

APROBAT
prin decizia Consiliului de Administrare al
„Uniunii pentru Echitate și Sănătate”
în baza Ordinului nr. __121/CA__ din 20 decembrie, 2023

INSTRUCȚIUNI
de securitate și sănătate

_____ *lațco Ala, președintă* _____
(numele, prenumele, semnătura persoanei responsabile)

CUPRINS:

1	PREVEDERI GENERALE.....	3
1.1	SPAȚIUL DE APLICARE.....	3
1.2	MODUL DE REVIZUIRE ȘI COMPLETARE	3
2	REGULI PENTRU REALIZAREA ACTIVITĂȚII ÎN DEPLINĂ SECURITATE ÎN ACTIVITATEA DE BIROU	4
3	INSTRUCȚIUNI DE SECURITATEA MUNCII LA UTILIZAREA ECHIPAMENTELOR DE BIROU	6
4	REGULI DE SECURITATE ȘI SĂNĂTATE ÎN MUNCĂ LA ORGANIZAREA LOCULUI DE MUNCĂ.....	7
5	OBLIGAȚIILE ANGAJATORULUI	9
6	INSTRUCȚIUNI DE APĂRARE ÎMPOTRIVA INCENDIILOR ÎN SPAȚIILE CU DESTINAȚIE ADMINISTRATIVĂ (BIROURI).....	9
7	PROTECȚIA DATELOR CU CARACTER PERSONAL.....	10
7.1	Măsurile generale de administrare a securității informaționale.....	14
7.2	Securitatea mediului fizic și a tehnologiilor informaționale folosite în procesul prelucrării datelor cu caracter personal	14
7.3	Identificarea și autentificarea.....	15
7.4	Controlul administrării accesului	15
7.5	Drepturile subiecților de date cu caracter personal	17
7.6	Stocarea, păstrarea și distrugerea datelor cu caracter personal prelucrate	17
7.7	Obligațiile angajaților privind protecția datelor cu caracter personal.....	18
8	INSTRUCȚIUNI DE SECURITATE ÎN LUCRUL CU BENEFICIARII DE SERVICII, INCLUSIV CU REFUGIAȚII... ..	18
	NOTĂ:	21

1 PREVEDERI GENERALE

A. Conținutul instrucțiunilor

Prezentele instrucțiuni sunt elaborate în conformitate cu prevederile Legislației RM în domeniul securității și sănătății în muncă și a Normelor metodologice de aplicare a legislației.

Conținutul instrucțiunilor din cadrul Uniunii pentru Echitate și Sănătate particularizează și concretizează:

- măsurile de prevenire a accidentelor și îmbolnăvirilor profesionale, în raport cu condițiile reale ale proceselor de muncă desfășurate;
- necesitatea și modalitatea de protecție a datelor cu caracter personal;
- obligațiile angajaților și instrucțiunile de securitate în lucrul cu beneficiarii de servicii, inclusiv cu refugiații.

B. Scopul instrucțiunilor

Scopul instrucțiunilor constă în detalierea și particularizarea prevederilor Legii securității și sănătății în muncă și Normele metodologice de aplicare a Legii, standardelor și altor reglementări în domeniu, la condițiile concrete de executare a activităților, astfel încât să fie stabilite modalitățile de acțiune pentru

- prevenirea tuturor riscurilor posibile de accidentare și îmbolnăvire profesională în cadrul organizației și protecția lucrătorilor la factorii de risc care se pot manifesta pe timpul desfășurării activităților în cadrul locului de muncă;
- asigurarea protecției datelor și securității în lucrul cu beneficiarii de servicii, inclusiv persoanele refugiate, specificând modalitatea de interacțiune cu beneficiarii de servicii și necesitatea asigurării confidențialității datelor personale ale acestora.

1.1 SPAȚIUL DE APLICARE

- Instrucțiunile date prezintă măsuri legislative de realizare a securității muncii și sunt obligatorii pentru tot personalul asociației, pe întreaga perioadă a desfășurării activităților specifice. Acestea au un domeniu larg de aplicare și sunt destinate a fi respectate în diferite medii de lucru. Ele sunt concepute pentru a proteja sănătatea, siguranța și bunăstarea angajaților, vizitatorilor și a altor persoane implicate în accesarea serviciilor și activităților realizate de organizație.

1.2 MODUL DE REVIZUIRE ȘI COMPLETARE

Instrucțiunile se revizuiesc periodic și se modifică ori de câte ori este necesar, ca urmare a modificărilor de natură legislativă, tehnologică sau neprevăzute. În cazul introducerii de noi operații, echipamente, etc. se completează cu măsurile adecvate la capitolul

corespunzător locului de muncă la care s-au operat modificările.

2 REGULI PENTRU REALIZAREA ACTIVITĂȚII ÎN DEPLINĂ SECURITATE ÎN ACTIVITATEA DE BIROU

- Lucrătorii au obligația să-și desfășoare activitatea de birou în așa fel încât, să nu expună la pericol de accidentare atât propria persoană, cât și celelalte persoane participante la procesul de muncă;
- La plecarea din birouri, lucrătorii vor fi atenți la coborârea scărilor, la deplasarea pe coridoare, evitându-se salturile peste trepte în timpul urcării sau coborârii, să nu execute alte operații ce le distrag atenția în timp ce se deplasează; Se va evita călcarea pe porțiuni alunecoase și pe orice alte obiecte care ar putea provoca alunecări.
- În cazul în care în incinta sediului au loc lucrări de amenajare sau reparații ale spațiilor aferente, se interzice deplasarea lucrătorilor în interiorul zonei de lucru, delimitate sau semnalizate corespunzător.
- Cu excepția cazurilor fortuite, deplasarea în cadrul asociației se va face într-un ritm normal, în special în zona scărilor și a ușilor. Orice deplasare dintr-o încăpere în alta se va efectua atent, cu fața înainte.
- În caz de necesitate, părăsirea locului de muncă se va face conform măsurilor stabilite și pe cât posibil fără panică, cunoscut fiind faptul că panica conduce la o creștere exponențială a consecințelor unor evenimente deosebite.
- Nu se depozitează în birouri substanțe inflamabile și toxice.
- Nu se blochează culoarele și scările de acces cu materiale ce ar împiedica evacuarea bunurilor în caz de incendiu sau intervenție pentru stingere.
- Înainte de folosirea unui scaun, trebuie controlată starea lui, după care se potrivește într-o poziție stabilă, evitându-se așezarea pe marginea lui.
- Este interzisă urcarea pe scaunul cu melc, rotative sau pe alte improvizații, pentru a lua un obiect aflat la înălțime. Pentru această operație, se recomandă un taburet solid, un podium sau o scară corespunzătoare.
- Înainte de îndepărtarea unui scaun de birou, trebuie să se asigure că nu există pericolul de a se răsturna obiecte sau lovi altă persoană.
- Este interzisă mișcarea de legănare pe două din picioarele scaunului deoarece există riscul de răsturnare pe spate.
- Pentru a se evita prinderea degetelor, trebuie apucate bine mânerul atunci când se închid sertarele birourilor sau ușile caselor de bani.
- Trebuie adus la cunoștința conducătorului locului de muncă dacă există piese de mobilier ale cărei margini nu sunt netede sau sunt crăpate, se mișcă sau prezintă defectțiuni.

- Atunci când se folosește un cutter pentru tăierea hârtiei, treb de departe de tăișul lamei.
- În sertare, obiectele tăioase sau ascuțite trebuie aranjate în compartimente separate.
- La producerea unei tăieturi sau răniri se va folosi trusa de prim-ajutor sau se va cere intervenție de specialitate.
- Pentru evitarea împiedicărilor, sertarele birourilor sau ale dulapurilor trebuie ținute închise.
- Înaintea începerii lucrului se verifică starea tehnică a echipamentelor din dotare, precum și existența și funcționalitatea mijloacelor de stingere a incendiilor.
- Remedierea eventualelor defecțiuni depistate va fi executată de către persoane calificate.
- Se va crea un spațiu de muncă ce permite accesul sau/și evacuarea rapidă la/de la locul de muncă al utilizatorilor și al personalului de întreținere.
- Fumatul este permis numai în locurile special amenajate, în conformitate cu legislația în vigoare.
- Se interzice consumul de alimente pe masă, pe suportul calculatorului sau deasupra tastaturii.
- Transportul manual al maselor, atunci când este cazul, nu va depăși 25-30 kg (în funcție de vârstă) pentru bărbați și 12 kg pentru femei.
- Suprafețele căilor de circulație pentru lucrători trebuie să fie netede și nealunecoase. Se va asigura un grad adecvat de curățenie pe jos, în încăperile de lucru și culoare, holuri, grupuri sanitare astfel încât să nu existe pericol de alunecare sau împiedicare.
- Pardoselile din încăperi trebuie să fie întreținute iar urmele de lichide trebuie înlăturate pentru a se evita alunecările. Trebuie semnalate și remediate orice defecțiuni în pardoseli (spărturi sau rupturi de linoleum, covoare, gresie, etc).
- În situații de îngheț, polei, zona de circulație aferentă sediului asociației sau punctului de lucru va fi curățată de zăpadă și se presăra pe jos materiale care să elimine riscul de accidentare prin alunecare.
- Ușile cu geamuri trebuie manevrate atent. Este interzis a se sprijini sau a se împinge sticla ușilor.
- La ieșirea din clădire, orice persoană se va asigura în toate direcțiile pentru a nu fi surprinsă de vreun mijloc de transport.
- În timpul programului trebuie folosită o încălțăminte corespunzătoare pentru a se evita orice sursă de accident.
- Pentru protecția personalului care face curățenie, cioburile de sticlă trebuie învelite și depuse în așa fel încât să poată fi ușor identificate, de preferat fiind să se lase la vedere pe birou.

- La terminarea programului, înainte de părăsirea biroului, tehn sursa de energie electrică, se va stinge lumina și se va verifica incinta pentru a nu exista pericolul declanșării unor incendii.

3 INSTRUCȚIUNI DE SECURITATEA MUNCII LA UTILIZAREA ECHIPAMENTELOR DE BIROU

- Nu se permite nici unui lucrător să utilizeze echipamentele de muncă din dotare fără a respecta instrucțiunile de folosire ale acestora și prezentele instrucțiuni proprii de prevenire și protecție.
- Este interzisă efectuarea de către lucrători a altor activități în afara sarcinilor de muncă (de ex.: schimbarea becurilor arse de către personal neautorizat).
- Orice element de birotică depistat ca defect va fi reparat imediat, iar dacă acest lucru nu este posibil, obiectul va fi retras în magazie, astfel încât să nu se permită folosirea sa în stare defectă și să se elimine astfel posibilitatea producerii unui accident;
- Orice operație de reglare, reparare, întreținere și curățare la un aparat electric se va efectua atunci când s-a întrerupt alimentarea cu energie electrică și după ce au fost deconectate.
- Repararea biroticii se va executa numai de personal calificat și autorizat.
- Lucrătorilor din birouri li se interzice:
 - a) să intervină la tablourile electrice, prize, ștechere, cordoane de alimentare sau la orice alte instalații auxiliare specifice;
 - b) să îndepărteze dispozitivele de protecție;
 - c) să permită intervenția neautorizată asupra echipamentului de muncă;
 - d) continuarea lucrului, atunci când constată o defecțiune.
- Orice fel de reparații la instalațiile electrice (tablou de siguranțe, prize, cabluri defecte etc.) sanitare, de încălzire, gaze și alte asemenea se vor executa prin firme specializate pe bază de comandă.
- Cablurile electrice de alimentare a aparatelor electrice (lămpi de birou, calculatoare etc.) vor fi amplasate astfel încât să se elimine posibilitatea accidentării prin împiedicarea persoanelor. Periodic se va proceda la verificarea integrității acestora și eliminarea oricărui pericol de electrocutare.
- Cordoanele de alimentare ale echipamentelor tehnice trebuie să respecte următoarele condiții:
 - a) să nu prezinte risc de electrocutare prin atingere directă, la trecerea pe planul de lucru sau pe pardoseală;
 - b) să aibă o lungime suficientă pentru a se adapta nevoilor reale și previzibile ale utilizatorilor, fără a fi supus la eforturi de întindere nejustificate;
 - c) să asigure accesul ușor pentru întreținere sau verificare.

- Se interzice utilizarea oricăror echipamente electrice prezentăr sparte sau avariate ca urmare a unor scurtcircuite, arcuri electrice etc., conductori dezizolați sau având izolația deteriorată.
- Este interzisă depozitarea sau amplasarea provizorie la înălțime (pe dulapuri, cuiere, etc.) a unor obiecte care prin cădere pot provoca accidente.
- Instalațiile electrice trebuie să fie bine izolate, iar echipamentele de muncă acționate electric trebuie legate la pământ.
- Este interzis a se scoate ștecherul din priză, trăgându-se de cordon.
- Cordoanele electrice prelungitoare sunt periculoase, putând provoca accidente prin electrocutare, deoarece izolația poate fi deteriorată atunci când suportă o sarcină dură (când se plasează pe acesta piciorul unui scaun sau mese metalice).
- Trebuie să se evite bararea trecerilor cu cordoane electrice.
- Trebuie semnalată orice uzură sau defect care apare la cordonul electric. El va putea fi reutilizat numai după ce a fost reparat sau înlocuit, după caz.
- Este interzis să se atingă sau țină cu mâna un obiect metalic (țeava sau radiatorul caloriferului etc.) în timp ce cu cealaltă mână se introduce ștecherul în priză.
- Este interzis ca operatorii aparatelor de birotică să-și repare singuri echipamentele de muncă cu care lucrează.
- Întreținerea și reglarea lor vor fi efectuate de personal calificat și autorizat.
- Orice operație de reglare, reparare, întreținere și curățare la mașini se va efectua atunci când s-a întrerupt alimentarea cu energie electrică și după ce au fost deconectate.
- Este interzis să se introducă conductoarele direct în priza electrică, fără să se folosească ștecherul, aceste improvizații putând duce la accidente grave prin electrocutare.
- Aparatura de birou trebuie fixată bine pe masa de lucru, pentru a elimina tendința de alunecare și cădere.
- La utilizarea echipamentelor electrice:
 - a) Este interzisă efectuarea de improvizații pentru fixarea echipamentelor.
 - b) Se interzice conectarea echipamentelor la prize defecte sau fără împământare.
 - c) Se interzice îndepărtarea dispozitivelor de protecție ale echipamentelor.

4 REGULI DE SECURITATE ȘI SĂNĂTATE ÎN MUNCĂ LA ORGANIZAREA LOCULUI DE MUNCĂ

- Amenajarea posturilor de lucru într-o încăpere se va realiza astfel încât să se asigure:
 - a) accesul facil al lucrătorului la locul de muncă;

- b) accesul rapid al lucrătorilor de întreținere la toate părțile ec cât posibil fără întreruperea celorlalte activități aflate în desfășurare;
- c) spațiul de lucru necesar facilitării comunicării între persoane și asigurării confidențialității lucrărilor executate.
- Instalațiile de ventilare a aerului nu trebuie să antreneze o creștere peste 3 dB a nivelurilor sonore din încăpere.
 - Resturile menajere sau rezultate în urma operațiilor de igienizare a spațiilor se vor colecta în saci din material plastic, în recipiente etanșe, confecționate din materiale rezistente, evacuarea făcându-se de o unitate de specialitate, înainte ca acestea să depășească capacitatea de depozitare și să intre în descompunere.
 - Prin dimensiunile și amenajarea sa, postul de lucru trebuie să asigure utilizatorului un spațiu suficient, care să îi permită să își schimbe poziția și să varieze mișcările.
 - Iluminatul general și iluminatul local (lămpi de lucru) trebuie să asigure condiții de iluminat satisfăcătoare și un contrast corespunzător între ecran și mediul înconjurător, ținând seama de tipul de activitate și de necesitățile vizuale ale utilizatorului.
 - Strălucirile și reflexiile supărătoare pe ecran sau pe orice alte echipamente trebuie evitate prin amenajarea locului de muncă și a postului de lucru în funcție de amplasarea și caracteristicile tehnice ale surselor de lumină artificială.
 - Posturile de lucru vor fi amenajate astfel încât sursele de lumină, cum ar fi ferestrele și alte deschideri, pereții transparenți sau translucizi, precum și echipamentele și pereții de culori deschise, să nu provoace străluciri orbitoare directe și să antreneze cât mai puțin posibil reflexii pe ecran.
 - Ferestrele trebuie prevăzute cu un sistem adecvat de acoperire, cu posibilități de reglare pentru a atenua lumina naturală la postul de lucru.
 - La amenajarea postului/posturilor de lucru trebuie să se țină seama de zgomotul emis de echipamentul care aparține postului/posturilor de lucru, în special pentru a se evita distragerea atenției sau perturbarea comunicării verbale.
 - Echipamentele care aparțin postului/posturilor de lucru nu trebuie să creeze disconfort lucrătorilor prin producerea de căldură în exces.
 - Toate radiațiile, cu excepția părții vizibile a spectrului electromagnetic, trebuie reduse la niveluri neglijabile în ceea ce privește protecția sănătății și securitatea lucrătorilor.
 - Trebuie să fie atins și menținut un nivel de umiditate corespunzător. Microclimatul va fi strict controlat (să nu se creeze curenți de aer supărători, umiditate mai mare de 40% pentru evitarea uscării mucoaselor).
 - În cazul în care în spațiile de lucru temperatura depășește valoarea de 25°C, se va asigura o viteză de mișcare a aerului de cel puțin 0,5 m/s, indiferent de intensitatea efortului fizic.

5 OBLIGAȚIILE ANGAJATORULUI

- Angajatorul are obligația de a face o analiză a posturilor de lucru pentru a evalua condițiile de securitate și sănătate oferite lucrătorilor, în special în ceea ce privește eventualele riscuri pentru vedere, probleme fizice și solicitare mentală.
- Angajatorul trebuie să ia măsuri corespunzătoare pentru a remedia riscurile constatate ținând cont de efectele suplimentare și/sau combinate ale riscurilor identificate.
- Angajatorul trebuie să informeze lucrătorii cu privire la folosirea zilnică a ecranului de vizualizare, care ar trebui să fie întreruptă periodic prin pauze sau schimbări de activitate, care să reducă suprasolicitarea în fața ecranului de vizualizare.
- Angajatorul trebuie să fie informat despre aspectele legate de securitatea și sănătatea la locul de muncă, în special asupra măsurilor aplicabile funcției angajatului.
- Angajatorul sau reprezentanții acestuia trebuie să fie informați cu privire la toate măsurile de securitate și sănătate.
- Angajatorul informează lucrătorii cu privire la necesitatea realizării examenului corespunzător al ochilor și al vederii, efectuat de o persoană care are competența necesară:
 - a) la intervale regulate, cel puțin o dată în an;
 - b) ori de câte ori apar tulburări de vedere care pot fi cauzate de activitatea la ecranul de vizualizare.

6 INSTRUCȚIUNI DE APĂRARE ÎMPOTRIVA INCENDIILOR ÎN SPAȚIILE CU DESTINAȚIE ADMINISTRATIVĂ (BIROURI)

- În vederea prevenirii incendiilor în birouri este interzis:
 - a) focul deschis;
 - b) folosirea instalațiilor și echipamentelor cu defecțiuni sau improvizații, nerespectarea instrucțiunilor de utilizare ori lăsarea acestora în funcțiune nesupravegheate;
 - c) folosirea unor mijloace de încălzire improvizate sau neomologate (reșouri, radiatoare electrice etc.);
 - d) depozitarea materialelor inflamabile și a altor substanțe ce pot constitui surse de izbucnire a incendiilor;
- Deșeurile de hârtie vor fi colectate în coșuri și evacuate la terminarea programului de activitate.
- La terminarea programului de activitate instalațiile electrice, de regulă, vor fi scoase de sub tensiune.

- În spațiile administrative ale universității, lichidele combustibil păstrate în bidoane metalice, ermetic închise și etichetate (în locuri ferite de posibilitatea izbucnirii unui eventual incendiu,) și numai în cantități de maximum 25
- Curățirea pardoselii (parchet, dușumea, etc.) de regulă se va face cu soluții pe bază de detergenți; în cazuri speciale, se poate face și cu soluții pe bază de diluanți numai la lumina zilei cu respectarea următoarelor reguli:
 - a) Scoaterea de sub tensiune a tuturor aparatelor electrice;
 - b) Stingerea tuturor corpurilor de iluminare electrică;
 - c) Asigurarea ventilației încăperilor respective, prin deschiderea ferestrelor.
 - d) Interzicerea folosirii ustensilelor (găleată, lighean, perie, etc.) din material plastic sau a cârpelor sintetice;
 - e) Interzicerea folosirii soluțiilor de curățat în amestec cu benzină, neofilină, etc.;
 - f) Interzicerea folosirii focului deschis, a fumatului, precum și utilizarea unor obiecte care pot provoca scânteii (brichete, chibrituri, etc).
- Se interzice păstrarea în birouri a materialelor inflamabile și a cârpelor de șters, îmbibate cu ulei, ceară, etc.
- În încăperile pentru birouri, se vor lua măsuri de reducere la minim a pericolului de incendiu, prin limitarea, la strictul necesar, a materialelor combustibile și respectarea celorlaltor reguli stabilite prin dispoziții ale rectorului, cum ar fi fumatul, folosirea focului deschis, etc.
- La terminarea programului de lucru, toate aparatele electrice se vor decupla de la rețeaua electrică a încăperii, interzicându-se depozitarea lor, în stare caldă lângă materialele combustibile.
- Pentru stingerea incendiilor în încăperile administrative ale universității, se va acționa, după caz, cu stingătoare cu gaz, pulbere sau cu apă pulverizată de la hidranții interiori/exteriori.

7 PROTECȚIA DATELOR CU CARACTER PERSONAL

În conformitate cu actele naționale - Constituția Republicii Moldova, Legea privind protecția datelor cu caracter personal nr. 133 din 08.07.2011, Legea privind accesul la informație nr. 982 din 11.05.2000 precum și Convenția pentru protecția persoanelor referitor la prelucrarea automatizată a datelor cu caracter personal ratificată de Republica Moldova prin Hotărîrea Parlamentului № 483-XIV din 2 iulie 1999 și alte acte normative în vigoare și legislația europeană - Convenția Consiliul Europei nr. 108 pentru protecția persoanelor cu privire la prelucrarea automată a datelor cu caracter personal, Angajatorul are obligația de a prelucra în condiții de siguranță și numai pentru scopurile specificate, datele cu caracter personal care îi sunt furnizate.

Asigurarea securității informaționale reprezintă o componentă esențială a activității organizației, aceasta fiind orientate atât asupra asigurării securității mediului fizic cât și

tehnologiilor și sistemelor informaționale utilizate cât și utiliz contextual activităților de prelucrare de date.

Avînd în vedere că siguranța nu poate fi garantată exclusiv cu ajutorul unor sisteme tehnice, prezenta Politică vizează, de asemenea, aspecte de ordin organizatorico-juridic și prezintă modalitatea de asigurare a disponibilității, integrității și confidențialității tuturor informațiilor, inclusiv datelor cu caracter personal prelucrate de organizație, atît în cadrul prelucrării manual cît și automatizate.

- Angajatorul oferă garanții subiecților vizați și declară că asigură protecția drepturilor și libertăților fundamentale ale persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal, și asigură dreptul la inviolabilitatea vieții private.
- Angajatorul își asumă responsabilitatea de a informa subiecții de date despre activitățile de prelucrare realizate în cadrul instituției, scopurile acestora, precum și măsurile de securitate aplicate în contextul activităților de serviciu realizate, ținîndu-se cont de potențialele pericole și riscurile reale la care pot fi expuse datele cu caracter personal ale subiecților vizați.
- Angajatorul va asigura protecția datelor cu caracter personal atît ale angajaților săi, cît și ale beneficiarilor de servicii, inclusiv ale refugiaților.
- Datele cu caracter personal vor fi prelucrate pentru îndeplinirea obligațiilor legale care îi revin organizației, și în conformitate cu art. 5 din Legea nr. 133/2011. În măsura în care sunt necesare categorii speciale de date cu caracter personal, organizația va solicita consimțămîntul în conformitate cu prevederile art. 6 alin. (1) lit. (a), (c), (d), (f) din Legea nr. 133/2011. În activitatea cu beneficiarii de servicii Uniunea va solicita consimțămîntul în conformitate cu prevederile art. 7 Prelucrarea datelor cu caracter personal privind starea de sănătate.
- Orice prelucrare de date cu caracter personal va fi realizată cu respectarea următoarelor principii:
 - a) prelucrarea urmează a fi realizată în mod corect și în conformitate cu prevederile legale;
 - b) colectarea urmează a fi realizată în scopuri determinate, explicite și legitime, iar ulterior să nu fie admisă prelucrarea într-un mod incompatibil cu aceste scopuri. Prelucrarea ulterioară a datelor cu caracter personal în scopuri statistice, de cercetare istorică sau științifică nu este considerată incompatibilă cu scopul colectării dacă se efectuează cu respectarea prevederilor legale și cu respectarea garanțiilor privind prelucrarea datelor cu caracter personal, prevăzute de normele ce reglementează activitatea statistică, cercetarea istorică și cea științifică;
 - c) asigurarea colectării unor date exacte și, dacă este necesar, actualizate. Datele inexacte sau incomplete din punctul de vedere al scopului pentru care sînt colectate și ulterior prelucrate se șterg sau se rectifică;
 - d) stocarea într-o formă care să permită identificarea subiecților datelor cu caracter

personal pe o perioadă care nu va depăși durata necesară

care sînt colectate și ulterior prelucrate datele. Stocarea datelor cu caracter personal pe o perioadă mai mare, în scopuri statistice, se va face cu respectarea garanțiilor privind prelucrarea datelor cu caracter personal, prevăzute de normele ce reglementează aceste domenii, și numai pentru perioada necesară realizării acestor scopuri.

- colectarea datelor cu caracter personal se realizează în următoarele scopuri:
 - a) recrutarea, selectarea și angajarea personalului și ținerea dosarelor salariaților;
 - b) arhivarea dosarelor personale ale salariaților;
 - c) înregistrarea și evidența beneficiarilor;
 - d) păstrarea și arhivarea pachetului de documente al beneficiarilor;
 - e) înregistrarea informațiilor contabile;
 - f) colectarea statistică și raportarea activității organizației.
- În acest sens vor fi colectate date cu caracter personal, care direct sau indirect identifică o persoană fizică, în special prin referire la un număr de identificare (cod personal), la unul sau mai multe elemente specifice proprii identității sale fizice, fiziologice, psihice, economice, culturale sau sociale. Datele cu caracter personal se împart în două categorii: obișnuite și speciale.
- Din categoria specială a datelor cu caracter personal va fi colectată informația care dezvăluie starea de sănătate, precum și cele privind condamnările penale ale unei persoane fizice.
- Din categoria obișnuită a datelor cu caracter personal, pentru angajații organizației, va fi colectată informația care dezvăluie:
 - numele, prenumele;
 - sexul;
 - data și locul nașterii;
 - cetățenia;
 - IDNP;
 - imagine;
 - situația familială;
 - situația militară;
 - datele personale ale membrilor de familie;
 - datele din permisul de conducere;
 - situația economică;
 - situația financiară și datele bancare;
 - semnătura;
 - datele din actele de stare civilă;

- numărul dosarului de pensie;
 - codul personal de asigurării sociale (CPAS);
 - codul asigurării medicale (CPAM);
 - numărul de telefon fix și mobil;
 - adresa (domiciliului/reședinței);
 - adresa de e-mail;
 - profesia și/sau locul de muncă;
 - formarea profesională: diplome – studii;
 - obișnuințele /preferințele /comportamentul.
- Din categoria obișnuită a datelor cu caracter personal, pentru beneficiarii organizației, va fi colectată informația care dezvăluie:
- numele, prenumele;
 - sexul;
 - data și locul nașterii;
 - cetățenia;
 - IDNP;
 - imagine;
 - situația familială;
 - datele personale ale membrilor de familie;
 - semnătura;
 - datele cu privire la starea civilă;
 - codul personal de protecție temporară (TO);
 - numărul de telefon fix și mobil;
 - adresa (domiciliului/reședinței) și de e-mail;
 - profesia și/sau locul de muncă;
 - obișnuințele /preferințele /comportamentul;
 - date cu referire la starea de sănătate sau socială.
- Angajatorul, ținând cont de specificul activității, transpune procedurile și măsurile necesare în vederea asigurării nivelului adecvat de protecție al prelucrării datelor cu caracter personal în cadrul sistemelor de evidență gestionate.
- 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. Toate resursele informaționale care conțin date cu caracter personal, păstrate pe: suporturi magnetice, optice, laser sau alte suporturi ale informației electronice, masive informaționale și baze de date; 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, sunt supuse protecției prin mijloace/procedee specifice.

7.1 Măsurile generale de administrare a securității informaționale

- 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 lemn/metalice care se încuie.
- Computerele, terminalele de acces și imprimantele sînt 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.
- Este asigurată securitatea și accesul fizic la mijloacele de reprezentare a informației care conține date cu caracter personal, în scopul împiedicării vizualizării acestora de către persoane neautorizate.
- 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.
- Toate programele utilizate în cadrul sistemului informatic respectă condițiile de licențiere.
- Este interzisă instalarea programelor de tip Shareware sau freeware, fără aprobarea administratorului sistemului informatic.

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

- Accesul în 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 sau însemnelor corespunzătoare (insigne, ecusoane, cartele de identificare).
- Se asigură administrarea și monitorizarea accesului fizic în toate punctele de acces la sistemele informaționale de date cu caracter personal, inclusiv se reacționează la încălcarea regimului de acces.
- Perimetrul de securitate al organizației reprezintă perimetru oficiilor în care se prelucrează și sau stochează date cu caracter personal.
- 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.
- Amplasarea mijloacelor de prelucrare a datelor cu caracter personal corespund necesității asigurării securității acestora contra accesului nesancționat, furturilor, incendiilor, inundațiilor și altor posibile riscuri.
- Ușile și ferestrele se încuie în cazul în care în încăperea lipsesc membrii.
- Computerele, serverele, alte terminale de acces sînt amplasate în locuri cu acces limitat

- Accesul în perimetrul de securitate al clădirilor unde se prelucrează și/sau stochează date cu caracter personal cu utilaje foto/video neautorizate este interzis, ținând 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 Cerințele față de asigurarea securității datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaționale de date cu caracter personal, aprobate prin Hotărârea Guvernului nr. 1123 din 14 decembrie 2010.
- 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.

7.3 Identificarea și autentificarea

A. Utilizatorilor

- 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 conține semnalmintele nivelului de accesibilitate al utilizatorului.
- Pentru confirmarea ID-ului utilizatorului sînt utilizate parole, mijloace fizice speciale de acces cu memorie (token) sau cartele cu microprocesoare, mijloace biometrice de autentificare, bazate pe caracteristici unice și individuale ale persoanei.
- 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 administratorul I.T.

B. Echipamentului

- Este asigurată posibilitatea identificării și autentificării echipamentului folosit în operațiunile de prelucrare a datelor cu caracter personal, cu menținerea acestor informații pentru o perioadă prelucrării.

7.4 Controlul administrării accesului

Sistematic este efectuat controlul acțiunilor utilizatorilor în vederea evaluării corectitudinii și conformării operațiunilor și acțiunilor efectuate prin intermediul sistemelor informaționale de date cu caracter personal.

A. Accesul de la distanță

- Toate metodele de acces de la distanță la sistemele informaționale de date cu caracter personal sunt securizate (utilizându-se VPN, 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 și permisă doar utilizatorilor, cărora aceasta le este necesar pentru îndeplinirea obiectivelor stabilite.

B. Limitarea folosirii tehnologiilor fără fir

- Accesul fără fir la sistemele informaționale de date cu caracter personal este limitat la maximum, este documentat, supus monitorizării și controlului.
- Accesul fără fir la sistemele informaționale de date cu caracter personal este permis doar în cazul utilizării mijloacelor criptografice de protecție a informației.
- Folosirea tehnologiilor fără fir se autorizează de persoanele responsabile, prin utilizarea unei rețele aparte.

C. 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.
- 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.
- Sunt implementate sisteme automatizate de depistare și semnalizare a incendiilor în birourile unde sînt amplasate sistemele informaționale de date cu caracter personal și mijloacele de prelucrare a datelor cu caracter personal.

D. Controlul vizitatorilor

Vizitatorilor în încăperile unde sunt amplasate date cu caracter personal sunt supravegheați. Accesul vizitatorilor se înregistrează în registre, care se păstrează minimum un an. La expirarea termenului de un an, registrele de înregistrare a vizitatorilor sunt supuse lichidării.

E. Dezvăluirea datelor cu caracter personal

Dezvăluirea formatului electronic al datelor cu caracter personal conținute în sistemele de evidență, prin rețele comunicaționale ori pe alt suport digital de stocare și păstrare, urmează a fi asigurată criptarea acestei informații sau examinarea posibilității utilizării unei conexiuni bilaterale prin canal securizat VPN. 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.).

7.5 Drepturile subiecților de date cu caracter personal

- 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 fi informată cu privire la:
 - identitatea operatorului;
 - scopul concret al prelucrării datelor cu caracter personal colectate;
 - destinatarii 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; dacă răspunsurile la întrebările cu ajutorul cărora se colectează datele sînt obligatorii sau voluntare, inclusiv consecințele posibile ale refuzului de a răspunde la întrebările prin care se colectează informația.
- 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. În acest sens, persoanele responsabile de prelucrarea datelor cu caracter personal, vor asigura accesul persoanei doar la datele cu caracter personal care-o vizează nemijlocit, fiind exclusă posibilitatea consultării datelor cu caracter personal ce vizează alți subiecți, conținute în fișele personale (alte materiale), cu excepția cazurilor în care solicitanții își realizează un interes legitim care nu prejudiciază interesele sau drepturile și libertățile fundamentale ale subiectului datelor cu caracter personal.

7.6 Stocarea, păstrarea și distrugerea datelor cu caracter personal prelucrate

- Accesul în spațiile/perimetrul unde sunt 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 instituționale /regulamentelor departamentale aprobate.
- Stocarea și păstrarea formatului electronic al datelor cu caracter personal, structurate în sisteme de evidență, în computere care sînt conectate la internet, nu sînt echipate cu mijloace de protecție speciale tehnice și de program și nu au instalate programe licențiate, programe antivirus licențiate, sisteme de control al securității soft-ului, de asigurare a efectuării periodice a copiilor de siguranță și de efectuare a auditului - este interzisă.
- Introducerea în perimetrul de securitate instituțional și utilizarea calculatoarelor personale ori a purtătorilor de informații în scopuri de serviciu este interzisă. Mai mult, accesul la computerele din dotare sînt protejate/restricționate prin crearea profilurilor de utilizatori, iar drepturile de administrator sînt încredințate doar persoanei

responsabile din cadrul organizației.

A. Gestionarea incidentelor de securitate

- 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.
- Personalul informează imediat superiorul ierarhic despre incidentele care încalcă securitatea sistemelor informaționale de date cu caracter personal.
- Prelucrarea incidentelor include depistarea, analiza, preîntâmpinarea dezvoltării, înlăturarea lor și restabilirea securității.

7.7 Obligațiile angajaților privind protecția datelor cu caracter personal

Toți angajații organizației au următoarele responsabilități:

- verificarea corectitudinii și actualității informației oferite referitor la propriul dosar de angajare;
- informarea responsabililor referitor la orice schimbare a datelor cu caracter personal;
- colectarea și prelucrarea cu acuratețe a datelor cu caracter personal, în conformitate cu prevederile legale, de către cei care au acces la acest tip de date.

Responsabilitatea pentru asigurarea securității datelor cu caracter personal precum și a informațiilor cu accesibilitate limitată aparține fiecărui angajat.

În caz de nerespectare a dispozițiilor Politicii de securitate persoana împuternicită de către organizație, cât și persoanele responsabile de sistemele de evidență, vor purta răspundere juridică, conform prevederilor Codului civil, Codului contravențional și Codului penal.

8 INSTRUCȚIUNI DE SECURITATE ÎN LUCRUL CU BENEFICIARII DE SERVICII, INCLUSIV CU REFUGIAȚII

Lucrul cu persoanele defavorizate, social vulnerabile, inclusiv persoanele refugiate, implică interacțiuni sensibile și respectuoase cu persoanele care au trecut prin situații dificile și traumatizante. Este important ca personalul organizației să fie conștient de nevoile și vulnerabilitățile acestor persoane și să acționezi într-un mod care să promoveze siguranța și bunăstarea acestora. Iată câteva instrucțiuni de securitate pentru a lucra cu astfel de persoane:

- *Respect și empatie:* Beneficiarii de servicii, inclusiv refugiații necesită a fi abordați întotdeauna cu respect și empatie. Este necesar a depune efort considerabil în a înțelege experiențele acestora și a oferi receptivitate la nevoile și sentimentele lor.
- *Confidențialitate și protecția datelor:* Personalul organizației trebuie să se asigure că protejează datele personale și informațiile sensibile ale beneficiarilor de servicii și ține cont de principiul confidențialității în activitatea pe care o desfășoară. Personalul organizației nu va dezvălui informația personală altor persoane fără acordul explicit al beneficiarilor.

- *Ascultă și înțelege:* Se va oferi spațiu și timp pentru ca beneficiarii să împărtășească povestea lor, dacă doresc să o facă. Angajatul va asculta cu atenție și va încerca să înțeleagă traumele și provocările prin care au trecut aceștia.
- *Non-judecată:* Personalul organizației, în special cel implicat în oferirea de servicii, nu va judeca beneficiarii, care s-au adresat după suport, pentru deciziile sau acțiunile lor anterioare. Este important să se țină cont de faptul că fiecare persoană are o poveste unică și a trecut prin experiențe dificile.
- *Protecție fizică:* Personalul se va asigura că beneficiarii de servicii se simt în siguranță în prezența sa. Dacă există amenințări sau riscuri potențiale, se va informa managerul de servicii, președintele asociației, sau alte autorități competente pentru a asigura protecția fizică a persoanelor în special vulnerabile.
- *Informare corectă:* Personalul necesită a fi informat cu privire la legile și politicile din țara sa referitoare la interacțiunea cu persoanele defavorizate, social vulnerabile, inclusiv persoanele refugiate. În acest context este obligatoriu de a înțelege drepturile și responsabilitățile acestor persoane, beneficiare de servicii, și de a le asigura acces la informații relevante.
- *Colaborare și resurse:* Personalul implicat direct în oferirea de servicii va interacționa cu organizații sau structuri specifice relevante specializate în oferirea asistenței persoanelor defavorizate, social vulnerabile, inclusiv persoanele refugiate, pentru a obține sprijinul și resursele necesare pentru a-i ajuta în procesul de integrare.
- *Conștientizare culturală:* Este important ca personalul implicat direct în oferirea de servicii să înțeleagă necesitățile de bază ale beneficiarilor, iar în cazul persoanelor refugiate să identifice și să înțeleagă nevoile culturale specifice ale acestora și să respecte practicile și tradițiile lor. Doar astfel, se va crea un mediu sigur și inclusiv pentru ei.
- *Sensibilitate culturală:* În cazul interacționării cu persoane de altă etnie, cetățenie, persoane refugiate, personalul organizației necesită a fi conștient de diversitatea culturală a acestor persoane și în acest context ar putea să învețe despre valorile, obiceiurile și tradițiile acestor persoane. La fel se vor evita generalizările și stereotipurile culturale și se va asigura respectarea identității culturale.
- *Limbă și comunicare:* Personalul implicat direct în oferirea de servicii se va asigura ca să dezvolte o comunicare clară și eficientă. În cazul în care există bariere lingvistice, se va solicita suportul colegilor, iar în cazul refugiaților, se vor invita interpreți sau servicii de traducere pentru a facilita comunicarea.
- *Abuz și exploatare:* Personalul implicat direct în oferirea de servicii va fi vigilent și va raporta orice suspiciune de abuz, exploatare sau trafic de persoane, indiferent din partea cui acestea au parvenit. Protejarea beneficiarilor de servicii de astfel de situații este o prioritate.

- *Asistență medicală și psihologică:* Personalul organizației se calitativ direct sau va referi la servicii de asistență medicală și psihologică calificată, beneficiarii de servicii, în special în cazul în care aceștia au trecut prin traume sau au probleme de sănătate fizică și mentală.
- *Integrare și incluziune:* Personalul organizației va sprijini eforturile de integrare și incluziune a beneficiarilor de servicii în comunitate, facilitându-le accesul la educație, locuri de muncă, servicii sociale cât și activități culturale.
- *Rețele de suport:* Personalul organizației va încuraja dezvoltarea rețelelor de suport între beneficiarii de servicii și familia acestora, în cazul refugiaților - între aceștia și comunitatea gazdă. Aceste rețele pot fi extrem de valoroase în procesul de integrare și adaptare.
- *Protecție juridică:* Beneficiarii de servicii vor fi îndrumați către resurse legale și asistență juridică primară și calificată , în dependență de situația cu care se confruntă, pentru a-și cunoaște și proteja drepturile legale.
- *Auto-îngrijire:* Lucrul cu persoanele defavorizate, social vulnerabile, inclusiv persoanele refugiate poate fi solicitant emoțional și psihologic. Managementul organizației se va asigura că personalul posedă metode de a gestiona stresul și sănătatea mentală pentru a se putea implica eficient și în continuare în sprijinirea acestor persoane.
- *Formare și competențe:* Managementul organizației se va asigura că personalul care lucrează cu persoanele defavorizate, social vulnerabile, inclusiv persoanele refugiate au o formare adecvată și cunoștințe relevante pentru a gestiona nevoile specifice ale acestora. Cunoștințele despre problemele specifice și despre resursele disponibile sunt esențiale.

Este important să se țină cont de faptul că fiecare situație și fiecare persoană beneficiară de servicii este unică. Abordarea specialiștilor trebuie să fie individualizată și adaptată nevoilor specifice ale acestora. Dacă personalul nou angajat nu are experiență în lucrul cu astfel de persoane, este întotdeauna recomandat ca în cadrul organizației să fie o persoană ce va putea oferi sprijin și formare specializată acestuia pentru a înțelege mai bine contextul și nevoile beneficiarilor organizației.

NOTĂ: În contextul lucrului cu refugiații, personalul organizației necesită să prezinte o abordare sensibilă, empatică și centrată pe nevoile specifice ale acestora. Personalul necesită a fi pregătit să se adapteze la situațiile diferite și să demonstreze disponibilitatea de a ajuta și de a oferi siguranță și sprijin pe parcursul procesului de refugiere și integrare.

NOTĂ:

1. Prezenta instrucțiune devine document cu răspundere juridică în cadrul asociației din momentul în care este aprobată prin decizia Consiliului de Administrare
2. Acest document, de la data intrării lui în vigoare și până la înlocuirea lui cu un alt document, ca urmare a schimbărilor legislative esențiale în domeniul securității și sănătății în muncă, protecției datelor cu caracter personal la nivel european sau național, este considerat un document de lucru, deci poate fi modificat ca conținut la unele articole, înlocuirea unor articole sau ștergerea acestora în totalitate.
3. Modificările se fac de către persoana desemnată responsabilă de domeniul securitate din cadrul asociației. Modificările de conținut, sau forma nouă a unui articol se realizează prin bararea a articolului respectiv și completarea pe verso a articolului modificat.
4. Modificarea se certifică cu semnătura și ștampila Președintelui/ei și se trece obligatoriu și data la care intră în vigoare noul conținut.
5. Abrogarea conținutului unui articol din prezenta instrucțiune se face de către persoana desemnată în securitatea și sănătatea în muncă din cadrul organizației.
6. Abrogarea se realizează prin bararea articolului respectiv și se certifică cu semnătura și ștampila Președintelui/ei.

Au luat act de cunoștință:

Nr.	Numele, prenumele	Funcția	Data	Semnătura
1.				
2.				
3.				
4.				
5.				
6.				
7.				
8.				
9.				
10.				

11.				
12.				
13.				
14.				
15.				
16.				
17.				
18.				
19.				
20.				
21.				
22.				
23.				
24.				
25.				
26.				
27.				
28.				
29.				
30.				
31.				
32.				
33.				
34.				
35.				
36.				

