii, modificării, copierii, blocării neautorizate a datelor cu caracter personal în reţelele de telecomunicaţie și resursele informaţionale;

c) Respectării cadrului normativ de folosire a sistemelor informaţionale şi a programelor de prelucrare a datelor cu caracter personal;
d) Asigurării caracterului complet, integru, veridic al datelor cu caracter personal în reţelele de telecomunicaţie şi resurselor informaţionale;
e) Păstrării posibilităţilor de gestionare a procesului de prelucrare şi păstrare a datelor cu caracter personal.
7. Protecţia datelor cu caracter personal prelucrate în sistemele informaţionale se efectuează prin următoarele metode:
1) Preîntâmpinarea conexiunilor neautorizate la reţelele informaţionale şi interceptării cu ajutorul mijloacelor tehnice a datelor cu caracter personal transmise prin aceste reţele;
2) Excluderea accesului neautorizat la datele cu caracter personal prelucrate;
3) Preîntâmpinarea acţiunilor speciale tehnice şi de program, care condiţionează distrugerea, modificarea datelor cu caracter personal sau defecţiuni în lucrul complexului tehnic şi de program;
4) Preîntâmpinarea acţiunilor intenţionate şi/sau neintenţionate a utilizatorilor interni şi/sau externi, precum şi a altor angajaţi ai deţinătorului de date cu caracter personal, care condiţionează distrugerea, modificarea datelor cu caracter personal sau defecţiuni în lucrul complexului tehnic şi de program.
5) Preîntâmpinarea scurgerii de informaţii care conţin date cu caracter personal, transmise prin canalele de legătură, este asigurată prin folosirea metodelor de cifrare a acestei informaţii, inclusiv cu utilizarea măsurilor organizaţionale, tehnice şi de regim.
6) Preîntâmpinarea distrugerii, modificării datelor cu caracter personal sau defecţiunilor în funcţionarea soft-ului destinat prelucrării datelor cu caracter personal este asigurată prin metoda folosirii mijloacelor de protecţie speciale tehnice şi de program, inclusiv a programelor licenţiate, programelor anti virus, organizării sistemului de control al securităţii soft-ului şi efectuarea periodică a copiilor de siguranţă.
8. Ordinea de acces la informaţia care conţine date cu caracter personal, prelucrată în cadrul sistemelor informaţionale, se stabileşte de Instituția Publică Centrul de Instruire și Inovații TIC-TEKWILL conform Regulamentului sistemului informaţional utilizat.

POLITICA DE SECURITATE A DATELOR CU CARACTER PERSONAL

9. Instituția Publică Centrul de Instruire și Inovații TIC-TEKWILL nominalizează responsabil de întocmirea, menţinerea, modificarea şi actualizarea politicii de securitate - Directorul.
10. Măsurile de securitate emise sunt stabilite conform regulamentelor de securitate ale fiecărui sistem care prelucrează date cu caracter personal. În acest sens, la Instituția Publică Centrul de Instruire și Inovații TIC-TEKWILL sunt create următoarele sisteme/registre de prelucrare a datelor cu caracter personal:
a) Registru de evidență a angajaților;
b) Registru de evidență a contractanților;
c) Supravegherea video.
11. Se numesc responsabili de administrarea sistemelor următoarele persoane:
a) Directorul:
• Registru de evidență a angajaților.
• Registru de evidență a contractanților.
b) Manager tehnic
• Supravegherea video.
12. Mecanismul de punere în aplicare a măsurilor de securitate pentru toate categoriile sistemelor informaţionale de date cu caracter personal este prevăzut de prezenta Politică de Securitate.
13. În cadrul activității Instituția Publică Centrul de Instruire și Inovații TIC-TEKWILL colectează și prelucrează cu acordul subiectului de date cu caracter personal, următoarele date cu caracter personal:

1) Numele, prenumele și după caz patronimicul;
2) sexul;
3) data și locul nașterii;
4) cetățenia;

5) IDNP;
6) datele personale ale membrilor de familie;
7) datele din permisul de conducere;
8) datele bancare;
9) semnătura;
10) situaţia familială;
11) situaţia militară;
12) datele din actele de stare civilă;
13) codul personal de asigurării sociale (CPAS);
14) codul asigurării medicale (CPAM);
15) numărul de telefon/fax;
16) numărul de telefon mobil;
17) adresa (domiciliului/reşedinţei);
18) adresa e-mail;
19) profesia şi/sau locul de muncă;
20) formarea profesională – diplome – studii.

14. Instituția Publică Centrul de Instruire și Inovații TIC-TEKWILL nu transmite date cu caracter personal ale subiecților în afara țării, cu excepția cazurilor prevăzute de lege sau expres acceptate de către aceștia.
15. Instituția Publică Centrul de Instruire și Inovații TIC-TEKWILL asigură angajaților săi dreptul de acces, de stocare, de prelucrarea informației ce conține date cu caracter personal.
16. Instituția Publică Centrul de Instruire și Inovații TIC-TEKWILL acordă accesul angajaților săi la prelucrarea datelor cu caracter personal, numai după ce au semnat o Declarație de Confidențialitate prin care s-au obligat să nu divulge informația ce conține date cu caracter personal obținută în timpul exercitării atribuțiilor de serviciu. **Modelul Declarației de Confidențialitate este anexat la prezenta Politică.**
17. Documentaţia tehnică cu privire la controalele de securitate este ţinută sub formă de registre de către persoana responsabilă, numită prin ordinul/decizia Instituția Publică Centrul de Instruire și Inovații TIC-TEKWILL pentru fiecare sistem informaţional în parte.
18. 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.
19. Rapoartele despre incidentele de securitate sunt înregistrate în registrele respective de către persoanele responsabile. Fiecare incident urmează a fi adus la cunoştinţa Instituția Publică Centrul de Instruire și Inovații TIC-TEKWILL în mod de urgenţă, pentru a putea fi identificată procedura de soluţionare a incidentului.

SECURITATEA MEDIULUI FIZIC ŞI A TEHNOLOGIILOR INFORMAŢIONALE FOLOSITE ÎN PROCESUL PRELUCRĂRII DATELOR CU CARACTER PERSONAL

Autorizarea accesului fizic

20. Accesul în sediile/oficiile/birourile ori spaţiile unde sunt amplasate sistemele informaţionale de date cu caracter personal este restricţionat, fiind permis doar persoanelor care au autorizaţia necesară şi doar în timpul programului de muncă.
21. Accesul se efectuează în baza permiselor eliberate angajaților.
22. Accesul în camera de servere este permisă doar salariaților Instituției Publice Centrul de Instruire și Inovații TIC-TEKWILL care au autorizare specială din partea Directorului. Persoanele terțe au acces în această încăpere doar sub stricta supraveghere a salariatului menționat mai sus. Toate operaţiunile de acces la servere sau alte mijloace tehnice sau software se face de către Directorul Instituției Publice Centrul de Instruire și Inovații TIC-TEKWILL.

Securitatea sediilor/oficiilor/birourilor și mijloacelor de prelucrare a datelor cu caracter personal

28. Perimetrul sediilor și încăperii în care sunt amplasate mijloacele de prelucrare a datelor cu caracter personal sunt păstrate integre din punct de vedere fizic, toți pereții sunt întregi, ușile se încuie, iar ferestrele se închid.

29. Computerele, serverele și alte terminale de acces, în limita posibilității sunt amplasate în locuri cu acces limitat pentru persoane străine. Accesul în încăperile respective sunt limitate prin scanarea cardului de acces.

30. Ușile și ferestrele se încuie în cazul în care în încăpere lipsesc angajații.

31. Amplasarea mijloacelor de prelucrare a datelor cu caracter personal corespunde necesității asigurării securității acestora contra accesului nesancționat, furturilor, incendiilor, inundațiilor și altor posibile riscuri.

32. 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.

33. Se vor implementa sisteme de constatare a intruziunilor pentru ușile exterioare și ferestrele amplasate în locuri accesibile.

34. Utilajul de rezervă și purtătorii de informații care conțin date cu caracter personal se păstrează în locuri care permit evitarea distrugerilor sau deteriorărilor ca rezultat al calamităților.

Controlul vizitatorilor

35. Trebuie asigurat controlul accesului fizic al vizitatorilor în încăperile unde sunt amplasate sistemele informaționale de date cu caracter personal.

36. Vizitatorii sistemelor informaționale de date cu caracter personal și alte persoane care accesează încăperile sunt supravegheați în încăperile unde aceștia au acces. În birourile cu acces interzis aceștia pot intra doar sub supravegherea personalului autorizat. În cazul depistării persoanelor cu acces interzis în birourile cu acces limitat, acești vor fi rugați să părăsească încăperea în mod cât mai urgent. Incidentul va fi adus la cunoștința Directorului Instituției Publice Centrul de Instruire și Inovații TIC-TEKWILL.

Securitatea electroenergetică

37. 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. 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.

38. Instituția Publică Centrul de Instruire și Inovații TIC-TEKWILL va depune efortul pentru a procura surse autonome de alimentare cu energie electrică de scurtă și lungă durată, care sunt folosite pentru terminarea corectă a sesiunii de lucru a sistemului (componentului) în cazul deconectării de la sursa principală de alimentare cu energie electrică.

Securitatea cablurilor de rețea

39. Cablurile de rețea, prin care se efectuează operațiuni de prelucrare a datelor cu caracter personal, sunt protejate contra conectărilor nesancționate sau deteriorărilor. Cablurile de tensiune sunt separate de cele comunicaționale pentru a exclude bruiajul. Managerul tehnic efectuează controale, nu mai rar decât o dată în lună, în scopul verificării cazurilor de conectare neautorizată la cablurile de rețea.

Asigurarea securității anti incendiare a sistemelor informaționale de date cu caracter personal

40. Instituția Publică Centrul de Instruire și Inovații TIC-TEKWILL dispune de mijloace de asigurare a securității anti incendiare a sediilor/oficiilor/birourilor unde sunt amplasate sistemele informaționale de date cu caracter personal și mijloacele de prelucrare a datelor cu caracter personal.

Controlul instalării şi scoaterii componentelor IT
41. Se exercită 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.

Măsurile generale de administrare a securităţii informaţionale
42. În cazul neutilizării temporare a purtătorilor de informaţie pe suport de hârtie sau electronici (digitali) care conţin date cu caracter personal, aceştia se păstrează în safeu metalic 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 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 Directorului Instituției Publice Centrul de Instruire și Inovații TIC-TEKWILL.

IDENTIFICAREA ŞI AUTENTIFICAREA UTILIZATORULUI SISTEMULUI INFORMAŢIONAL DE DATE CU CARACTER PERSONAL

Identificarea şi autentificarea utilizatorului
43. Este efectuată identificarea și autentificarea utilizatorilor sistemelor informaționale de date cu caracter personal și a proceselor executate în numele acestor utilizatori.
Toți utilizatorii (inclusiv personalul care asigură susținerea tehnică, administratorii de rețea, programatorii și administratorii bazelor de date) au un identificator personal (ID-ul utilizatorului), care nu trebuie să conţină semnalmentele nivelului de accesibilitate al utilizatorului. Pentru confirmarea ID-ului utilizatorului sunt utilizate parole. În cazul în care a fost depusă cererea de demisie, în cazul când 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 în mod automat în decursul a două săptămâni de la ultimul acces, sau în mod individual imediat la momentul introducerii modificării în raportul de muncă.
44. Se utilizează autentificarea multifactorială, care include parole complexe, cu includerea simbolurilor, literelor, cifrelor în combinaţie complexă. În mod obligatoriu fiecare parolă conţine una sau mai multe litere scrise cu majusculă. Parola nu va conține inițialele sau date care pot caracteriza o anumită persoană (data de naștere, adresă, nume etc).

Identificarea şi autentificarea echipamentului
45. Este asigurată posibilitatea identificării și autentificării echipamentului folosit în operațiunile de prelucrare a datelor cu caracter personal.

Administrarea identificatorilor utilizatorilor
46. Administrarea identificatorilor utilizatorilor include:
1) identificarea univocă a fiecărui utilizator;
2) verificarea autenticităţii fiecărui utilizator;
3) obținerea autorizației de la persoana responsabilă pentru eliberarea ID-ului utilizatorului doar în cazul semnării declarației de confidențialitate și trecerii procedurii de instruire;
4) garantarea faptului că ID-ul utilizatorului este eliberat unei persoane determinate concret;
5) executarea copiilor de arhivă a ID-urilor utilizatorilor.

Asigurarea conexiunii bilaterale în cazul introducerii informaţiei de autentificare a utilizatorilor
47. Se asigură conexiunea bilaterală a Instituției Publice Centrul de Instruire și Inovații TIC-TEKWILL cu utilizatorul în momentul trecerii de către acesta a procedurilor de autentificare, care nu compromite mecanismul de autentificare.

Utilizarea parolelor în procesul asigurării securităţii informaţionale
48. Se respectă regulile de asigurare a securităţii informaţionale în cazul alegerii şi folosirii parolelor care includ:
1) păstrarea confidenţialităţii parolelor;
2) modificarea parolelor de fiecare dată când sunt prezente indiciile eventualei compromiteri a sistemului sau parolei;
3) alegerea parolelor calitative cu o mărime de minimum 8 simboluri, care nu sunt legate de informaţia cu caracter personal a utilizatorului, nu conţin simboluri identice consecutive şi nu sunt compuse integral din grupuri de cifre sau litere;
4) modificarea parolelor odată în lună;
5) dezactivarea procesului automatizat de înregistrare (cu folosirea parolelor salvate).
6) introducerea greşită a parolei de trei ori presupune blocarea imediată a contului.

Administrarea parolelor utilizatorilor
49. Se folosesc identificatoare individuale pentru fiecare utilizator şi parole individuale ale acestora pentru asigurarea posibilităţii de stabilire a responsabilităţii. Este asigurată posibilitatea utilizatorilor de a alege şi schimba parolele individuale, inclusiv de activare a procedurii de evidenţă a introducerilor greşite ale acestora. Se asigură blocarea accesului după trei tentative greşite de autentificare. Este asigurată păstrarea istoriilor anterioare ale parolelor în formă de hash a utilizatorilor (pentru o perioada de un an) şi prevenirea folosirii repetate a acestora. La momentul introducerii, parolele nu se reflectă pe monitor. Parolele se păstrează în formă cifrată, utilizându-se algoritmul criptografic unilateral (funcţia hash).

ADMINISTRAREA ACCESULUI UTILIZATORILOR

Administrarea accesului
50. Se implementează mecanisme de înregistrare şi evidenţă a persoanelor care au acces sau participă la operaţiunile de prelucrare a datelor cu caracter personal şi care, în caz de necesitate, permit identificarea cazurilor neautorizate de acces sau de prelucrare ilegală a datelor cu caracter personal.

Administrarea conturilor de acces (account)
51. Este efectuată administrarea conturilor de acces a utilizatorilor care prelucrează date cu caracter personal, inclusiv crearea, activarea, modificarea, revizuirea, dezactivarea şi ştergerea acestora. Sunt folosite mijloace automatizate de suport în scopul administrării conturilor de acces. Se folosesc mijloace automatizate de înregistrare şi informare despre crearea, modificarea, dezactivarea şi încetarea acţiunii conturilor de acces.

Acordarea accesului
52. Este autorizat accesul la sistemele informaţionale de date cu caracter personal în conformitate cu prezenta Politică de securitate de către persoanele numite la pct. 11.

Revizuirea drepturilor de acces ale utilizatorilor
53. Drepturile de acces ale utilizatorilor la sistemele informaţionale de date cu caracter personal sunt revizuite cu regularitate pentru asigurarea faptului că nu au fost acordate drepturi de acces neautorizate (maximum peste fiecare şase luni) şi după oricare schimbare de statut al utilizatorului.

Repartizarea obligaţiilor şi învestirea cu minimul de drepturi şi competenţe
54. Repartizarea obligaţiilor subiecţilor care asigură funcţionarea sistemelor informaţionale de date cu caracter personal este efectuată prin intermediul învestirii cu drepturi/competenţe corespunzătoare de acces, prin ordinul/decizia Directorului Instituției Publice Centrul de Instruire și Inovații TIC-TEKWILL întocmit în acest sens. Utilizatorii sistemelor informaţionale de date cu caracter personal se învestesc doar cu acele drepturi/competenţe, care sunt necesare pentru realizarea de către ei a obiectivelor stabilite acestora.

Informaţii de avertizare
55. Înainte de acordarea accesului în sistem, utilizatorii sunt informaţi despre faptul că folosirea sistemelor informaţionale de date cu caracter personal este controlată și că folosirea neautorizată a acestora se urmărește în conformitate cu legislația.

Blocarea sesiunii de lucru
56. Sesiunea de lucru în sistemul informaţional, destinat prelucrării datelor cu caracter personal, se blochează automat, după maxim 20 minute de perioadă inactivă a utilizatorului fapt care face imposibil accesul de mai departe până în momentul când utilizatorul nu deblochează sesiunea de lucru prin metoda trecerii repetate a procedurilor de identificare și autentificare.

Controlul administrării accesului
57. Se efectuează controlul acţiunilor utilizatorului în vederea evaluării corectitudinii și conformării operaţiunilor și acţiunilor efectuate prin intermediul sistemelor informaţionale de date cu caracter personal.

Marcarea documentelor
58. Informaţia ieșită din sistem, care conţine date cu caracter personal, se marchează, indicându-se prescripţii pentru prelucrarea ulterioară și răspândirea acesteia, inclusiv indicându-se numărul de identificare unic al deţinătorului de date cu caracter personal.

Accesul de la distanţă
59. Toate metodele de acces de la distanţă la sistemele informaţionale de date cu caracter personal sunt securizate (utilizându-se VPN, criptarea, cifrarea etc.), precum și sunt documentate, supuse monitorizării și controlului. Fiecare metodă de acces de la distanţă la sistemele informaţionale de date cu caracter personal se autorizează de Instituția Publică Centrul de Instruire și Inovații TIC-TEKWILL și este permisă doar utilizatorilor, cărora aceasta le este necesar pentru îndeplinirea obiectivelor stabilite.

Limitarea folosirii tehnologiilor fără fir
60. Accesul fără fir la sistemele informaţionale de date cu caracter personal este documentat, supus monitorizării și controlului. Accesul fără fir la sistemele informaţionale de date cu caracter personal este permis doar cu acordul Directorului Instituției Publice Centrul de Instruire și Inovații TIC-TEKWILL prin coordonarea cu personalul.

Administrarea accesului echipamentului portativ și mobil
61. Accesul la sistemele informaţionale de date cu caracter personal cu folosirea echipamentului portativ și mobil se documentează, este monitorizat și controlat. Folosirea echipamentului portativ și mobil este autorizată de Directorul Instituției Publice Centrul de Instruire și Inovații TIC-TEKWILL.

PROTECŢIA SISTEMELOR INFORMAŢIONALE ȘI COMUNICAŢIILOR ÎN CARE SÎNT PRELUCRATE DATE CU CARACTER PERSONAL

Divizarea programelor aplicative
62. Se asigură separarea posibilităţilor funcţionale ale utilizatorului de posibilităţile funcţionale de gestionare a sistemelor informaţionale de date cu caracter personal.

Informaţia restantă
63. Sunt preîntâmpinate tentativele dezvăluirii neautorizate sau neintenţionate a informaţiei restante care conţine date cu caracter personal, prin intermediul resurselor informaţionale general accesibile.

Prioritățile resurselor
64. Este asigurată posibilitatea limitării, cu ajutorul mecanismelor de stabilire a priorităţilor, a folosirii resurselor informaţionale în care sunt prelucrate date cu caracter personal.

Protecţia perimetrului sistemelor informaţionale în care sunt prelucrate date cu caracter personal

65. Se efectuează monitorizarea permanentă și controlul comunicaţiilor la perimetrul exterior al sistemelor informaţionale de date cu caracter personal, inclusiv la cele mai importante puncte de contact în interiorul perimetrului acestor sisteme informaţionale.

Amplasarea resurselor general accesibile se asigură în spaţiile special destinate a reţelei de calcul cu interfeţele fizice de reţea.

Este asigurată imposibilitatea accesului din exterior a utilizatorilor la reţeaua internă în care se prelucrează date cu caracter personal.

Asigurarea integrităţii și confidențialității datelor cu caracter personal transmise

66. Se asigură integritatea și confidențialitatea datelor cu caracter personal transmise, utilizându-se mijloacele de protecţie criptografică.

AUDITUL SECURITĂŢII ÎN SISTEMELE INFORMAŢIONALE DE DATE CU CARACTER PERSONAL

67. Managerul tehnic întocmește 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/terminare a sesiunii de lucru a programelor aplicative și 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 procesului;

c) ID-ul utilizatorului;

d) rezultatul tentativei de pornire – pozitivă sau negativă.

3) Se efectuează înregistrarea tentativelor de obţinere a accesului (de executare a operaţiunilor) pentru aplicaţii și procese destinate prelucrării datelor cu caracter personal, conform următorilor parametri:

a) data și timpul tentativei de obţinere a accesului (executare a operaţiunii);

b) denumirea (identificatorul) aplicaţiei sau procesului;

c) ID-ul utilizatorului;

d) specificaţiile resursei protejate (identificator, nume logic, nume fișier, număr etc.);

e) tipul operaţiunii solicitate (citire, înregistrare, ștergere etc.);

f) rezultatul tentativei de obţinere a accesului (executare a operaţiunii) – pozitivă sau negativă.

4) Se efectuează înregistrarea modificărilor drepturilor de acces (competenţelor) utilizatorului și statutului obiectelor de acces, conform următorilor parametri:

a) data și timpul modificării competenţelor;

b) ID-ul administratorului care a efectuat modificările;

c) ID-ul utilizatorului și competenţele acestuia sau specificarea obiectelor de acces și statutul nou al acestora.

68. În caz de deranjament al auditului securităţii în sistemele informaţionale de date cu caracter personal sau completării întregului volum de memorie repartizat pentru păstrarea rezultatelor auditului, este informat Directorul și/sau persoana responsabilă de politica de securitate a datelor cu caracter personal și întreprinse măsuri în vederea restabilirii capacităţii de lucru a sistemului de audit.

69. Se efectuează monitorizarea permanentă și analiza înregistrărilor de audit a securităţii în sistemele informaţionale de date cu caracter personal, în scopul depistării activităţilor neobișnuite sau suspecte de utilizare a acestor sisteme informaţionale, cu întocmirea raportului referitor la cazurile depistării acestor activităţi, stocate în mijloacele electronice de calcul.

70. Rezultatele auditului securităţii în sistemele informaţionale de date cu caracter personal, care reprezintă operaţiuni 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 confidenţialităţii și integrităţii acestora.

71. Durata stocării rezultatelor auditului securității în sistemele informaționale de date cu caracter personal se justifică în politica de securitate a datelor cu caracter personal, dar în orice caz acest termen nu este mai mic de 1 an, pentru a fi posibil folosirea acestora în calitate de probe în cazul incidentelor de securitate, unor eventuale investigații sau procese judiciare. În cazul în care procesul judiciar va dura mai mult de un an, datele menționate mai sus se vor păstra pe toată durata procesului judiciar.

ASIGURAREA INTEGRITĂŢII INFORMAŢIEI CARE CONŢINE DATE CU CARACTER PERSONAL ŞI A TEHNOLOGIILOR INFORMAŢIONALE

Înlăturarea deficiențelor de soft destinat prelucrării datelor cu caracter personal

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

Asigurarea protecţiei contra programelor dăunătoare (viruşilor)

73. Se asigură protecția contra infiltrării programelor dăunătoare în soft-urile destinate prelucrării datelor cu caracter personal, măsură care asigură posibilitatea reînnoirii automate și la timp a mijloacelor de asigurare a protecției contra programelor dăunătoare și signaturilor de virus.
74. Se asigură administrarea centralizată a mecanismelor de protecție contra programelor dăunătoare în soft-urile destinate prelucrării datelor cu caracter personal.

Tehnologiile şi mijloacele de constatare a intruziunilor

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

Asigurarea integrităţii soft-urilor şi informaţiei

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

Testarea posibilităţilor funcţionale de asigurare a securităţii sistemelor informaţionale de date cu caracter personal

77. 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).

COPIILE DE REZERVĂ ŞI RESTABILIREA INFORMAŢIEI CARE CONŢINE DATE CU CARACTER PERSONAL ŞI IT

Copiile de rezervă ale informaţiei care conţine date cu caracter personal

78. Copiile de siguranță a informațiilor care conțin date cu caracter personal și soft-urilor folosite pentru prelucrările automatizate a datelor cu caracter personal, sunt efectuate odată la șase luni.
Copiile de siguranţă se testează în scopul verificării siguranței purtătorilor de informaţii şi integrităţii informaţiei care conţine date cu caracter personal.
Procedurile de restabilire a copiilor de siguranţă se actualizează și se testează cu regularitate, în scopul asigurării eficacităţii acestora.

GESTIONAREA INCIDENTELOR DE SECURITATE A SISTEMELOR INFORMAŢIONALE DE DATE CU CARACTER PERSONAL

Instructajul de reacţionare la incidentele de securitate a sistemelor informaţionale de date cu caracter personal

79. Managerul tehnic care asigură exploatarea sistemelor informaționale de date cu caracter personal va trece, de regulă o dată în an, instruirea referitor la responsabilitățile și obligațiile în cazul executării acțiunilor de gestionare și reacționare la incidentele de securitate.

80. În cazul depistării unui incident de securitate, este asigurat mecanismul de informare neîntârziată a Directorului Instituției Publice Centrul de Instruire și Inovații TIC-TEKWILL.
81. În cazul producerii incidentelor de securitate în cadrul Instituției Publice Centrul de Instruire și Inovații TIC-TEKWILL, persoana resposabilă va întreprinde măsurile necesare pentru depistarea sursei de producere a incidentului, va efectua analiza acestuia și va înlătura cauzele incidentului de securitate cu informarea, în termen de 72 ore din momentul producerii incidentului de securitate, a Centrului Național pentru Protecția Datelor cu Caracter Personal al Republicii Moldova.
82. Pînă la 31 ianuarie a fiecărui an, operatorul de date cu caracter personal informează în scris Centrului Național pentru Protecția Datelor cu Caracter Personal al Republicii Moldova despre incidentele de securitate constatate.
83. Prelucrarea incidentelor include în mod obligatoriu depistarea, analiza, preîntâmpinarea dezvoltării, înlăturarea lor și restabilirea securității inițiale, precum și crearea unor mecanisme de evitare a ulterioarelor incidente asemănătoare.
84. Incidentele de securitate a sistemelor informaţionale de date cu caracter personal se urmăresc și se documentează în regim permanent.