PROCEDURĂ DOCUMENTATĂ DE SISTEM

PRIVIND MUNCA ÎN AFARA SEDIULUI ANGAJATORULUI LA NIVELUL CASEI DE CULTURĂ A STUDENȚILOR DIN BUCUREȘTI

1.LISTA RESPONSABILILOR CU ELABORAREA, VERIFICAREA ŞI APROBAREA EDIŢIEI ÎN CADRUL EDIŢIEI PROCEDURII PRIVIND MUNCA ÎN AFARA SEDIULUI ANGAJATORULUI

Nr crt.	Elemente privind responsabilii/ operațiunea	Numele și prenumele	Funcția	Data	Semnătura
0	1	2	3	4	5
1.1.	Elaborat	Gherghina Ioana	Responsabil DPO	14.05.2021	
1.2.	Verificat	Mihai Munteniță	Președinte Comisie SCIM și SNA	14.05.2021	
1.3.	Avizat	Mihai Munteniță	Președinte Comisie SCIM și SNA	17.05.2021	
1.4.	Aprobat	Dorin-Adrian COTEȚ	Directorul Casei de Cultură a Studenților din București	17.05.2021	

2.SITUAŢIA EDIŢIILOR ŞI A REVIZIILOR ÎN CADRUL EDIŢIILOR PROCEDURII PRIVIND MUNCA ÎN AFARA SEDIULUI ANGAJATORULUI

Nr crt.	Ediția sau, după caz, revizia în cadrul ediției	Componenta revizuită	Modalitatea reviziei	Semnătura șefului comp.	Data de la care se aplică prevederile ediției sau reviziei ediției
0	1	2	3	4	5
2.1.	Ediția I	-	-		17.05.2021
2.2.	Revizia 0	-	-		
2.3.	Revizia 1	-	-		
2.4.	Ediția II	-	-		
2.5.	Revizia 0	x	OSGG nr.600/2018		

3.LISTA CUPRINZÂND PERSOANELE LA CARE SE DIFUZEAZĂ EDIȚIA DIN CADRUL EDIȚIEI PROCEDURII PRIVIND MUNCA ÎN AFARA SEDIULUI ANGAJATORULUI

Se difuzează în format electronic fiecărui responsabil cu aplicarea procedurii documentate, conform OSGG nr.600/2018, pentru aprobarea Codului controlului intern managerial al entităților publice.

Nr. crt.	Scopul difuzării	Exemplar nr.	Compartiment	Funcția	Nume și prenume	Data primirii	Data retragerii	Semnătura
	1	2	3	4	5	6		7
3.1.	Aplicare	1	Toate structurile	Salariați CCSB	Lista anexă			
3.2.	Informare	1	Toate structurile	Salariați CCSB	Lista anexă			
3.3.	Evidență	1	Secretariat Comisie SCIM și SNA	Secretar Comisie SCIM și SNA	Lista anexă			
3.4.	Arhivare	1	Secretariat Comisie SCIM și SNA	Secretar Comisie SCIM și SNA	Lista anexă			

1. Scopul procedurii 3

2. Domeniul de aplicare 4

3. Documente de referință (reglementări) 4

3.1. Reglementări internaționale 4

3.2. Legislația primară 4

3.3. Documente interne 4

4. Definiții și abrevieri 4

4.1. Definiții ale termenilor: 4

4.2. Abrevieri ale termenilor 6

5. Descrierea procedurii 6

5.1. Generalități 6

5.1.1. Reglementări legale privind munca la domiciliu - Codului muncii 6

5.1.2. Reglementări legale privind telemunca - Legea 81/2018 7

5.2. Detalierea activităților 9

5.2.1. Munca în afara sediului angajatorului cu echipamente puse la dispoziție de către angajator 9

5.2.2. Responsabilități specifice privind munca în afara sediului angajatorului cu echipamente puse la dispoziție de către angajator 11

Conducătorul entității 11

Responsabilul cu resursele umane 12

Conducătorii departamentelor / compartimentelor / șeful ierarhic superior al salariatului 12

Responsabilul cu gestionarea / mentenanța sistemului informatic 12

Responsabilul cu protecția datelor cu caracter personal 13

Salariați 14

5.2.3. Munca în afara sediului angajatorului cu echipamentele angajatului 15

5.2.2. Responsabilități specifice privind munca în afara sediului angajatorului folosind echipamentele salariatului 17

Conducătorul entității 17

Responsabilul cu resursele umane 18

Conducătorii departamentelor / compartimentelor / șeful ierarhic superior al salariatului 18

Responsabilul cu gestionarea / mentenanța sistemului informatic 18

Responsabilul cu protecția datelor cu caracter personal 19

Salariați 19

5.3. Măsuri tehnice și organizatorice de protecție a datelor cu caracter personal în contextul muncii în afara sediului angajatorului 20

5.3.1. Măsuri de protecție împotriva atacurilor cibernetice 20

5.3.2. Utilizarea dispozitivelor mobile în condiții de securitate 22

5.3.2.1. Protecția datelor cu caracter personal prelucrate pe dispozitive furnizate de Casa de Cultura a Studentilor din Bucuresti 22

5.3.2.2. Protecția datelor cu caracter personal prelucrate pe dispozitive mobile personale 23

5.3.2.3. Utilizarea mesageriei electronice 24

5.3.2.3.1. Trimiterea și primirea mesajelor electronice 25

5.3.2.3.2. Monitorizarea facilităţilor de mesagerie electronică 26
5.3.2.3.3. Folosirea E-mail-ului 27
5.3.3. Acces controlat la sistemul informatic al Casei de Cultura a Studentilor din Bucuresti 28
5.3.3.1. Recomandări de securitate privind accesul la sistemul informatic al Casei de Cultura a Studentilor din Bucuresti 28
5.3.3.1.1. Gestionarea accesului utilizatorilor 29
5.3.3.1.1.1. Înregistrarea şi anularea înregistrării utilizatorului 29
5.3.3.1.1.2. Furnizarea accesului utilizatorilor 30
5.3.3.1.1.3. Eliminarea sau revizuirea drepturilor de acces 30
5.3.3.1.1.4. Administrarea drepturilor de acces privilegiate 31
5.3.3.1.1.5. Autentificarea utilizatorului pentru conexiuni externe 31
5.3.3.1.1.6. Accesul de la distanţă al furnizorului asupra reţelei Casei de Cultura a Studentilor din Bucuresti 31
5.3.3.1.1.7. Recomandări privind stabilirea parolelor de acces 32
5.3.3.1.1.8. Responsabilităţile utilizatorului 32
5.3.3.1.1.9. Evaluarea gradului de securitate şi siguranţă a sistemelor şi aplicaţiilor noi 33
5.4. Recomandări sintetice privind organizarea muncii în alte locaţii decât sediul angajatorului 34

6. Resurse materiale 34

7. Formulare 34
Formular de analiză procedură 34
Formular de distribuire a procedurii 34
Formular de evidenţă a modificărilor procedurii 35

8. Anexe 37
ANEXA 1 Declaraţia angajatului privind însuşirea şi respectarea politicii de securitate a informaţiilor 37
ANEXA 2 Infografic CERT-RO "Recomandări pentru angajatori" 37Error! Bookmark not defined.
ANEXA 3 Infografic CERT-RO "Recomandări pentru angajaţi" 38
ANEXA 4 Model email cu recomandăritrimis de angajatorcătreangajaţi 44

1. Scopul procedurii

1.1. Prezenta procedură stabileşte modul în care se organizează munca salariaţilor Casei de Cultura a Studentilor din Bucuresti în afara sediului angajatorului.
1.2. Scopul acestei proceduri este de a stabili controalele/măsurile care trebuie să fie aplicate atunci când se utilizează dispozitive mobile pentru desfăşurarea activităţii în afara sediului angajatorului.
Se intenţionează să se reducă următoarele riscuri:

- Pierderea sau furtul de dispozitive mobile, inclusiv datele de pe acestea
- Compromiterea informaţiilor protejate
- Introducerea în reţea a virusilor şi a programelor malware
- Pierderea / afectarea reputaţiei angajatorului

1.3. Toate controalele stabilite în această procedură se respectată în orice moment în care se utilizează și se transportă dispozitive mobile din / spre locația unde se desfășoară munca în afara sediului angajatorului.

2. Domeniul de aplicare

2.1. Procedura se aplică de către departamentul / compartimentul de resurseumane al Casei de Cultura a Studentilor din Bucuresti.
2.2. Această procedură se aplică tuturor sistemelor, persoanelor și proceselor care constituie sistemele informatice ale organizației, inclusiv membrii conducerii, directorii, angajații, furnizorii și alte părți terțe care au acces la sistemele Casei de Cultura a Studentilor din Bucuresti.
2.3. Măsurile de protecție a datelor cu caracter personal prevăzute în prezenta procedură se aplică de către conducere și de către toți salariații Casei de Cultura a Studentilor din Bucuresti.

3. Documente de referință (reglementări)

3.1. Reglementări internaționale

- REGULAMENT nr. 679 din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor).

3.2. Legislația primară

- LEGE Nr. 53/2003 din 24 ianuarie 2003 *** Republicată, Codul muncii cu modificările și completările ulterioare;
- Legea nr. 81/2018 privind reglementarea activității de telemuncă;
- Legea nr. 190 din 18 iulie 2018 privind măsuri de punere în aplicare a Regulamentului (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor);
- Ordonanța de Urgență nr. 192/2020 pentru modificarea și completarea Legii nr. 55/2020 privind unele măsuri pentru prevenirea și combaterea efectelor pandemiei de COVID-19, precum și pentru modificarea lit. a) a art. 7 din Legea 81/2018 privind reglementarea activității de telemuncă.

3.3. Documente interne

- ROI / ROF;
- Decizii ale Directorului Casei de Cultura a Studentilor din Bucuresti
- Fișe de post.

4. Definițiișiabrevieri

4.1. Definiții ale termenilor:

Nr. crt.	Termenul	Definiția
1.	Atribuție	Un ansamblu de sarcini de același tip, necesare pentru realizarea unei anumite activități sau a unei părți a acesteia, care se execută periodic sau continuu și care implică cunoștințe specializate pentru realizarea unui obiectiv specific.
2.	BYOD	Bring Your Own Device - metodă de lucru pentru angajați care presupune utilizarea de către salariați a propriilor dispozitive

		mobile pentru desfășurarea activității de telemuncă.
3.	Compartiment	Direcție generală, direcție, departament, serviciu, birou, comisii, inclusiv instituție/structură fără personalitate juridică aflată în subordinea, în coordonarea, sub autoritatea Casei de Cultura a Studentilor din Bucuresti.
4.	Fișa postului	Document care precizează sarcinile și responsabilitățile ce-i revin titularului postului, condițiile de lucru, standardele de performanță, modalitatea de recompensare, precum și caracteristicile personale necesare angajatului pentru îndeplinirea cerințelor postului. Document în care se descrie un post din cadrul unei organizații, precizandu-se rolul acestuia, precum și relațiile profesionale pe care trebuie să le aibă ocupantul postului cu ceilalți angajați în vederea realizării obiectivelor specifice postului respectiv.
5.	Gestionarea documentelor	Procesul de administrare a documentelor unei institutii, pentru a servi intereselor acesteia, pe parcursul întregii lor durate de viață, de la început, prin procesul de creare, revizuire, organizare, stocare, utilizare, partajare, identificare, arhivare și până la distrugerea lor.
6.	Informarea cu privire la clauzele contractului de munca	Obligația angajatorului de a informa persoana selectata în vederea angajării ori, dupăcaz, salariatul, cu privire la clauzele esențiale pe care intenționează să le înscrie în contract sau să le modifice (art. 17 Codul muncii).
7.	Informarea persoanei vizate	Orice informații menționate la articolele 13 și 14 și orice comunicări în temeiul articolelor 15-22 și 34 din Regulamentul 679/2016 referitoare la prelucrare, furnizate persoanei vizate într-o formă concisă, transparentă, inteligibilă și ușor accesibilă, utilizând un limbaj clar și simplu. Informațiile se furnizează în scris sau prin alte mijloace, inclusiv, atunci când este oportun, în format electronic.
8.	Înscris	Act, scrisoare, cerere, notă etc. scris/ă de mână (olograf) sau redactat/ă în format electronic și apoi tipărit/ă în format fizic.
9.	Mijloace ale tehnologiei informației și comunicațiilor	Includ: - Dispozitivele mobile pentru desfășurarea activității de telemuncă: Calculatoare, Laptop-uri, Notebook-uri, Tablete, Smartphone-uri, Smart Watch-uri etc.; - Canale de comunicare: E-mail, aplicații/formulare de transmitere de informații online/prin internet, platforme de comunicare online/prin internet etc.
10.	Munca în afara sediului angajatorului	Munca prestată de salariat în regim de muncă la domiciliu sau de telemuncă.
11.	Munca la domiciliu	Atribuțiile specifice funcției pe care o dețin salariații și care sunt desfășurate la domiciliul salariaților.
12.	Petiție	Cererea, reclamația, sesizarea sau propunerea formulată în scris ori prin poștă electronică, pe care un cetățean, un grup sau o organizație legal constituită o poate adresa instituției.

13.	Telemuncă	Formă de organizare a muncii prin care salariatul, în mod regulat și voluntar, își îndeplinește atribuțiile specifice funcției, ocupației sau meseriei pe care o deține, în alt loc decât locul de muncă organizat de angajator, cel puțin o zi pe lună, folosind tehnologia informației și comunicațiilor.
14.	Telesalariat	Orice salariat care desfășoară activitatea în condiții de telemuncă

4.2. Abrevieri ale termenilor

Nr.crt.	Abrevierea	Termenul abreviat
1.	A	Aprobare
2.	Ah	Arhivare
3.	BYOD	Bring Your Own Device
4.	Ap	Aplicare
5.	E	Elaborare
6.	PO	Procedura operațională
7.	PS	Procedură de sistem
8.	V	Verificat

5. Descrierea procedurii

Prezenta procedură reglementează modul cum se organizează și se desfășoară munca în afara sediului angajatorului, în condiții speciale (pandemie, epidemie, stare de urgență etc.), precum și în condiții normale, în baza deciziei unilaterale a angajatorului privind munca la domiciliu (conform prevederilor art. 48 din Codul muncii), sau prin acordul părților (conform prevederilorLegii 81/2018).

Prezenta procedură reglementează modul cum se folosesc mijloacele tehnologiei informației și comunicațiilor în munca în afara sediului angajatorului.

Prezenta procedură reglementează responsabilitățile părților implicate cu privire la utilizarea și securizarea mijloacelor tehnologiei informației și comunicațiilor în funcție de deținătorul proprietății asupra dispozitivelor mobile cu care se desfășoară munca în afara sediului angajatorului.

5.1. Generalități

5.1.1. Reglementări legale privind munca la domiciliu – Codului muncii

- În vederea îndeplinirii sarcinilor de serviciu ce le revin, salariații cu munca la domiciliu își stabilesc singuri programul de lucru.
- Angajatorul este îndrept să verifice activitatea salariatului cu munca la domiciliu, în condițiile stabilite prin contractul individual de muncă.
- Contractul individual de muncă la domiciliu se încheie numai în formă scrisă și conține, în afara elementelor prevăzute la art. 17 alin. (2), următoarele:

a) Precizarea expresă că salariatul lucrează la domiciliu;
b) Programul în cadrul căruia angajatorul este îndrept să controleze activitatea salariatului său și modalitatea concretă de realizare a controlului;

c) Obligaţia angajatorului de a asigura transportul la şi de la domiciliul salariatului, după caz, al materiilor prime şi materialelor pe care le utilizează în activitate, precum şi al produselor finite pe care le realizează.

- Prin contractele colective de muncă şi/sau prin contractele individuale de muncă se pot stabili şi alte condiţii specifice privind munca la domiciliu, în conformitate cu legislaţia în vigoare.
- Obligaţia de informare a persoanei selectate în vederea angajării sau a salariatului se consideră îndeplinită de către angajator la momentul semnării contractului individual de muncă sau a actului adiţional, după caz.
- Persoana selectată în vederea angajării ori salariatul, după caz, va fi informată cu privire la cel puţin următoarele elemente:

a) Identitatea părţilor;
b) locul de muncă sau, în lipsa unui loc de muncă fix, posibilitatea ca salariatul să muncească în diverse locuri;
c) sediul sau, după caz, domiciliul angajatorului;
d) funcţia/ocupaţia conform specificaţiei Clasificării ocupaţiilor din România sau altor acte normative, precum şi fişa postului, cu specificarea atribuţiilor postului;
e) criteriile de evaluare a activităţii profesionale a salariatului aplicabile la nivelul angajatorului;
f) riscurile specifice postului;
g) data de la care contractul urmează să îşi producă efectele;
h) în cazul unui contract de muncă pe durată determinată sau al unui contract de muncă temporară, durata acestora;
i) durata concediului de odihnă la care salariatul are dreptul;
j) condiţiile de acordare a preavizului de către părţile contractante şi durata acestuia;
k) salariul de bază, alte elemente constitutive ale veniturilor salariale, precum şi periodicitatea plăţii salariului la care salariatul are dreptul;
l) durata normală a muncii, exprimată în ore/zişi ore/săptămână;
m) indicarea contractului colectiv de muncă ce reglementează condiţiile de muncă ale salariatului;
n) durata perioadei de probă.

- Angajatorul poate modifica temporar locul şi felul muncii, fără consimţământul salariatului, şi în cazul unor situaţii de forţă majoră, cu titlu de sancţiune disciplinară sau ca măsură de protecţie a salariatului, încazurile şi în condiţiile prevăzute de Codul muncii.

5.1.2. Reglementări legale privind telemunca - Legea 81/2018

- Activitatea de telemuncă se bazează pe acordul de voinţă al părţilor şi se prevede în mod expres în contractul individual de muncă odată cu încheierea acestuia pentru personalul nou-angajat sau prin act adiţional la contractul individual de muncă existent.
- Refuzul salariatului de a consimţi la prestarea activităţii în regim de telemuncă nu poate constitui motiv de modificare unilaterală a contractului individual de muncă şi nu poate constitui motiv de sancţionare disciplinară a acestuia.
- Învederea îndeplinirii atribuţiilor ce le revin, telesalariaţii organizează programul de lucru de comun acord cu angajatorul, în conformitate cu prevederile contractului individual de muncă, regulamentului intern şi/sau contractului colectiv de muncă aplicabil, în condiţiile legii.
- Angajatorul este îndrept să verifice activitatea telesalariatului, în condiţiile stabilite prin contractul individual de muncă, regulamentul intern şi/sau contractul colectiv de muncă aplicabil, încondiţiile legii.
- În cazul activităţii de telemuncă, contractul individual de muncă conţine, în afara elementelor prevăzute la art. 17 alin. (3) din Legea nr. 53/2003, republicată, cu modificările şi completările ulterioare, următoarele:

a) Precizarea expresă că salariatul lucrează în regim de telemuncă;
b) Perioada și/sau zilele în care telesalariatul își desfășoară activitatea la un loc de muncă organizat de angajator;
c) locul/locurile desfășurării activității de telemuncă, convenite de părți;
d) programul în cadrul căruia angajatorul este îndrept să verifice activitatea telesalariatului și modalitatea concretă de realizare a controlului;
e) modalitatea de evidențierea orelor de muncă prestate de telesalariat;
f) responsabilitățile părților convenite în funcție de locul/locurile desfășurării activității de telemuncă, inclusiv responsabilitățile din domeniul securității și sănătății în muncă;
g) obligația angajatorului de a asigura transportul la și de la locul desfășurării activității de telemuncă al materialelor pe care telesalariatul le utilizează în activitatea sa, după caz;
h) obligația angajatorului de a informa telesalariatul cu privire la dispozițiile din reglementările legale, din contractul colectiv de muncă aplicabil și/sau regulamentul intern, în materia protecției datelor cu caracter personal, precum și obligația telesalariatului de a respecta aceste prevederi;
i) măsurile pe care le ia angajatorul pentru ca telesalariatul să nu fie izolat de restul angajaților și care asigură acestuia posibilitatea de a se întâlni cu colegii în mod regulat;
j) condițiile în care angajatorul suportă cheltuielile aferente activității în regim de telemuncă.

- Prin contractele colective de muncă aplicabile și/sau prin contractele individuale de muncă și regulamentele interne se pot stabili și alte condiții specifice privind telemunca în conformitate cu Legea nr. 53/2003, republicată, cu modificările și completările ulterioare și cu Legea dialogului social nr. 62/2011, republicată, cu modificările și completările ulterioare.
- Angajatorul are următoarele obligații specifice privind securitatea și sănătatea în muncă a telesalariatului:

a) Să asigure mijloacele aferente tehnologiei informației și comunicațiilor și/sau echipamentele de muncă sigure necesare prestării muncii, cu excepția cazului în care părțile convin altfel;
b) Să instaleze, să verifice și să întrețină echipamentul de muncă necesar, cu excepția cazului în care părțile convin altfel;
c) Să asigure condiții pentru ca telesalariatul să primească o instruire suficientă și adecvată în domeniul securității și sănătății în muncă, în special sub formă de informații și instrucțiuni de lucru, specifice locului de desfășurare a activității de telemuncă și utilizării echipamentelor cu ecran de vizualizare: la angajare, la schimbarea locului de desfășurare a activității de telemuncă, la introducerea unui nou echipament de muncă, la introducerea oricărei noi proceduri de lucru.

- Telesalariatul trebuie să își desfășoare activitatea, în conformitate cu pregătirea și instruireasa, precum și cu instrucțiunile primite din partea angajatorului, astfel încât să nu expună la pericol de accidentare sau îmbolnăvire profesională nici propria persoană, nici alte persoane care pot fi afectate de acțiunile sau omisiunile sale întimpul procesului de muncă.
- În mod deosebit, telesalariatul are următoarele obligații:

a) Să informeze angajatorul cu privire la echipamentele de muncă utilizate și la condițiile existente la locurile desfășurării activității de telemuncă și să îi permită acestuia accesul, în măsura în care este posibil, învederea stabilirii și realizării măsurilor de securitate și sănătate în muncă, necesare conform clauzelor din contractul individual de muncă, ori în vederea cercetării evenimentelor;
b) să nu schimbe condițiile de securitate și sănătate în muncă de la locurile în care desfășoară activitatea de telemuncă;

c) să utilizeze numai echipamente de muncă care nu prezintă pericol pentru securitatea şi sănătatea sa;
d) să îşi desfăşoare activitatea cu respectarea dispoziţiilor privind obligaţiile lucrătorilor, aşa cum sunt ele prevăzute în Legea securităţii şi sănătăţii în muncă nr. 319/2006, cu modificările ulterioare, precum şi în conformitate cu clauzele contractului individual de muncă;
e) să respecte regulile specifice şi restricţiile stabilite de către angajator cu privire la reţele de internet folosite sau cu privire la folosirea echipamentului pus la dispoziţie.

- Pentru aplicarea şi verificarea condiţiilor de muncă ale telesalariatului, reprezentanţii organizaţiilor sindicale la nivel de unitate ori reprezentanţii salariaţilor au acces la locurile de desfăşurare a activităţii de telemuncă, în condiţiile stipulate în contractul colectiv de muncă sau contractul individual de muncă ori regulamentul intern, după caz.
- Pentru verificarea aplicării şi respectării cerinţelor legale din domeniul securităţii şi sănătăţii în muncă şi al relaţiilor de muncă, reprezentanţii autorităţilor competente au acces la locurile de desfăşurare a activităţii de telemuncă, în condiţiile stipulate în Legea nr. 108/1999 pentru înfiinţarea şi organizarea Inspecţiei Muncii, republicată, cu modificările ulterioare.
- În cazul în care locul de desfăşurarea activităţii telesalariatului este la domiciliul acestuia, accesul se acordă doar în urma notificării în avans a telesalariatului şi sub rezerva consimţământului acestuia.

5.2. Detalierea activităţilor

5.2.1. Munca în afara sediului angajatorului cu echipamente puse la dispoziţie de către angajator

1. Conducătorul entităţii emite decizia / dispoziţia prin care salariatul / salariaţii îşi desfăşoară activitatea la domiciliu sau încheie un acord cu salariatul pentru telemuncă;
2. Responsabilul cu resursele umane din entitate întocmeşte contractul individual de muncă / actul adiţional la contractul individual de muncă privind modificarea locului de desfăşurare a activităţii angajatului precizând, în condiţiile legii, dacă este muncă la domiciliu sau telemuncă;
3. Conducătorul entităţii / Conducătorii departamentelor / compartimentelor / şeful ierarhic superior al salariatului actualizează fişele de post ale salariaţilor conform modificărilor prevăzute la art. 5.2.1., punctul 2;
4. Conducătorul entităţii dispune modificarea Regulamentului de ordine interioară / întocmirea unei anexe la ROI care să cuprindă toate modificările produse de munca în afara sediului angajatorului;
5. Responsabilul cu resursele umane din entitate prelucrează salariaţilor modificările ROI, întocmeşte procesul verbal şi se asigură ca salariaţii au semnat de luare la cunoştinţă;
6. Conducătorul entităţii emite decizia / dispoziţia prin care stabileşte faptul că salariaţii îşi vor desfăşura activitatea în afara sediului angajatorului cu echipamente puse la dispoziţie de către angajator;
7. Responsabilul cu gestionarea / mentenanţa sistemului informatic al entităţii verifică echipamentele de lucru, implementează sisteme / măsuri de securizare a acestora şi predă echipamentele salariaţilor pe baza de proces-verbal în care va preciza explicit aplicaţiile / programele instalate pe aceste dispozitive;

8. Responsabilul cu gestionarea / mentenanța sistemului informatic al entității întocmește și monitorizează calendarul de verificare a echipamentelor și de schimbare a parolelor de acces pe echipamente;
9. Responsabilul cu gestionarea / mentenanța sistemului informatic al entității semnalează de urgență conducerii orice nerespectare de către salariați a calendarului de schimbare a parolelor de acces pe echipamente;
10. Responsabilul cu gestionarea / mentenanța sistemului informatic al entității întocmește și monitorizează calendarul de efectuare a copiilor de siguranță a datelor personale prelucrate pe respectivul dispozitiv;
11. Responsabilul cu gestionarea / mentenanța sistemului informatic al entității semnalează de urgență conducerii orice nerespectare de către salariați a calendarului de efectuare a copiilor de siguranță a datelor personale prelucrate pe respectivul dispozitiv;
12. Responsabilul cu gestionarea / mentenanța sistemului informatic al entității comunică de urgență conducerii entității și responsabilului cu protecția datelor cu caracter personal orice defecțiune a dispozitivelor mobile care a cauzat întreruperea accesului la datele personale sau a condus la coruperea / distrugerea totală sau parțială a datelor personale;
13. Conducătorul entității dispune măsurile legale împotriva salariatului în conformitate cu Regulamentul intern, dacă, în urma evaluării echipamentului, se constată că defecțiunea dispozitivelor mobile care a produs întreruperea accesului la datele personale sau a condus la coruperea / distrugerea totală sau parțială a datelor personale a fost cauzată de salariat, din neglijență sau cu intenție;
14. Responsabilul cu gestionarea / mentenanța sistemului informatic al entității ia măsuri urgente pentru remedierea defecțiunii și recuperarea / refacerea integrității datelor personale;
15. Responsabilul cu protecția datelor cu caracter personal analizează faptele semnalate de responsabilul cu gestionarea / mentenanța sistemului informatic al entității și, dacă s-a produs o încălcare a securității datelor personale, pune în aplicare prevederile procedurii interne de notificarea ANSPDCP;
16. Responsabilul cu gestionarea / mentenanța sistemului informatic al entității comunică de urgență conducerii entității și responsabilului cu protecția datelor cu caracter personal orice acces / tentativă de acces neautorizat / divulgare neautorizată a datelor cu caracter personal prelucrate pe respectivul dispozitiv;
17. Responsabilul cu gestionarea / mentenanța sistemului informatic al entității ia măsuri urgente pentru securizarea dispozitivului respectiv;
18. Responsabilul cu protecția datelor cu caracter personal analizează faptele semnalate de responsabilul cu gestionarea / mentenanța sistemului informatic al entității și, dacă s-a produs o încălcare a securității datelor personale, pune în aplicare prevederile procedurii interne de notificarea ANSPDCP;
19. Conducătorul entității dispune reinstruirea salariatului în cauză sau a tuturor salariaților cu privire la securizarea dispozitivelor mobile;
20. Responsabilul cu gestionarea / mentenanța sistemului informatic al entității susține sesiunea de instruire dispusă de conducerea entității, întocmește procesul verbal, îl arhivează corespunzător și transmite o copie a acestuia către responsabilul cu protecția datelor cu caracter personal;
21. Responsabilul cu gestionarea / mentenanța sistemului informatic al entității elaborează instrucțiuni privind utilizarea în condiții de securitate a echipamentelor pe care le prelucrează salariaților;

22. Salariații semnează declarația privind însușirea și respectarea politicii de securitate a informațiilor, conform modelului din Anexa 1;
23. Responsabilul cu gestionarea / mentenanța sistemului informatic al entității elaborează procedura de lucru privind securitatea informațiilor în contextul muncii în afara sediului angajatorului și o prelucrează salariaților care semnează procesul verbal de instruire întocmit de responsabilul cu gestionarea / mentenanța sistemului informatic al entității;
24. Responsabilul cu protecția datelor cu caracter personal întocmește materialul de instruire a salariaților cu privire la măsurile tehnice și organizatorice implementate de angajator pentru protecția datelor cu caracter personal în contextul muncii în afara sediului angajatorului. Salariații semnează procesul verbal de instruire întocmit de responsabilul cu protecția datelor cu caracter personal;
25. Conducătorul entității stabilește modalitățile de monitorizare a respectării obligațiilor specifice ale salariaților pe perioada desfășurării activității profesionale în afara sediului angajatorului;
26. Responsabilul cu resursele umane din entitate prelucrează salariaților modalitățile de monitorizare de către angajator a respectării obligațiilor specifice ale salariaților pe perioada desfășurării activității profesionale în afara sediului angajatorului și întocmește procesul-verbal pe care angajații îl semnează;
27. Responsabilul cu gestionarea / mentenanța sistemului informatic al entității activează sistemul de ștergere de la distanță a dispozitivului în cazul în care au încetat raporturile de muncă cu angajatul, indiferent din ce motive, iar acesta refuză să înapoieze imediat angajatorului dispozitivele mobile pe care a lucrat;
28. Conducătorul entității ia toate măsurile legale pentru recuperarea dispozitivelor mobile de la salariații cu care au încetat raporturile de muncă, precum și a datelor personale prelucrate pe acestea;
29. Conducătorul entității solicită sprijinul autorităților competente pentru recuperarea dispozitivelor mobile de la salariații cu care au încetat raporturile de muncă, încazul în care aceștia refuză să le predea benevol;
30. La încetarea raporturilor de muncă, salariații predau dispozitivele mobile, pe bază de proces-verbal, responsabilului cu gestionarea / mentenanța sistemului informatic al entității;
31. Responsabilul cu gestionarea / mentenanța sistemului informatic al entității verifică și schimbă imediat orice credențiale de pe dispozitivele mobile folosite de un angajat cu care au încetat raporturile de muncă.

5.2.2. Responsabilități specifice privind munca în afara sediului angajatorului cu echipamente puse la dispoziție de către angajator

Conducătorul entității

- Emite decizia / dispoziția / încheie acordul prin care salariatul / salariații își desfășoară activitatea în afara sediului angajatorului;
- După caz, actualizează fișele de post ale salariaților conform prevederilor art. 5.2.1., punctul 2 din prezenta procedură;
- Dispunem o dificare a Regulamentului de ordine interioară / întocmirea unei anexe la ROI care să cuprindă toate modificările produse de munca în afara sediului angajatorului;
- Emite decizia / dispoziția prin care stabilește faptul că salariații își vor desfășura activitatea în afara sediului angajatorului cu echipamente puse la dispoziție de către angajator;
- Dispune măsurile legale împotriva salariatului, dacă, în urma evaluării echipamentului, se constată că defecțiunea dispozitivelor mobile care a produs întreruperea accesului la datele

personale sau a condus la coruperea / distrugerea totală sau parţială a datelor personale a fost cauzată de salariat;

- Dispune reinstruirea salariatului în cauză sau a tuturor salariaţilor cu privire la securizarea dispozitivelor mobile;
- Stabileşte modalităţile de monitorizare a respectării obligaţiilor specifice ale salariaţilor pe perioada desfăşurării activităţii profesionale în afara sediului angajatorului.
- Ia toate măsurile legale pentru recuperarea dispozitivelor mobile de la salariaţii cu care au încetat raporturile de muncă, precum şi a datelor personale prelucrate pe acestea;
- Solicită sprijinul autorităţilor competente pentru recuperarea dispozitivelor mobile de la salariaţii cu care au încetat raporturile de muncă, în cazul în care aceştia refuză să le predea benevol.

Responsabilul cu resursele umane

- Întocmeşte contractul individual de muncă / actul adiţional la contractul individual de muncă privind modificarea locului de desfăşurare a activităţii angajatului şi înregistrează modificarea în Reges;
- Prelucrează salariaţilor modificările ROI;
- Întocmeşte procesul verbal şi se asigură ca salariaţii au semnat de luare la cunoştinţă;
- Arhivează corespunzător procesul-verbal;
- Transmite o copie a procesului-verbal către Responsabilul cu protecţia datelor cu caracter personal;
- Prelucrează salariaţilor modalităţile de monitorizare de către angajator a respectării obligaţiilor specifice ale salariaţilor pe perioada desfăşurării activităţii profesionale în afara sediului angajatorului şi întocmeşte procesul-verbal de prelucrare cu privire la aceste măsuri pe care angajaţii îl semnează;
- Arhivează corespunzător procesul-verbal;
- Transmite o copie a procesului-verbal către Responsabilul cu protecţia datelor cu caracter personal.

Conducătorii departamentelor / compartimentelor / şeful ierarhic superior al salariatului

- Actualizează fişele de post ale salariaţilor conform modificărilor prevăzuteîn art. 5.2.1., punctul 2 din prezenta procedură;

Responsabilul cu gestionarea / mentenanţa sistemului informatic

- Verifică echipamentele de lucru, implementează sisteme / măsuri de securizare a acestora;
- Predă echipamentele salariaţilor pe baza de proces-verbal în care precizează explicit aplicaţiile / programele instalate pe aceste dispozitive;
- Arhivează corespunzător procesul-verbal;
- Transmite o copie a procesului-verbal către Responsabilul cu protecţia datelor cu caracter personal;
- Întocmeşte şi monitorizează calendarul de verificare a echipamentelor şi de schimbare a parolelor de acces pe echipamente;
- Semnalează de urgenţă conducerii orice nerespectare de către salariaţi a calendarului de verificare a echipamentelor şi de schimbare a parolelor de acces pe echipamente de către salariaţi;
- Întocmeşte şi monitorizează calendarul de efectuare a copiilor de siguranţă a datelor personale prelucrate pe respectivul dispozitiv;
- Semnalează de urgenţă conducerii orice nerespectare de către salariaţi a calendarului de efectuare a copiilor de siguranţă a datelor personale prelucrate pe respectivul dispozitiv;

- Comunică de urgență conducerii entității și responsabilului cu protecția datelor cu caracter personal orice defecțiune a dispozitivelor mobile care a cauzat întreruperea accesului la datele personale sau a condus la coruperea / distrugerea totală sau parțială a datelor personale;
- Ia măsuri urgente pentru remedierea defecțiunii și recuperarea / refacerea integrității datelor personale;
- Comunică de urgență conducerii entității și responsabilului cu protecția datelor cu caracter personal orice acces / tentativă de acces neautorizat / divulgare neautorizată a datelor cu caracter personal prelucrate pe respectivul dispozitiv;
- Ia măsuri urgente pentru securizarea dispozitivului respectiv;
- Susține sesiunea de reinstruire cu privire la securizarea dispozitivelor mobile dispusă de conducerea entității,
- Întocmește procesul verbal pe care salariatul / salariații îl semnează;
- Arhivează corespunzător procesul-verbal;
- Transmite o copie a procesului-verbal către responsabilul cu protecția datelor cu caracter personal;
- Elaborează instrucțiuni privind utilizarea în condiții de securitate a echipamentelor utilizate în munca în afara sediului angajatorului;
- Prelucrează salariaților instrucțiunile privind utilizarea în condiții de securitate a echipamentelor folosite în munca în afara sediului angajatorului;
- Întocmește procesul-verbal de prelucrare către salariați a instrucțiunilor privind utilizarea în condiții de securitate a echipamentelor folosite în munca în afara sediului angajatorului;
- Arhivează corespunzător procesul-verbal;
- Transmite o copie a procesului-verbal către Responsabilul cu protecția datelor cu caracter personal;
- Elaborează procedura de lucru privind securitatea informațiilor în contextul muncii în afara sediului angajatorului;
- Prelucrează salariaților procedura de lucru privind securitatea informațiilor în contextul muncii în afara sediului angajatorului;
- Întocmește procesul verbal de instruire a salariaților privind procedura de lucru privind securitatea informațiilor în contextul muncii în afara sediului angajatorului;
- Arhivează corespunzător procesul-verbal;
- Transmite o copie a procesului-verbal către Responsabilul cu protecția datelor cu caracter personal;
- Activează sistemul de ștergere de la distanță a dispozitivului în cazul în care au încetat raporturile de muncă cu angajatul, indiferent din ce motive, iar acesta refuză să înapoieze imediat angajatorului dispozitivele mobile pe care a lucrat;
- Verifică și schimbă imediat orice credențiale de pe dispozitivele mobile folosite de un angajat cu care s-au încetat raporturile de muncă.

Responsabilul cu protecția datelor cu caracter personal

- Întocmește materialul de instruire a salariaților cu privire la măsurile tehnice și organizatorice implementate de angajator pentru protecția datelor cu caracter personal în contextul muncii în afara sediului angajatorului;
- Arhivează corespunzător procesul-verbal;
- Arhivează corespunzător copia procesului-verbal semnat de luare la cunoștință de către salariați privind modificările ROI transmis de responsabilul cu resursele umane;
- Arhivează corespunzător copia procesului verbal semnat de luare la cunoștință de către salariați privind modalitățile de monitorizare de către angajator a respectării obligațiilor

specifice ale salariaților pe perioada desfășurării activității profesionale în afara sediului angajatorului, transmis de responsabilul cu resursele umane;

- Arhivează corespunzător copia procesului-verbal de predare-primire a dispozitivelor mobile către salariați, transmis de responsabilul cu gestionarea / mentenanța sistemului informatic al entității;
- Analizează faptele semnalate de responsabilul cu gestionarea / mentenanța sistemului informatic al entității și, dacă s-a produs o încălcare a securității datelor personale prin defectarea dispozitivelor mobile, pune în aplicare prevederile procedurii interne de notificarea ANSPDCP;
- Arhivează corespunzător copia procesului-verbal de reinstruire a salariatului / salariaților cu privire la securizarea dispozitivelor mobile, transmis de responsabilul cu gestionarea / mentenanța sistemului informatic al entității;
- Analizează faptele semnalate de responsabilul cu gestionarea / mentenanța sistemului informatic al entitățiișI, dacă s-a produs o încălcare a securității datelor personale prin nerespectarea de către salariat a măsurilor de securizare a dispozitivelor mobile și, dacă s-a produs o încălcare a securității datelor personale, pune în aplicare prevederile procedurii interne de notificarea ANSPDCP;
- Arhivează corespunzător copia procesului-verbal de prelucrare către salariați a instrucțiunilor privind utilizarea în condiții de securitate a echipamentelor folosite în munca în afara sediului angajatorului, transmis de responsabilul cu gestionarea / mentenanța sistemului informatic al entității;
- Arhivează corespunzător copia procesului-verbal de instruire a salariaților cu privire la procedura privind securitatea informațiilor în contextul muncii în afara sediului angajatorului, transmis de responsabilul cu gestionarea / mentenanța sistemului informatic al entității.

Salariați

- Semnează procesul-verbal de luare la cunoștință modificările ROI;
- Participă la sesiunile de instruire și semnează procesul-verbal de instruire cu privire la modalitățile de monitorizare de către angajator a respectării obligațiilor specifice ale salariaților pe perioada desfășurării activității profesionale în afara sediului angajatorului;
- Semnează procesul-verbal de predare-primire a echipamentelor / dispozitivelor mobile puse la dispoziție de angajator pentru munca în afara sediului angajatorului;
- Respectă calendarul de verificare a echipamentelor și de schimbare a parolelor de acces pe echipamente;
- Respectă calendarul de efectuare a copiilor de siguranță a datelor personale prelucrate pe dispozitivele mobile puse la dispoziție de angajator pentru munca în afara sediului angajatorului;
- Notifică de urgență responsabilul cu gestionarea / mentenanța sistemului informatic al entității despre orice defecțiune a dispozitivelor mobile care a cauzat în treruperea accesului la datele personale sau a condus la coruperea / distrugerea totală sau parțială a datelor personale;
- Notifică de urgență responsabilul cu protecția datelor personale despre orice acces / tentativă de acces neautorizat / divulgare neautorizată a datelor cu caracter personal prelucrate pe dispozitivele mobile puse la dispoziție de angajator pentru munca în afara sediului angajatorului;
- Semnează declarația privind însușirea și respectarea politicii de securitate a informațiilor, conform modelului din Anexa 1;

- Participă la sesiunile de instruire și semnează procesul-verbal de instruire cu privire la măsurile tehnice și organizatorice implementate de angajator pentru protecția datelor cu caracter personal în contextul muncii în afara sediului angajatorului;
- Respectă toate măsurile tehnice și organizatorice pentru care au fost instruiți;
- Participă la sesiunea de instruire și semnează procesul verbal de instruire a salariaților privind procedura de lucru privind securitatea informațiilor în contextul muncii în afara sediului angajatorului;
- La încetarea raporturilor de muncă, predau dispozitivele mobile, pe bază de proces-verbal, responsabilului cu gestionarea / mentenanța sistemului informatic al entității.

5.2.3. Munca în afara sediului angajatorului cu echipamentele angajatului

1. Conducătorul entității emite decizia / dispoziția prin care salariatul / salariații își desfășoară activitatea în afara sediului angajatorului folosind dispozitivele mobile personale ale angajaților;
2. Conducerea entității încheie contract de comodat / de închiriere cu salariatul pentru dispozitivele mobile personale ale acestuia ce urmează a fi utilizate pentru munca în afara sediului angajatorului;
3. În măsura în care este posibil, pentru munca în afara sediului angajatorului se va solicita salariatului să pună la dispoziția acestuia dispozitive mobile care nu conțin date personale / spații de lucru personale ale salariatului;
4. În cazul în care nu este posibil ca salariatul să pună la dispoziția angajatorului dispozitive mobile care nu conțin date personale / spații de lucru personale ale salariatului, acesta semnează o declarație prin care își asumă faptul că este restricționat accesul oricărei persoane (familie, rude, prieteni, cunoștințe etc.) la dispozitivul mobil personal pus la dispoziția angajatorului;
5. Responsabilul cu resursele umane din entitate întocmește contractul individual de muncă / actul adițional la contractul individual de muncă privind modificarea locului de desfășurarea activității angajatului;
6. Conducătorul entității / Conducătorii departamentelor / compartimentelor / șeful ierarhic superior al salariatului actualizează fișele de post ale salariaților conform modificărilor prevăzute la art. 5.2.1., punctul 2;
7. Conducătorul entității dispune modificarea Regulamentului de ordine interioară / întocmirea unei anexe la ROI care să cuprindă toate modificările produse de munca în afara sediului angajatorului;
8. Responsabilul cu resursele umane din entitate prelucrează salariaților modificările ROI, întocmește procesul verbal și se asigură ca salariații au semnat de luare la cunoștință;
9. Conducătorul entității emite decizia / dispoziția prin care stabilește faptul căsalariații își vor desfășura activitatea în afara sediului angajatorului cu echipamentele personale ale salariaților;
10. Responsabilul cu gestionarea / mentenanța sistemului informatic al entității verifică echipamentele de lucru puse la dispoziție de salariați, creează un spațiu de lucru pe dispozitivul salariatului, special dedicat muncii în afara sediului angajatorului și implementează sisteme / măsuri de securizare a acestora, inclusiv posibilitatea ștergerii de la distanță a dispozitivului în caz de pierdere, furt sau încetare a raporturilor de muncă cu salariatul. Întocmește procesul-verbal în care va preciza explicit operațiunile efectuate pe dispozitivul salariatului și aplicațiile / programele instalate pe aceste dispozitive;

11. Responsabilul cu gestionarea / mentenanța sistemului informatic al entității întocmește și monitorizează calendarul de verificare a echipamentelor și de schimbare a parolelor de acces pe spațiul de lucru special dedicat pe dispozitiv muncii în afara sediului angajatorului;
12. Responsabilul cu gestionarea / mentenanța sistemului informatic al entității semnalează de urgență conducerii orice nerespectare de către salariați a calendarului de verificare a dispozitivului și de schimbare a parolelor de acces pe spațiul de lucru special dedicat pe dispozitivul salariatului pentru munca în afara sediului angajatorului;
13. Responsabilul cu gestionarea / mentenanța sistemului informatic al entității întocmește și monitorizează calendarul de efectuare a copiilor de siguranță a datelor personale prelucrate pe spațiul de lucru special dedicat pe dispozitivul salariatului pentru munca în afara sediului angajatorului;
14. Responsabilul cu gestionarea / mentenanța sistemului informatic al entității semnalează de urgență conducerii orice nerespectare de către salariați a calendarului de efectuare a copiilor de siguranță a datelor personale prelucrate pe dispozitivul salariatului pentru munca în afara sediului angajatorului;
15. Responsabilul cu gestionarea / mentenanța sistemului informatic al entității comunică de urgență conducerii entității și responsabilului cu protecția datelor cu caracter personal orice defecțiune a dispozitivelor mobile ale salariatului care a cauzat întreruperea accesului la datele personale sau a condus la coruperea / distrugerea totală sau parțială a datelor personale;
16. Conducătorul entității dispune măsurile legale împotriva salariatului în conformitate cu Regulamentul intern, dacă, în urma evaluării echipamentului, se constată că defecțiunea dispozitivelor mobile care a produs în treruperea accesului la datele personale sau a condus la coruperea / distrugerea totală sau parțială a datelor personale a fost cauzată de salariat, din neglijență sau cu intenție;
17. Remedierea defecțiunii și recuperarea / refacerea integrității datelor personale cade în sarcina responsabilului cu gestionarea / mentenanța sistemului informatic al entității, sau, în cazul în care defecțiunea nu poate fi remediată de acesta și se folosesc servicii externalizate specializate, responsabilul cu gestionarea / mentenanța sistemului informatic al entități va șterge datele personale ale angajatorului de pe dispozitivsau le vacripta/securiza, înainte de a trimite dispozitivul la reparat, în așa fel încât datele să nu poată fi accesate în timpul reparației;
18. Responsabilul cu protecția datelor cu caracter personal analizează faptele semnalate de responsabilul cu gestionarea / mentenanța sistemului informatic al entității și, dacă s-a produs o încălcare a securității datelor personale, pune în aplicare prevederile procedurii interne de notificarea ANSPDCP;
19. Responsabilul cu gestionarea / mentenanța sistemului informatic al entității comunică de urgență conducerii entității și responsabilului cu protecția datelor cu caracter personal orice acces / tentativă de acces neautorizat / divulgare neautorizată a datelor cu caracter personal prelucrate pe spațiul de lucru creat pe dispozitivul salariatului pentru munca în afara sediului angajatorului;
20. Responsabilul cu gestionarea / mentenanța sistemului informatic al entitățiii a măsuri urgente pentru securizare a dispozitivului respectiv;
21. Responsabilul cu protecția datelor cu caracter personal analizează faptele semnalate de responsabilul cu gestionarea / mentenanța sistemului informatic al entității și, dacă s-a produs o încălcare a securității datelor personale, pune în aplicare prevederile procedurii interne de notificarea ANSPDCP;

22. Conducătorul entității dispune reinstruirea salariatului în cauză sau a tuturor salariaților cu privire la securizarea dispozitivelor mobile;
23. Responsabilul cu gestionarea / mentenanța sistemului informatic al entității susține sesiunea de instruire dispusă de conducerea entității, întocmește procesul verbal, îl arhivează corespunzător și transmite o copie a acestuia către responsabilul cu protecția datelor cu caracter personal;
24. Responsabilul cu gestionarea / mentenanța sistemului informatic al entității elaborează instrucțiuni privind utilizarea în condiții de securitate a echipamentelor pe care le prelucrează salariaților;
25. Salariații semnează declarația privind însușirea și respectarea politicii de securitate a informațiilor, conform modelului din Anexa 1;
26. Responsabilul cu gestionarea / mentenanța sistemului informatic al entității elaborează procedura de lucru privind securitatea informațiilor în contextul muncii în afara sediului angajatorului și o prelucrează salariaților care semnează procesul verbal de instruire întocmit de responsabilul cu gestionarea / mentenanța sistemului informatic al entității;
27. Responsabilul cu protecția datelor cu caracter personal întocmește materialul de instruire a salariaților cu privire la măsurile tehnice și organizatorice implementate de angajator pentru protecția datelor cu caracter personal în contextul muncii în afara sediului angajatorului. Salariații semnează procesul verbal de instruire întocmit de responsabilul cu protecția datelor cu caracter personal;
28. Conducătorul entității stabilește modalitățile de monitorizare a respectării obligațiilor specifice ale salariaților pe perioada desfășurării activității profesionale în afara sediului angajatorului;
29. Responsabilul cu resursele umane din entitate prelucrează salariaților modalitățile de monitorizare de către angajator a respectării obligațiilor specifice ale salariaților pe perioada desfășurării activității profesionale în afara sediului angajatorului și întocmește procesul-verbal pe care angajații îl semnează.

5.2.2. Responsabilități specifice privind munca în afara sediului angajatorului folosind echipamentele salariatului

Conducătorul entității

- Emite decizia / dispoziția prin care salariatul / salariații își desfășoară activitatea în afara sediului angajatorului folosind dispozitivele mobile personale ale angajaților;
- Încheie contract de comodat / de închiriere cu salariatul pentru dispozitivele mobile personale ale acestuia ce urmează a fi utilizate pentru munca în afara sediului angajatorului;
- În măsura în care este posibil, pentru munca în afara sediului angajatorului, solicită salariatului să pună la dispoziție dispozitive mobile care nu conțin date personale / spații de lucru personale ale acestuia;
- Actualizează fișele de post ale salariaților conform modificărilor prevăzute la art. 5.2.1., punctul 2;
- Dispune modificarea Regulamentului de ordine interioară / întocmire a unei anexe la ROI care să cuprindă toate modificările produse de munca în afara sediului angajatorului;
- Emite decizia / dispoziția prin care stabilește faptul că salariații își vor desfășura activitatea în afara sediului angajatorului cu echipamentele personale ale salariaților;
- Dispune măsurile legale împotriva salariatului, în conformitate cu Regulamentul intern, dacă, în urma evaluării echipamentului, se constată că defecțiunea dispozitivelor mobile care a produs întreruperea accesului la datele personale sau a condus la coruperea / distrugerea totală sau parțială a datelor personale a fost cauzată de salariat, din neglijență sau cu intenție;

- Dispune reinstruirea salariatului în cauză sau a tuturor salariaților cu privire la securizarea dispozitivelor mobile;
- Stabilește modalitățile de monitorizare a respectării obligațiilor specifice ale salariaților pe perioada desfășurării activității profesionale în afara sediului angajatorului.

Responsabilul cu resursele umane

- Întocmește contractul individual de muncă / actul adițional la contractul individual de muncă privind modificarea locului de desfășurare a activității angajatului;
- Prelucrează salariaților modificările ROI, întocmește procesul verbal și se asigură ca salariații au semnat de luare la cunoștință;
- Arhivează corespunzător procesul-verbal și transmite o copie către responsabilul cu protecția datelor personale;
- Prelucrează salariaților modalitățile de monitorizare de către angajator a respectării obligațiilor specifice ale salariaților pe perioada desfășurării activității profesionale în afara sediului angajatorului și întocmește procesul-verbal pe care angajații îl semnează.
- Arhivează corespunzător procesul-verbal și transmite o copie către responsabilul cu protecția datelor personale.

Conducătorii departamentelor / compartimentelor / șeful ierarhic superior al salariatului

- Actualizează fișele de post ale salariaților conform modificărilor prevăzute în art. 5.2.1., punctul 2 din prezenta procedură;

Responsabilul cu gestionarea / mentenanța sistemului informatic

- Verifică echipamentele de lucru puse la dispoziție de salariați, creează un spațiu de lucru pe dispozitivul salariatului, special dedicat muncii în afara sediului angajatorului și implementează sisteme / măsuri de securizarea acestora, inclusiv posibilitatea ștergerii de la distanță a dispozitivului în caz de pierdere, furt sau încetare a raporturilor de muncă cu salariatul. Întocmește procesul-verbal în care va preciza explicit operațiunile efectuate pe dispozitivul salariatului și aplicațiile / programele instalate pe aceste dispozitive;
- Întocmește și monitorizează calendarul de verificare a echipamentelor și de schimbare a parolelor de acces pe spațiul de lucru special dedicat pe dispozitiv muncii în afara sediului angajatorului;
- Semnalează de urgență conducerii orice nerespectare de către salariați a calendarului de verificare a dispozitivului și de schimbare a parolelor de acces pe spațiul de lucru special dedicat pe dispozitivul salariatului pentru munca în afara sediului angajatorului;
- Întocmește și monitorizează calendarul de efectuare a copiilor de siguranță a datelor personale prelucrate pe spațiul de lucru special dedicat pe dispozitivul salariatului pentru munca în afara sediului angajatorului;
- Semnalează de urgență conducerii orice nerespectare de către salariați a calendarului de efectuare a copiilor de siguranță a datelor personale prelucrate pe dispozitivul salariatului pentru munca în afara sediului angajatorului;
- Comunică de urgență conducerii entității și responsabilului cu protecția datelor cu caracter personal orice defecțiune a dispozitivelor mobile ale salariatului care a cauzat întreruperea accesului la datele personale sau a condus la coruperea / distrugerea totală sau parțială a datelor personale;
- Remediază defecțiunea și recuperează / reface integritatea datelor personale;
- În cazul în care nu poate remedia defecțiunea și se folosesc servicii externalizate specializate, șterge datele personale ale angajatorului de pe dispozitiv sau le criptează / securizează, înainte

de a trimite dispozitivul la reparat, în așa fel încât datele să nu poată fi accesate în timpul reparației;

- Comunică de urgență conducerii entității și responsabilului cu protecția datelor cu caracter personal orice acces / tentativă de acces neautorizat / divulgare neautorizată a datelor cu caracter personal prelucrate pe spațiul de lucrucreat pe dispozitivul salariatului pentru munca în afara sediului angajatorului;
- Ia măsuri urgente pentru securizarea dispozitivului respectiv;
- Susține sesiunea de instruire dispusă de conducerea entității, întocmește procesul verbal, îl arhivează corespunzător și transmite o copie a acestuia către responsabilul cu protecția datelor cu caracter personal;
- Elaborează instrucțiuni privind utilizarea în condiții de securitatea echipamentelor pe care le prelucrează salariaților;
- Elaborează procedura de lucru privind securitatea informațiilor în contextul muncii în afara sediului angajatorului și o prelucrează salariaților care semnează procesul verbal de instruire întocmit de responsabilul cu gestionarea / mentenanța sistemului informatic al entității.

Responsabilul cu protecția datelor cu caracter personal

- Întocmește materialul de instruire a salariaților cu privire la măsurile tehnice și organizatorice implementate de angajator pentru protecția datelor cu caracter personal în contextul muncii în afara sediulu angajatorului;
- Arhivează corespunzător procesul-verbal;
- Arhivează corespunzător copia procesului-verbal semnat de luare la cunoștință de către salariați privind modificările ROI transmis de responsabilul cu resursele umane;
- Arhivează corespunzător copia procesului verbal semnat de luare la cunoștință de către salariați privind modalitățile de monitorizare de către angajator a respectării obligațiilor specifice ale salariaților pe perioada desfășurării activității profesionale în afara sediului angajatorului, transmis de responsabilul cu resursele umane;
- Arhivează corespunzător copia procesului-verbal în care responsabilul cu gestionarea / mentenanța sistemului informatic al entității precizează explicit operațiunile efectuate pe dispozitivul salariatului și aplicațiile / programele instalate pe aceste dispozitive;
- Analizează faptele semnalate de responsabilul cu gestionarea / mentenanța sistemului informatic al entității și, dacă s-a produs o încălcare a securității datelor personale, pune în aplicare prevederile procedurii interne de notificarea ANSPDCP;
- Arhivează corespunzător copia procesului-verbal de reinstruire a salariatului / salariaților cu privire la securizarea dispozitivelor mobile, transmis de responsabilul cu gestionarea / mentenanța sistemului informatic al entității;
- Arhivează corespunzător copia procesului-verbal de prelucrare către salariați a instrucțiunilor privind utilizarea în condiții de securitate a echipamentelor utilizate în munca în afara sediului angajatorului transmis de responsabilul cu gestionarea / mentenanța sistemului informatic al entității;
- Arhivează corespunzător copia procesului-verbal de instruire a salariaților cu privire la procedura privind securitatea informațiilor în contextul muncii în afara sediului angajatorului, transmis de responsabilul cu gestionarea / mentenanța sistemului informatic al entității.

Salariați

- Încheie contract de comodat / de închiriere cu angajatorul pentru dispozitivele mobile ce urmează a fi utilizate pentru munca în afara sediului angajatorului;

- În măsura în care este posibil, pentru munca în afara sediului angajatorului, pune la dispoziția acestuia dispozitive mobile care nu conțin date personale / spații de lucru personale;
- În cazul în care nu este posibil să pună la dispoziția angajatorului dispozitive mobile care nu conțin date personale / spații de lucru personale, semnează o declarație prin care își asumă faptul că este restricționat accesul oricărei persoane (familie, rude, prieteni, cunoștințe etc.) la dispozitivul mobil personal pus la dispoziția angajatorului;
- Semnează contractul individual de muncă / actul adițional la contractul individual de muncă privind modificarea locului de desfășurare a activității angajatului;
- Semnează fișa de post actualizată conform modificărilor prevăzute la art. 5.2.1., punctul 2;
- Semnează procesul-verbal privind modificările ROI;
- Semnează procesul-verbal de predare-primire a dispozitivului mobil în care se precizează explicit operațiunile efectuate pe dispozitivul salariatului și aplicațiile / programele instalate pe aceste dispozitive;
- Respectă calendarul de verificare a echipamentelor și de schimbare a parolelor de acces pe spațiul de lucru special dedicat pe dispozitiv muncii în afara sediului angajatorului;
- Respectă calendarul de efectuare a copiilor de siguranță a datelor personale prelucrate pe spațiul de lucru special dedicat pentru munca în afara sediului angajatorului;
- Comunică de urgență responsabilului cu gestionarea / mentenanța sistemului informatic al entității orice defecțiune a dispozitivelor mobile care a cauzat întreruperea accesului la datele personale sau a condus la coruperea / distrugerea totală sau parțială a datelor personale;
- Comunică de urgență responsabilului cu gestionarea / mentenanța sistemului informatic al entității orice acces / tentativă de acces neautorizat / divulgare neautorizată a datelor cu caracter personal prelucrate pe spațiul de lucru creat pe dispozitivul salariatului pentru munca în afara sediului angajatorului;
- Pune de urgență la dispoziția responsabilului cu gestionarea / mentenanța sistemului informatic al entității dispozitivului pentru securizarea corespunzătoare a acestuia;
- Participă la sesiunea de reinstruire dispusă de conducătorul entității cu privire la securizarea dispozitivelor mobile și semnează procesul-verbal de instruire;
- Ia la cunoștința și respectă instrucțiunile privind utilizare a în condiții de securitate a echipamentelor;
- Semnează declarația privind însușirea și respectarea politicii de securitate a informațiilor, conform modelului din Anexa 1;
- Participă la sesiunea de instruire și semnează procesul-verbal de instruire cu privire la prevederile procedurii de lucru privind securitatea informațiilor în contextul muncii în afara sediului angajatorului;
- Participă la sesiunea de instruire și semnează procesul-verbal de instruire cu privire la măsurile tehnice și organizatorice implementate de angajator pentru protecția datelor cu caracter personal în contextul muncii în afara sediului angajatorului;
- Participă la sesiunea de instruire și semnează procesul-verbal de instruire cu privire la modalitățile de monitorizare de către angajator a respectării obligațiilor specifice ale salariaților pe perioada desfășurării activității profesionale în afara sediului angajatorului.

5.3. Măsuri tehnice și organizatorice de protecție a datelor cu caracter personal în contextul muncii în afara sediului angajatorului

5.3.1. Măsuri de protecție împotriva atacurilor cibernetice

- Nu se deschid fișierele primite prin e-mail decât în situația în care se cunoaște expeditorul iar, în cazul unei suspiciuni se va anunța de urgență personalului de specialitate;

- Nu se accesează "ofertele" irezistibile din mediul online, indiferent de forma prin care se primesc (email, whatsapp, messenger, facebook etc.)
- Backup-ul fișierelor se efectuează pe un dispozitiv care nu este conectat la rețea;
- Dispozitivele utilizate pentru navigare online sunt updatate și au instalate soluții de securitate (firewall, antivirus, antimalware etc.);
- Încălcarea securității datelor prin atacuri cibernetice se comunică imediat responsabilului cu protectia datelor personale, care apelează numărul unic 1911 pentru raportarea acestora și se notifică ANSPDCP;
- Nu se introduc în rețea echipamente străine (router, stick, modem, laptop), iar dispozitivele mobile proprii se scanează pentru detectarea virușilor cibernetici înainte de utilizare;
- Fișierele care conțin date personale aflate pe dispozitive mobile (laptop, tabletă, memorie USB) se criptează pentru ca, în caz de pierdere sau furt să nu poată fi accesate de persoane neautorizate;
- Pe dispozitivele mobile nu se instalează programe / aplicații din surse nesigure sau fără licență. Instalarea programelor / aplicațiilor cade în sarcina responsabilului cu gestionarea / mentenanța sistemului informatic al entității, iar în cazul muncii în afara sediului angajatorului, instalarea programelor / aplicațiilor se face doar de către responsabilului cu gestionarea / mentenanța sistemului informatic al entității;
- Pe dispozitivele mobile nu se introduc / prelucrează date din surse nesigure, memorie USB, DVD etc. Dacă este necesar, pentru salvarea de date în formă criptată se folosește doar stick USB dedicat, folosit doar în scopul muncii în afara sediului angajatorului;
- De pe echipamentele de serviciu sau cele dedicate muncii în afara sediului angajatorului nu se deschid site-uri nesigure, nu se descarcă fișiere de pe internet decât în interes de serviciu, nu se deschid e-mailuri necunoscute, suspecte. Se cere vigilență sporită la descărcarea și deschiderea atașamentelor de e-mail, nu se descarcă dacă sunt din surse necunoscute care nu sunt de încredere. Dacă emailul pare să fie trimis de o persoană cunoscută dar nesolicitat, se cere confirmarea persoanei respective că a trimis mesajul;
- Utilizatorii sunt obligați să țină confidențiale datele cu care lucrează, atât în timpul programului de lucru cât și după încetarea acestuia;
- În locul unde persoane străine pot vedea monitorul în timpul lucrului, acesta trebuie protejat prin repoziționarea monitorului sau conform posibilităților;
- Utilizatorii păstrează strict secrete numele de utilizator, parolele de acces la stații și programe și nu le dezvăluie nimănui. În caz că există posibilitatea să fie aflate de către o altă persoană, acestea vor fi schimbate de urgență;
- Utilizatorii închid aplicațiile dacă părăsesc stația iar, dacă nimeni nu lucrează la stație, se blochează stația cu Ctrl +Alt +Del – "Lock this computer".
- Utilizatorii permit actualizarea programelor antivirus în vederea securizării permanente a sistemului;
- Documentele care conțin date personale sau confidențiale pot fi copiate doar cu acordul conducerii;
- Documentele care conțin date personale și care trebuie aruncate vor fi distruse cu distrugatorul de documente, dacă acesta există în locația unde se desfășoară munca în afara sediului angajatorului. Dacă acest dispozitiv nu există, documentele pe suport de hârtie care trebuie distruse se stochează în siguranță și se predau periodic angajatorului care va dispune distrugerea ireversibilă a acestora.

5.3.2. Utilizarea dispozitivelor mobile în condiții de securitate

Dispozitivele mobile utilizate pentru prelucrarea datelor cu caracter personal includ elemente precum:

- Laptop-uri
- Notebook-uri
- Tablete
- Smartphone-uri
- Smart Watch-uri

5.3.2.1. Protecțiadatelor cu caracter personal prelucrate pe dispozitive furnizate de Casa de Cultura a Studenților din București

- Pentru prelucrarea datelor personale în numele Casei de Cultura a Studenților din București se folosesc numai dispozitivele mobile furnizate de Casa de Cultura a Studenților din București sau cele concesionate / închiriate de la salariat.
- Echipamentele mobile folosite pentru munca la distanță sunt configurate de către responsabilul cu gestionarea / mentenanța sistemului informatic al entității în concordanță cu politicile / procedurile Casei de Cultura a Studenților din București privind securitatea datelor cu caracter personal.
- Salariații asigură accesul la dispozitiv pentru rezolvarea audit / verificare și pentru întreținere.
- Transportul dispozitivului de lucru se face într-un loc protejat și nu se expune unor situații în care acesta se poate deteriora.
- Dispozitivul de lucru nu este lăsat nesupravegheat, la vedere, cum ar fi pe bancheta din spate a unei mașini.
- Nu se elimină nici un semn de identificare de pe dispozitiv, cum ar fi o etichetă a companiei sau un număr de serie.
- Dispozitivul este blocat atunci când nu este folosit de către posesorul lui și codul nu este ușor accesibil (cum ar fi un postit lipit de laptop cu parola scrisă pe el).
- Nu se adaugă echipamente hardware periferice fără aprobarea responsabilului cu gestionarea / mentenanța sistemului informatic al entității.
- Pe dispozitiv nu se stochează informații protejate decât dacă acest lucru a fost autorizat și dacă au fost introduse protecții adecvate (de exemplu criptarea).
- Nu se păstrează date de acces împreună cu dispozitivul (la un loc cu dispozitivul), numerele de identificare personale sau alte elemente de securitate.
- Ecranul dispozitivului se blochează după o scurtă perioadă de neutilizare și necesită un cod de accessau o parolă pentru a-l debloca.
- Parolele de acces utilizate sunt puternice și greu de ghicit.
- Nu se setează pe dispozitiv nici un fel de conectări neasigurate (adică cele care nu necesită o parolă).
- Dispozitivul furnizat de organizație este destinat exclusiv muncii în afara sediului angajatorului și nu se permite utilizarea acestuia de către familie sau prietenii și nu este folosit pentru activități personale.
- Crearea copiilor de siguranță a datelor personale / salvarea acestora se face în mod regulat, iar salariatul se asigură că dispozitivul este conectat la rețeaua Casei de Cultura a Studenților din București pentru efectuarea acestei operațiuni.
- Nu se creează backup-uri de informații protejate necriptate.
- Dispozitivul este verificat periodic pentru actualizarea programelor antivirus, iar salariatul se asigură că dispozitivul este conectat la rețeaua Casei de Cultura a Studenților din București pentru efectuarea acestei operațiuni și nu dezactivează protecția antivirus de pe dispozitiv.
- Dispozitivul nu se conectează la rețele non Casa de Cultura a Studenților din București cum ar fi wireless sau Internet, cu excepția cazului în care este utilizată o rețea VPN (Virtual Private Network).
- În locuri publice se amplasează dispozitivul astfel încât utilizatorii neautorizați să nu poată vizualiza, sau să facă fotografii sau video clipuri ecranului.

5.3.2.2. Protecţia datelor cu caracter personal prelucrate pe dispozitive mobile personale

În contextul muncii în afara sediului operatorului, activităţile pot fi desfăşurate şi pe dispozitivele mobile ale salariaţilor "Bring Your Own Device" (BYOD).

Problemele comune şi problemele de securitate cu BYOD pot include:

- Utilizarea aparatului de către alţi membri ai familiei
- Stocarea automată a datelor în facilităţile de backup în cloud
- Expunerea crescută la pierderi potenţiale în situaţii sociale, de ex. pe plajă, într-un bar
- Acces potenţial la site-uri care nu respectă politica de utilizare acceptabilă a organizaţiilor
- Conectarea la reţele nesigure, de ex. hotspot wireless care nu este securizat
- Protecţia anti-virus şicât de des este actualizat dispozitivul
- Instalarea de aplicaţii potenţial dăunătoare pe dispozitiv (de multe orif ără ca utilizatorul să fie conştient de faptul că este malware)

Măsuri de securitate în contextul muncii în afara sediului operatorului folosind sistemul BYOD:

- Casa de Cultura a Studenţilor din Bucureşti evaluează fiecare cerere BYOD în mod individual, pentru a stabili:
  - ❑ Identitatea persoanei care face cererea
  - ❑ Motivul comercial al cererii
  - ❑ datele care vor fi stocate sau prelucrate pe dispozitiv
  - ❑ dispozitivul specific care va fi utilizat
- Solicitările privind BYOD se trimit către responsabilul cu gestionarea / mentenanţa sistemului informatic al entităţii şi către responsabilul cu protecţia datelor cu caracter personal.
- Gradul de control exercitat de organizaţie asupra dispozitivului BYOD este adecvat sensibilităţii datelor deţinute de acesta.
- Casa de Cultura a Studenţilor din Bucureşti monitorizează şi verifică nivelul de conformitate al dispozitivului în concordanţă cu politica / procedura de securitate a datelor personale adoptate de Casa de Cultura a Studenţilor din Bucureşti.
- Metodele şi momentele monitorizării şi auditului sunt făcute / stabilite astfel încât intimitatea proprietarului dispozitivului să nu fie invadată şi sunt în conformitate cu legislaţia aplicabilă în materie de confidenţialitate. Nu se efectuează monitorizarea utilizării dispozitivului în afara programului de lucru.
- Pentru evitarea intruziunii în spaţiul privat al salariatului de pe dispozitivul mobil al acestuia, pe care l-a pus la dispoziţia angajatorului pentru munca în afara sediului acestuia, se adoptă soluţii tehnice de tipul instalării pe dispozitive a unor maşini virtuale (ex: https://www.virtualbox.org/) sau al altor soluţii tehnice similare care permit accesul şi controlul angajatorului pe acel dispozitiv, inclusiv ştergerea la distanţă şi protejarea datelor personale, astfel încât să nu fie şterse şi datele personale ale salariatului.
- În cazul în care salariatul a pus la dispoziţia angajatorului un dispozitiv pe care nu deţine date personale ale acestuia, dispozitivul angajatului poate fi şters de la distanţă, integral, dacă:
  - ❑ Dispozitivul este pierdut;
  - ❑ Angajatul îşi încetează raporturile de muncă;

-Departamentul IT detectează o încălcare a securităţii datelor sau a procedurilor de utilizare / securizare a datelor personale, un virus sau o ameninţare similară la adresa securităţii infrastructurii de date şi tehnologii a Casei de Cultura a Studenţilor din Bucureşti.

- Încazul în care dispozitivul este pierdut sau furat, proprietarul informează responsabilul cu gestionarea / mentenanţa sistemului informatic al entităţii cât mai curând posibil, oferind detalii despre circumstanţele pierderii şi sensibilitatea informaţiilor stocate pe acesta. Casa de Cultura a Studenţilor din Bucureşti blochează accesul pe "maşina virtuală" / şterge de la distanţă datele prelucrate pe "maşina virtuală", sau şterge integral conţinutul dispozitivului, dacă acesta a fost pus la dispoziţia angajatorului fără să conţină date private.
- La încetarea raporturilor de muncă, proprietarul dispozitivului permite ca dispozitivul să fie auditat şi să fie eliminate toate datele şi aplicaţiile legate de companie.

Categoriai nformaţiei	Exemple	Cine poateaveaac cesprin BYOD	Tipuri de dispozitive BYOD	Controalenecesare	Comentarii
Nivelul 0 - Public	Cataloguri de produse, informaţiidesprepre ţuri, adrese de locaţie ale companieişinumere de contact	Oricine	Orice	Niciunul	Acesteinformaţii sunt în general accesibilepubliculuişiacc esateprinmijloaceaccesib ilepublicului, de ex. un site web
Nivelul 1 - Protejat	Proceduri interne, detaliidespreprodus , comunicaţii interne ale companiei etc. e-mail confidenţial	Angajaţişialte părţiinteresat eautorizate	Laptop-uri Tabletele Smartphone-uri	Protecţieprinparolă pentrudispozitiv Blocareinactivă Ştergere de la distanţă conform prezenteiproceduri Protecţiaprinparolă pentruaplicaţie Audituriperiodice	Aceastăzonăesteceamaip robabilăutilizare a BYOD din cadrulorganizaţiei
Nivelul 2 - Limitat	InformaţiidespreRe surseumane, informaţiibancare, informaţii cu caracter personal acoperite de legislaţiaprivindpro tecţiadatelor	Grupurirestrâ nse de angajaţi	Numai Laptop-uri	Criptare full disk VPN Patching automatizat Anti-virus Firewall Audituriperiodice	Acesteinformaţiitrebuiea ccesatenumaiprindispozi tive cu controalestricte de securitate. Acestlucrupoateîmpiedic apracticutilizareaunuidis pozitiv BYOD înfuncţie de circumstanţe
Nivelul 3 - Confidential	Planuri de resurse ale companiei, propunericomercial e, informaţiifinanciare nepublicate	Nimeni	Nimic	Nu e aplicabil	Acesteinformaţiitrebuiea ccesatenumaiprininterm ediulunordispozitivefurni zate de organizaţie, cu controalestricte de securitate

5.3.2.3. Utilizarea mesageriei electronice

Recomandări generale privind utilizarea mesageriei electronice în cadrul Casei de Cultura a Studenţilor din Bucureşti :

- În comunicările prin sistemul de mesagerie electronică al Casei de Cultura a Studenţilor din Bucureşti se respectă întocmai procedura internă privind utilizarea mesageriei electronice în condiţii de siguranţă.
- Recomandările privind utilizarea mesageriei electronice în cadrul Casei de Cultura a Studenţilor din Bucureşti se respectă de către toţi utilizării acestor facilităţi, indiferent de mijloacele sau locaţia de acces, de ex. Prin intermediul dispozitivelor mobile sau în afara sediului angajatorului.
- Recomandările privind utilizarea mesageriei electronice în cadrul Casei de Cultura a Studenţilor din Bucureşti se aplică tuturor sistemelor, persoanelor şi proceselor care constituie sistemele informatice ale Casei de Cultura a Studenţilor din Bucureşti, inclusiv membrilor conducerii, directorilor, angajaţilor, furnizorii şi altor părţi terţe care au acces la sistemele Casei de Cultura a Studenţilor din Bucureşti .
- Pentru orice neclarităţi privind utilizarea mesageriei electronice în cadrul Casei de Cultura a Studenţilor din Bucureşti salariaţii se adresează responsabilului cu gestionarea / mentenanţa sistemului informatic al entităţii şi / sau responsabilului cu protecţia datelor cu caracter personal.

5.3.2.3.1. Trimiterea şi primirea mesajelor electronice

- Facilităţile de mesagerie electronică furnizate de Casei de Cultura a Studenţilor din Bucureşti se folosesc numai pentru comunicări oficiale, în interesul Casei de Cultura a Studenţilor din Bucureşti. Nu se utilizează un cont personal de e-mail în acest scop.
- Instrucţiunile Casei de Cultura a Studenţilor din Bucureşti privind transmiterea de informaţii clasificate prin mesaje electronice se respectă întocmai şi înorice moment.
- Toate mesajele trimise dintr-un cont de organizaţie rămân proprietatea Casei de Cultura a Studenţilor din Bucureşti şi sunt considerate ca făcând parte din înregistrările Casei de Cultura a Studenţilor din Bucureşti . Toate mesajele Casei de Cultura a Studenţilor din Bucureşti sunt considerate comunicări oficiale ale Casei de Cultura a Studenţilor din Bucureşti şi sunt tratate în consecinţă.
- Casa de Cultura a Studenţilor din Bucureşti are dreptul legal de a monitoriza şi de a controla utilizarea mesajelor electronice de către utilizatorii autorizaţi, pentru a evalua conformitatea cu politicile şi procedurile Casei de Cultura a Studenţilor din Bucureşti.
- Ştergerea unui mesaj dintr-un cont de e-mail al Casei de Cultura a Studenţilor din Bucureşti, alocat salariaţilor, nu înseamnă că a fost eliminat definitiv din sistemele informatice ale Casei de Cultura a Studenţilor din Bucureşti , prin urmare, astfel de mesaje pot fi supuse auditului şi revizuirii.
- Având în vedere faptul că nu se poate garanta că un mesaj va fi recepţionat sau citit de către un destinatar şi că mesajele pot fi interpretate în moduri diferite, înfuncţie de cultura, rolul şi chiar starea de spirit a persoanei care le citeşte, se va decide punctual dacă utilizarea mesajelor electronice este un mijloc adecvat de transmitere a informaţiilor şi dacă o alternativă precum telefonul ar fi preferabilă, în special dacă mesajul este urgent sau complex.
- Pentru a preveni transmiterea accidentală către destinatari neautorizaţi de mesaje care conţin informaţii protejate, nu se foloseşte / se dezactivează funcţia de completare automată a unor texte şi e-mail-uri unde sistemul sugerează destinatari pe baza caracterelor tipărite deja.
- Nu se trimit mesaje inutile către liste de distribuţie, în special cele cu circulaţie largă, cum ar fi "lista globală" a tuturor angajaţilor. Atunci când este necesar, aceste mesaje trebuie transmise prin departamentul de comunicaţii al Casei de Cultura a Studenţilor din Bucureşti .
- Nu se trimit mesaje care conţin materiale defăimătoare, obscene, care nu respectă politica de egalitate şi diversitate a instituţiei sau pe care un destinatar ar putea să le considere inadecvate, în mod rezonabil. În cazul în care există suspiciuni că mesajul dorit se încadrează în această categorie, se consultă Responsabilul cu protecţia datelor personale înainte de a trimite mesajul.

Sistemul de mesagerie electronică oficial al Casei de Cultura a Studenţilor din Bucureşti **nu se utilizează**pentru:

- ❑ Distribuirea de materiale comerciale sau publicitare nesolicitate, scrisori în lanţ sau alte tipuri de poştă nedorită de orice fel, către alte organizaţii;

- ❑ Trimiterea de materiale care încalcă drepturile de autor sau drepturile de proprietate intelectuală ale altei persoane sau organizații;
- ❑ Activități ce corup sau distrug datele altor utilizatori sau care perturbă altfel activitatea altor utilizatori;
- ❑ Distribuirea de imagini, date obscene sau indecente ofensatoare, indecente sau alte materiale sau orice date care pot fi văzute ca imagini obscene sau indecente;
- ❑ Trimiterea de materiale / informații care pot provoca neplăceri, inconveniente sau anxietate inutilă altora;
- ❑ Trimiterea către alte persoane de mesaje abuzive, amenințătoare sau de agresiune;
- ❑ Transmiterea de materiale care să discrimineze sau să încurajeze discriminarea pe motive de rasă, sex, orientare sexuală, stare civilă, dizabilități, convingeri politice sau religioase;
- ❑ Transmiterea de materiale defăimătoare sau de afirmații false, de natură înșelătoare;
- ❑ Activități care încalcă confidențialitatea altor utilizatori;
- ❑ Trimiterea de mesaje anonime – adică fără identificarea clară a expeditorului;
- ❑ Orice alte activități care aduc sau pot produce prejudicii Casei de Cultura a Studenților din București .

- ● Mesajele nedorite sau spamul se șterg fără a fi citite. Nu se răspunde la acest tip de mesaje, deoarece acest lucru poate confirma existența unei adrese valide pentru expeditor, ceea ce va duce la alte comunicări nedorite.

5.3.2.3.2. Monitorizarea facilităților de mesagerie electronică

Utilizarea mesageriei electronice în cadrul Casei de Cultura a Studenților din București este monitorizată și înregistrată centralizat pentru:

- planificarea și gestionarea eficientă a capacității resurselor
- evaluarea conformității cu politicile și procedurile interne
- asigurarea că standardele impuse sunt menținute / respectate
- prevenirea și detectarea infracțiunilor
- investigarea utilizării neautorizate

- ● Monitorizarea facilităților de mesagerie electronică se efectuează numai de către personalul autorizat.
- ● Procedurile de monitorizare se aplicătuturorutilizatorilorși pot include verificareaconținutuluimesajelor.
- ● În cazul în care sunt suspiciuni că unitățile de mesagerie electronică sunt utilizate abuziv de un salariat și în afara limitelor permise de politicile și procedurile interne, se contactează managerul IT și Responsabilului cu protecția datelor personale. Sesizările sunt investigate în conformitate cu procedurile documentate și, după caz, în funcție de dovezile furnizate. Casa de Cultura a Studenților din București are obligația legală de a furniza astfel de informații organelor abilitate, la solicitarea acestora, în condițiile legii.

- Nu se accesează contul oficial de mesagerie electronică al altui utilizator fără permisiunea utilizatorului autorizat al contului sau fără permisiunea scrisă a supervizorului acestuia. În astfel de cazuri, accesarea contului oficial de mesagerie electronică al altui utilizator trebuie justificată temeinic și se deschid numai mesaje care sunt relevante pentru problema în cauză.

5.3.2.3.3. Folosirea E-mail-ului

Toate e-mailurile trimise de la adresele institutieiției către destinatarii din afara instituției vor purta în mod automat următoarea notă de responsabilitate:
"Informațiile conținute în acest mesaj sunt destinate exclusiv destinatarului și pot conține informații protejate. Dacă nu sunteți destinatarul, ștergeți acest mesaj și notificați expeditorul; nu trebuie să copiați sau să distribuiți acest mesaj sau să dezvăluiți conținutul său nimănui. Orice opinii exprimate în acest mesaj sunt cele ale persoanei (persoanelor) și nu neapărat ale organizației. Nu se poate invoca acest mesaj fără confirmarea scrisă din partea unui reprezentant autorizat al conținutului său. Nici o garanție nu implică faptul că acest mesaj sau orice atașament este fără virus sau nu a fost interceptat și modificat."
Recomandări pentru folosirea emailului oficial creat pentru salariații Casei de Cultura a Studenților din București :

- Nu se folosește funcția de redirecționare automată - "auto forwarding" în e-mailuri, de ex. În timpul unei vacanțe, în cazul în care există posibilitatea ca aceasta să aibă ca rezultat transmiterea de informații protejate către un destinatar care nu deține o autorizație de securitate suficientă pentru nivelul informațiilor implicate.
- Căsuța poștală este configurată cu o limitare a mărimii acesteia.
- Administrarea contului de e-mail se face pentru a rămâne în limita de dimensiune a cutiei poștale, utilizând facilitatea de arhivare inclusă în majoritatea conturilor de e-mail.
- Dacă s-a atins limita maximă de stocare a e-mailurilor, se contactează responsabilul cu gestionarea / mentenanța sistemului informatic al entității pentru îndrumări.
- Pentru a evita blocarea cutiilor poștale ale altor utilizatori și pentru evitarea perturbării consecvente a activității, dacă mesajul e-mail are o distribuție largă, se utilizează link-uri către fișierele din mesajele de e-mail, în loc să se atașeze o copie a fișierului.
- În cazul în care dimensiunea documentelor trimise prin e-mail depășește limita de dimensiune la nivel de sistem (cel mai adesea limita este 20Mb), se contactează cu responsabilul cu gestionarea / mentenanța sistemului informatic al entității pentru îndrumări.
- Nu se accesează e-mailuri / link-uri suspecte primite prin e-mail și care pot conține viruși informatici, adware și alte tipuri de programe malware. Software-ul antivirus furnizat de. Casa de Cultura a Studenților din București rulează

permanent pe fiecare dispozitiv care are acces la reţea şi nu este dezactivat în nici o circumstanţă.

- Se raportează de urgenţă responsabilului cu gestionarea / mentenanţa sistemului informatic al entităţii orice suspiciune că s-a instalat un virus informatic saucă s-a primit un e-mail care poate conţine unul. Nu se deschid ataşamente care pot conţine un virus.
- În plus, **nu** trebuie să:
  - ❑ transmiteţi prin e-mail orice fişier ce credeţi că este infectat de un virus
  - ❑ descărcaţi date sau programe de orice natură din sursene cunoscute
  - ❑ dezactivaţi sau reconfiguraţi sistemul antivirus instalat care funcţionează pe un computer utilizat pentru a accesa facilităţile de e-mail
  - ❑ transmiteţi avertismente despre virusuri, altele decât cele ale responsabilului cu gestionarea / mentenanţa sistemului informatic al entităţii

5.3.3. Acces controlat la sistemul informatic al Casei de Cultura a Studenţilor din Bucureşti

Casa de Cultura a Studenţilor din Bucureşti pune în aplicare măsuri de restricţionarea accesului la sistemul informatic care sunt adecvate şi proporţionale cerinţei de protecţie a afacerii şi a datelor cu caracter personal prelucrate.

Cerinţele de protecţie a afacerii şi a datelor cu caracter personal prelucrate sunt cele specificate de proprietarii activelor implicate şi depind de factori precum:

- ❑ Clasificarea de securitate a informaţiilor stocate şi procesate de un anumit sistem sau serviciu.
- ❑ Legislaţia relevantă care se poate aplica în România.
- ❑ Cadrul de reglementare în care funcţionează organizaţia şi sistemul.
- ❑ Obligaţiile contractuale faţă de părţi terţe.
- ❑ Amenintarile, vulnerabilităţile şi riscurile implicate.
- ❑ Disponibilitatea organizaţiei pentru risc.

5.3.3.1. Recomandări de securitate privind accesul la sistemul informatic al Casei de Cultura a Studenţilor din Bucureşti

- Recomandările de securitate privind accesul la sistemul informatic al Casei de Cultura a Studenţilor din Bucureşti se respectă de către toate persoanele şi toate sistemele Casei de Cultura a Studenţilor din Bucureşti .
- Cerinţele privind securitatea informaţiilor sunt clar precizate în instrucţiunile de lucru / procedura internă şi trebuie să ţină seama de standardele Casei de Cultura a Studenţilor din Bucureşti.
- În elaborarea instrucţiunilor / permisiunilor de acces la sistemele şi serviciile Casei de Cultura a Studenţilor din Bucureşti se respectă următoarele principii generale:

  - ❑ ***Apărarea în profunzime***– Securitatea nu trebuie să depindă de nici un control unic, ci să fie suma unui număr de controale complementare

- ***Celmai mic privilegiu***– Abordarea implicită trebuie să fie aceea de a presupune că accesul nu este necesar, mai degrabă decât să presupunem că este
- ***Trebuie să știi***– Accesul este acordat numai informațiilor necesare pentru a îndeplini un rol și nimic mai mult
- ***Trebuiefolosit***– Utilizatorii vor putea accesa facilitățile fizice și logice necesare pentru rolul lor.

- Selecția furnizorilor de servicii Cloud se face luând în considerare următoarele considerente legate de acces:
  - Funcțiile de înregistrareși de anulare a înregistrării utilizatorului;
  - Facilități pentru gestionarea drepturilor de acces la serviciul Cloud;
  - Dacăpoate fi controlat accesul la serviciile Cloud, la funcțiile serviciului Cloud și la datele clienților serviciului Cloud;
  - Disponibilitatea autentificării mai multor utilizatori pentru conturile de administrator;
  - Existența procedurilor de alocare a informațiilor secrete, cum ar fi parolele.

5.3.3.1.1. Gestionarea accesului utilizatorilor

- Casa de Cultura a Studenților din București elaborează și implementează proceduri de control al accesului utilizatorilor, pentru reglementarea accesului autorizat la sistemele Casa de Cultura a Studenților din București și pentru prevenirea accesului neautorizat. Procedurile acoperă toate etapele ciclului de viață al accesului utilizatorilor, de la înregistrarea inițială a utilizatorilor până la anularea finală a înregistrării utilizatorilor care nu mai au nevoie de acces.
- Drepturile de acces ale utilizatorilor se revizuiesc la intervale regulate.
- Conturile de administrare a sistemului trebuie alocate numai utilizatorilor autorizați pentru administrarea sistemului.

5.3.3.1.1.1. Înregistrarea și anularea înregistrării utilizatorului

- Cererea de acces la sistemele informatice și la rețeaua Casei de Cultura a Studenților din București se transmite responsabilului cu gestionarea / mentenanța sistemului informatic al entității pentru analiză și aprobare.
- Toatecererile de acces la sistemele informatice și la rețeaua Casei de Cultura a Studenților din București sunt procesate conform procedurii interne care asigură efectuarea unor verificări adecvate de securitate și obținerea corectă a unei autorizații, înainte de crearea contului de utilizator.
- La crearea contului de utilizator se aplică principiul segregării sarcinilor, astfel încât crearea contului de utilizator și atribuirea permiselor de acces să fie efectuate de persoane diferite.
- Fiecare cont de utilizator are alocat un nume de utilizator unic și nu este asociat cu un anumit individ.
- Nu se creează conturi de utilizator generice care urmează a fi utilizate de un grup de persoane.

- La crearea / configurarea contului de utilizator se foloseşte o parola puternică ce este comunicată utilizatorului prin mijloace sigure. Utilizatorul schimbă parola la prima utilizare a contului.
- La încetarea raporturilor de muncă cu salariatul se suspendă accesul acestuia la sistemele informatice ale Casei de Cultura a Studenţilor din Bucureşti în ultima zi de lucru a angajatului. Suspendarea accesului la sistemele informatice ale Casei de Cultura a Studenţilor din Bucureşti se face la solicitarea superiorului ierarhic al fostului salariat şi se efectuează de către responsabilul cu gestionarea / mentenanţa sistemului informatic al entităţii.
- În situaţiile excepţionale în care se consideră că există riscul ca angajatul să acţioneze cu rea credinţă împotriva angajatorului, înainte sau după rezilierea contractului individual de muncă, cererea de suspendare a accesului la sistemele informatice ale Casei de Cultura a Studenţilor din Bucureşti poate fi aprobată şi pusă în aplicare înainte de notificarea de reziliere / încetare a contractului individual de muncă, mai ales dacă salariatul are drepturi privilegiate de acces, de ex. Administratorul domeniului.
- Conturile de utilizator sunt iniţial suspendate sau dezactivateşi nu eliminate.
- Numele conturilor de utilizator nu se refolosesc.

5.3.3.1.1.2. Furnizarea accesului utilizatorilor

- Fiecare utilizator primeşte drepturi de acces la sistemele informatice ale Casei de Cultura a Studenţilor din Bucureşti proporţional cu sarcinile pe care trebuie să le îndeplinească.
- Dreptul de acces la sistemele informatice ale Casei de Cultura a Studenţilor din Bucureşti este bazat pe roluri, adică un cont de utilizator este adăugat unui grup ce a fost creat cu permisiunile de acces cerute de rolul respectiv.
- Rolurile de grup sunt menţinute în conformitate cu cerinţele de afaceri ale Casei de Cultura a Studenţilor din Bucureşti, iar orice modificare a acestora este autorizată şi controlată în mod oficial prin intermediul procesului de gestionare a schimbărilor de roluri.
- Nu se acordă drepturi de acces suplimentare / ad-hoc conturilor de utilizator din afara rolurilor grupului.
- În cazul în care sunt necesare permisiuni suplimentare de acces, acestea se solicită în mod oficial, respectând procedura internă.

5.3.3.1.1.3. Eliminarea sau revizuirea drepturilor de acces

- Revizuirea / eliminarea dreptului de acces se impune şi se efectuează ori de câte ori în cetează relaţiile de muncă cu un salariat sau ca urmare a schimbării funcţiei / încadrării / modificării atribuţiilor / sarcinilor de serviciu ale acestuia în Casa de Cultura a Studenţilor din Bucureşti .
- Este interzisă administratorilor sistemului informatic al Casei de Cultura a Studenţilor din Bucureşti orice schimbare a propriilor conturi de utilizator sau a drepturilor de acces ale acestora.

5.3.3.1.1.4. Administrarea drepturilor de acces privilegiate

- Drepturile de acces privilegiate, cum ar fi cele asociate conturilor la nivel de administrator, sunt identificate pentru fiecare sistem sau reţea şi sunt strict controlate.
- Utilizatorii tehnici (cum ar fi personalul de asistenţă / mentenanţă IT) nu folosesc zilnic conturile de utilizator cu acces privilegiat, ci un cont de utilizator separat - "admin" care se creează şi se utilizează numai atunci când sunt necesare privilegii suplimentare.
- Conturile de utilizator separat - "admin" sunt specifice unui individ, de ex. "Popescu George Admin".
- Dreptul de acces "administrator" este alocat numai persoanelor ale căror roluri necesită astfel de permisiuni şi care au beneficiat de o instruire suficientă pentru a înţelege implicaţiile utilizării acestora.
- Unde este posibil, se evită utilizarea conturilor cu acces privilegiat în rutine automatizate, cum ar fi lucrări de tip sortare sau interfaţă. În cazul în care acest lucru nu este posibil, parola utilizată trebuie protejată şi schimbată după fiecare accesare a contului respectiv.

5.3.3.1.1.5. Autentificarea utilizatorului pentru conexiuni externe

- Pentru reducerea riscului compromiterii securităţii reţelei Casei de Cultura a Studenţilor din Bucureşti se evită utilizarea modemurilor organizaţiei pe calculatoarele / laptopurile / dispozitivele mobile care nu sunt din cadrul Casei de Cultura a Studenţilor din Bucureşti sauconectarea acestora la reţeaua Casei de Cultura a Studenţilor din Bucureşti .
- Se solicită autorizarea specifică prealabilă înainte de a conecta orice echipament la reţeaua Casei de Cultura a Studenţilor din Bucureşti.
- În cazul în care accesul la reţeaua Casei de Cultura a Studenţilor din Bucureşti este necesar prin intermediul reţelelor VPN, se solicită o autorizaţie specifică prealabilă.
- Pentru reducerea riscului accesului neautorizat de pe internet la reţeaua Casei de Cultura a Studenţilor din Bucureşti se aplică sistemul autentificării cu doi factori pentru accesul de la distanţă, în conformitate cu principiul "ceva ce aveţi şi ceva ce ştiţi".

5.3.3.1.1.6. Accesul de la distanţă al furnizorului asupra reţelei *Casei de Cultura a Studenţilor din Bucureşti*

- Partenerii Casei de Cultura a Studenţilor din Bucureşti sau furnizorii nu primesc detalii despre cum să acceseze reţeaua Casei de Cultura a Studenţilor din Bucureşti fără o autorizaţie specifică prealabilă.
- Orice modificare a conexiunii furnizorului (de exemplu, la terminarea unui contract) se transmite imediat la responsabilul cu gestionarea / mentenanţa sistemului informatic al entităţii, astfel încât accesul să fie revizuit sau eliminat.

- Toate drepturile și metodele de acces sunt controlate de responsabilul cu gestionarea / mentenanțasistemului informatic al entității.
- Partenerii Casei de Cultura a Studenților din București sau furnizorii contactează responsabilul cu gestionarea / mentenanța sistemului informatic al entității ori de câte ori este necesar pentru a solicita permisiunea de a se conecta la rețea și se păstrează un jurnal de activitate în acest sens.
- Software-ul de acces de la distanță și conturile de utilizator se dezactivează atunci când nu sunt utilizate sau când au încetat raporturile contractuale cu partenerii sau furnizorii Casei de Cultura a Studenților din București Casei de Cultura a Studenților din București.

5.3.3.1.1.7. Recomandări privind stabilirea parolelor de acces

- Casa de Cultura a Studenților din București utilizează metode suplimentare de autentificare bazate pe o evaluare a riscurilor ce iau în considerare:
  - ❑ Valoarea bunurilor protejate
  - ❑ Gradul de amenințare
  - ❑ Costul metodei suplimentare de autentificare
  - ❑ Ușurința utilizării și a caracterului practic al metodei propuse
  - ❑ Orice alte controale relevante în vigoare
- Metodele de autentificare multifactorială se pun în aplicare și sunt menținute în siguranță.
- Metoda "Single Sign-On (SSO)" este utilizată în cadrul rețelei Casei de Cultura a Studenților din București , cu excepția cazului în care cerințele de securitate impun o conectare ulterioară.
- Orice excepție de la aceste reguli trebuie autorizata de responsabilul cu gestionarea / mentenanța sistemului informatic al entității.

5.3.3.1.1.8. Responsabilitățile utilizatorului

- Casa de Cultura a Studenților din București implementează metode eficiente pentru a reduce riscul și vulnerabilitățile sistemului informatic din organizație.
- Fiecare utilizator al dispozitivelor / echipamentelor / rețelei informatice a Casei de Cultura a Studenților din București protejează credențialele de acces alocate și nu folosește contul individual de lucru în scopuri personale.
- Pentru a maximiza securitatea informațiilor Casei de Cultura a Studenților din București , fiecare utilizator:
  - ❑ Folosește o parolă puternică, în conformitate cu regulile stabilite în prezenta procedură.
  - ❑ Nu divulgă nimănui parola și nu permite nimănui accesul la contul individual de lucru.
  - ❑ Nu înregistrează parola în scris sau electronic, de exemplu într-un fișier sau în e-mail.
  - ❑ Nu utilizează aceeași parolă pentru alte conturi de utilizator, personale sau legate de afacerile Casei de Cultura a Studenților din București .
  - ❑ Nu lasă dispozitivele nesupravegheate sau conectate la rețea.

- ❑ Nu lasă la vedere, pe ecran, documente care conțin informații de acces, cum ar fi numele de conectare și parolele.
- ❑ Informează imediat responsabilul cu gestionarea / mentenanța sistemului informatic al entității despre orice modificare a roluluișia cerințelor de acces.

5.3.3.1.1.9. Evaluarea gradului de securitate și siguranță a sistemelor și aplicațiilor noi

- Casa de Cultura a Studenților din București implementează măsuri adecvate pentru evaluarea sistemelor noi sau modificate semnificativ.
- Sistemele / aplicațiile noi cuprind un model de securitate care include suport pentru următoarele:
  - ❑ Crearea de conturi individuale de utilizator
  - ❑ Definirea rolurilor sau grupurilor la care pot fi alocate conturile de utilizator
  - ❑ Alocarea permisiunilor către obiecte (de exemplu, fișiere, programme, meniuri) de diferite tipuri (de exemplu, citiți, scrieți, ștergeți, executați) la subiecte (conturi și grupuri de utilizatori)
  - ❑ Furnizarea de vizualizări diferite ale opțiunilor din meniuri și ale datelor în funcție de contul de utilizator și nivelele de permisiune ale acestuia
  - ❑ Administrarea contului de utilizator, inclusiv posibilitatea de a dezactiva și șterge conturile
  - ❑ Controalele de conectare a utilizatorilor, cum ar fi:
    - ➔ Nu se afișează parola așa cum este introdusă
    - ➔ Blocarea contului odată ce numărul de încercări greșite de conectare depășește un prag specificat
    - ➔ Oferă informații despre numărul de încercări de conectare nereușite și ultima conectare reușita odată ce utilizatorul a fost conectat cu succes
    - ➔ Restricții de conectare bazate pe dată și timp
    - ➔ Restricții de conectare asupra dispozitivului și locației
  - ❑ Timpul de inactivitate al utilizatorului
  - ❑ Administrarea parolei, incluzând:
    - ➔ Abilitatea utilizatorului de a schimba parola
    - ➔ Control asupra parolelor acceptabile
    - ➔ Expirarea parolei
    - ➔ Stocarea și transmisia parolei criptate
  - ❑ Facilități de audit pentru securitate, inclusiv logare/delogare, încercări de conectare nereușite, activități de acces la obiecte și administrare de cont
- În timpul dezvoltării software-ului, codul sursă al programului este protejat împotriva accesului neautorizat.
- Accesul la programele de utilitate care oferă o metodă de ocolire a securității sistemului (de exemplu, instrumentele de manipulare a datelor) este strict controlat și utilizarea lor este limitată.

5.4. Recomandări sintetice privind organizarea muncii în alte locații decât sediul angajatorului

Angajatorul va transmite angajaților prin email recomandări scrise privind organizarea activității profesionale în alte spații decât sediul companiei.

Un model de email cu recomandări face obiectul Anexei 4.

6. Resurse materiale

Resursele materiale puse la dispoziția salariatului pot include următoarele, sau orice alt tip de resurse sunt necesare pentru desfășurarea activității specifice a salariatului:

- Copiator/scanner;
- Rechizite;
- Linie telefonică/fax;
- Calculator / laptop / tabletă / smartphone.

7. Formulare

Formular de analiză procedură

Anterior aprobării și intrării în vigoare, procedura se transmite spre analiză compartimentelor implicate, în vederea exprimării unui punct de vedere.

Nr. crt.	Compartiment	Nume și prenume conducător compartiment	Înlocuitor de drept sau delegat	Aviz favorabil		Aviz nefavorabil		
				Semnătură	Data	Observații	Semnătură	Data
1	2	3	4	5	6	7	8	9

Formular de distribuire a procedurii

După aprobarea procedurii, aceasta se distribuie compartimentelor implicate sau tuturor compartimentelor, înfuncție de tipul procedurii.

Nr. exemplar	Compartiment	Numeși prenume	Data primirii	Semnătură	Data retragerii procedurii înlocuite	Semnătură	Data intrării în vigoare

1	2	3	4	5	6	7	8
1.	**Exemplarul nr. 1 (originalul) se păstrează la responsabilul desemnat, în cazul procedurilor de sistem și la compartimentul inițiator, în cazul procedurilor operaționale**						
2.	Compartiment 1 (Exemplar nr. 2 – copie)						
3.	Compartiment 2 (Exemplar nr. 3 – copie)						

Formular de evidență a modificărilor procedurii

Procedura documentată este supusă permanent monitorizării și după caz, actualizării prin revizii sau ediții.

Nr. crt.	Ediție	Data ediției	Revizie	Data reviziei	Nr. pagină modificată	Descriere modificare	Semnătură conducător compartiment
1	**2**	**3**	**4**	**5**	**6**	**7**	**8**

Anexa la punctual 3.

3.1.
1.Compartimentul cultural — artistic;
2. Compartimentul financiar — contabilitate — resurse umane;
3. Compartimentul achiziții publice — investiții — patrimoniu — administrativ —secretariat și relații publice;

3.2. Salariati CCSBucuresti
- Apostu Elena Loredana
- Avramut Andreea Mihaela
- Bogatu Mihai
- Bordas Paul
- Chiran Liliana
- Cotet Dorin Adrian
- Daringa Rasnoveanu Oltea Clara
- Dobre Iuliana
- Fratila Luminita
- Gheorghe Nelu Marian
- Gherasimescu Claudiu
- Gherghina Ioana
- Hanceriuc Doinita Paula
- Laslau Pavel
- Muntenita Mihai
- Radulescu Nicolita
- Radulescu Tudorel
- Spranceana Stefan Silviu
- Todor Serghei Mihai
- Virtejeanu Smaranda

3.3. Secretariat Comisie SCIM si SNA
- Radulescu Nicolita
- Daranga Rasnoveanu Oltea Clara
- Gherghina Ioana

3.4. Daringa Rasnoveanu Oltea Clara

8. Anexe

ANEXA 1

DECLARAŢIA ANGAJATULUI PRIVIND ÎNSUŞIREA ŞI RESPECTAREA POLITICII DE SECURITATE A INFORMAŢIILOR

Vă rugăm să citiţi următorul rezumat al principalelor idei ale politicilor Casei de Cultura a Studenţilor din Bucureşti în ceea ce priveşte securitatea informaţiilor.

1. Am luat la cunoştinţă despre faptul că utilizarea de către mine a sistemelor informatice şi de comunicaţii ale Casei de Cultura a Studenţilor din Bucureşti pot fi monitorizate şi/sau înregistrate în scopuri legale.
2. Am luat la cunoştinţă şi sunt de acord cu faptul că sunt responsabil pentru folosirea şi protejarea credenţialelor de acces puse la dispoziţie de Casa de Cultura a Studenţilor din Bucureşti : cont de utilizator şi parolă, simbol de acces sau alte elemente care îmi pot fi furnizate.
3. Mă angajez să nu folosesc numele de utilizator ş iparola altcuiva pentru a accesa sistemele Casei de Cultura a Studenţilor din Bucureşti .
4. Am luat la cunoştinţă despre faptul că este interzisă accesarea sistemelor unui computer la care nu am primit acces.
5. Mă angajez să protejez orice material trimis, primit, stocat sau prelucrat de mine, în funcţie de nivelul de clasificare atribuit acestuia, inclusiv copii electronice şi pe hartie.
6. Mă angajez să marchez orice material securizat pe care îl creez conform instrucţiunilor publicate, astfel încât acesta să rămână protejat corespunzător.
7. Am luat la cunoştinţă despre faptul că este interzisă transmiterea / divulgarea de informaţii nesecurizate prin intermediul internetului (email sau alte metode) şi mă angajez să nu transmit informaţii în interes de serviciu şi conform decât dacă sunt folosite metode adecvate (ex. criptarea) pentru a fi protejate de accesul neautorizat.
8. Mă angajez să mă asigur întotdeauna că introduc adresa de email a destinatarului corect, astfel încât informaţiile transmise să nu fie compromise.
9. Măangajezsămăasigurîntotdeaunacă nu sunt privit de cătrepersoaneneautorizateîntimpcelucrezşivoiaveagrijăîntimpultipăririiinformaţiilorsecurizate.
10. Măangajezsăpăstrezînsiguranţădocumentelesecurizatetipariteşimăasigurîntotdeaunacăacestea sunt distruseireversibilatuncicândacestea nu mai sunt necesare.
11. Mă angajez să nu las computerul nesupravegheat, astfel încât accesul neautorizat la date să poată fi obţinut prin intermediul contului meu, în timp ce eu sunt plecat.
12. Mă angajez să fiu mereu la curent cu politica de securitate a Casei de Cultura a Studenţilor din Bucureşti , cu procedurile implementate şi orice altă instrucţiune specială referitoare la munca mea.
13. Mă angajez să informez de urgenţă superiorul meu dacă detectez, suspectez sau sunt martor al unui incident ce poate reprezenta o încălcare a securităţii, sau dacă observ orice slăbiciune de securitate a informaţiilor în sistemele sau serviciile Casei de Cultura a

Studenților din București .

14. Am luat la cunoștință despre faptul că este interzisă ocolirea controalelor de securitate ale sistemului, sau să le utilizez în alte scopuri decât cele intenționate și mă angajez să respect aceste prevederi.
15. Am luat la cunoștință despre faptul că este interzisă scoaterea echipamentul sau a informațiilor din incinta Casei de Cultura a Studenților din București fără o aprobare corespunzătoare și mă angajez să respect aceste prevederi.
16. Mă angajez să iau măsuri de precauție suplimentare pentru a proteja toate computerele și dispozitivele mobile atunci când le transport în afara spațiilor Casei de Cultura a Studenților din București (de exemplu lăsând un laptop nesupravegheat sau expus într-o mașină, astfel încât să fie expus riscului de furt).
17. Mă angajez să nu introduc viruși sau alte programe dăunătoare în sistem sau în rețea.
18. Am luat la cunoștință despre faptul că este interzisă dezactivarea protecției antivirus instalată pe dispozitivul pe care lucrez și mă angajez să respect aceste prevederi.
19. Mă angajez să respect obligațiile legale, naționale sau contractuale pe care Casa de Cultura a Studenților din București mi le-a impus ca fiind relevante pentru rolul meu.
20. În cazul în care decid încetarea raporturilor de muncă cu Casei de Cultura a Studenților din București, voi informa directorul înainte de îndepărtarea tuturor informațiilor importante reținute în contul meu.

Declaratie

Am citit rezumatul politicii de securitate a informațiilor de mai sus și sunt de acord să respect conținutul acesteia și cel al oricărei alte politici / proceduri relevante despre care Casa de Cultura a Studenților din București mă poate înștiința.

Numeleutilizatorului:

Semnăturautilizatorului:

Data: