Anexa nr. 6

(la HCD nr. 40/2019)

Politica de utilizare a internetului și comunicațiilor

I. Cadrul general

(1) Această politică se referă la toate aspectele legate de utilizarea tehnologiei informației și a comunicațiilor (IT&C) de către Asociația Națională a Evaluatorilor Autorizați din România, numită în continuare „Asociația".

(2) Prezenta politică oferă îndrumare cu privire la utilizarea internetului, a email-ului și a comunicațiilor mobile, a sistemului de parole și a suporturilor media externe.

(3) Această politică se aplică tuturor angajaților Asociației, precum și membrilor Consiliului director, ai Consiliilor filialelor și ai grupurilor de lucru care utilizează tehnologii IT&C puse la dispoziție de Asociație.

(4) Această politică se completează cu următoarele documente:

- Regulamentul European 2016/679 privind protecția persoanelor fizice referitor la prelucrarea datelor cu caracter personal și libera circulație a acestor date, pus în aplicare în România prin Legea 190/2018;
- Politica de securitate a datelor cu caracter personal.

II. Roluri și responsabilități

(5) Administratorul rețelei IT este responsabil cu furnizarea tehnologiilor și echipamentelor adecvate pentru asigurarea activității eficiente a Asociației.

(6) Toți angajații Asociației și terții care utilizează tehnologiile puse la dispoziție de Asociație au responsabilitatea de a cunoaște toate aspectele acestei politici, în special cele referitoare la securitatea informațiilor și a echipamentelor folosite, având în vedere că utilizarea necorespunzătoare a email-ului și a internetului poate avea consecințe serioase atât asupra persoanelor implicate cât și asupra Asociației.

III. Raportarea incidentelor de securitate

(7) Incidentele de securitate referitoare la orice aspect al acestei politici trebuie raportate imediat administratorului rețelei IT. Pentru referințe suplimentare legate de incidentele de securitate și raportarea acestora se va consulta Procedura de securitate a datelor cu caracter personal.

SECȚIUNEA A – EMAILUL

IV. Utilizarea emailului în activități oficiale

(8) Această politică se aplică tuturor emailurilor compuse și transmise de la adresele sau conturile de email ale Asociației, precum și emailurilor personale transmise utilizând facilitățile IT ale Asociației.

(9) Toate emailurile utilizate pentru a desfășura sau susține activitățile oficiale ale Asociației vor fi transmise de la o adresă de tipul "@anevar.ro".

(10) Conturile de email non-business (personale) pot fi utilizate, în unele situații, pentru a desfășura sau susține activități oficiale ale Asociației, cu respectarea recomandărilor prezentei politici.

(11) Toate emailurile care reprezintă aspecte de natură oficială sau administrativă sunt proprietatea Asociației și nu a unor persoane fizice (angajați sau terți care utilizează facilitățile IT ale Asociației).

(12) Emailurile stocate pe echipamentele Asociației sunt considerate parte a documentelor Asociației. Statutul juridic al unui mesaj de email este similar celorlalte forme de comunicare scrisă. În consecință, un email transmis cu ajutorul facilităților oferite de Asociație cu scopul de a desfășura sau susține activitățile Asociației va fi considerat comunicare oficială din partea Asociației.

(13) Emailurile oficiale transmise în exteriorul Asociației pot include următorul disclaimer:

"Datele cu caracter personal pe care le dezvăluiți Asociației Naționale a Evaluatorilor Autorizați din România vor fi prelucrate în conformitate cu Regulamentul European 2016/679. Pentru mai multe informații cu privire la modul în care utilizăm datele dumneavoastră cu caracter personal vă rugăm să consultați politica noastră de confidențialitate.

Acest email și orice atașament al său poate conține informații confidențiale și este destinat doar persoanei căreia îi este adresat. Dacă ați primit din greșeală acest mesaj, vă rugăm să notificați imediat expeditorul. În cazul în care nu sunteți destinatarul acestui email, vă rugăm să nu dezvăluiți, distribuiți, imprimați sau utilizați informațiile pe care le conține și să îl ștergeți imediat.

Deşi luăm toate măsurile rezonabile pentru a identifica orice virus informatic, este posibil ca ataşamentele acestui email să conţină virusuri informatice pe care programele noastre anti-virus nu au reuşit să le depisteze. Vă recomandăm să scanaţi cu propriul dumneavoastră anti-virus, documentele ataşate, înainte de a le deschide. Asociaţia Naţională a Evaluatorilor Autorizaţi din România nu va accepta nici o responsabilitate pentru eventualele daune produse de virusuri informatice transmise prin intermediul ataşamentelor acestui mesaj."

V. Emailului ca formă de comunicare

(14) Emailul reprezintă o metodă deschisă şi transparentă de comunicare. Cu toate acestea, nu există o garanţie că mesajul va fi primit sau citit sau că textul acestuia va fi înţeles în sensul intenţionat de expeditor. Din acest motiv, responsabilitatea alegerii emailului ca forma cea mai potrivită de a transmite informaţii urgente sau confidenţiale revine persoanei care transmite un email.

(15) În general, emailul nu este o metodă sigură de comunicare. Prin urmare, angajaţii Asociaţiei vor lua în considerare dacă emailul reprezintă metoda cea mai adecvată de a transmite un mesaj. Datele cu caracter personal sau informaţiile confidenţiale vor fi transmise ca ataşamente parolate, parola fiind comunicată separat (preferabil verbal) sau printr-un alt mesaj.

(16) Utilizatorii care nu sunt siguri cu privire la adecvarea mesajelor care urmează a fi transmise prin email se vor consulta cu reprezentanţii conducerii Asociaţiei (superiorul ierarhic / directorul general / Preşedintele) anterior demarării activităţii respective.

(17) Un email nu trebuie considerat mai puţin formal decât o scrisoare. La transmiterea emailurilor către exterior, expeditorii vor fi atenţi să nu includă materiale care ar putea afecta negativ imaginea Asociaţiei sau relaţia acesteia cu membrii, colaboratorii, publicul larg sau instituţiile publice.

(18) La transmiterea unui email către mai mulţi destinatari, se va utiliza câmpul "BCC" / "CCI", astfel încât să nu fie divulgate altor persoane adresele de email ale destinatarilor. În caz contrar, vor fi încălcate principiile legate de protecţia datelor cu caracter personal, prevăzute de Regulamentul European 2016/679.

(19) Facilităţile IT puse la dispoziţie de Asociaţie nu vor fi folosite pentru:

- transmiterea de materiale nesolicitate cu caracter comercial sau de promovare, a scrisorilor înlănțuite (scrisori în care destinatarului i se solicită să retransmită mesajul unui anumit număr de persoane) sau de junk-mail de orice natură către alte organizații;
- transmiterea neautorizată (fără permisiunea conducerii Asociației) către o terță parte a unor materiale confidențiale legate de activitățile Asociației;
- transmiterea de materiale care ar putea încălca drepturile de autor, inclusiv drepturile de proprietate intelectuală;
- activități care irosesc în mod inutil eforturile personalului sau resursele rețelei sau activități care ar putea bloca în mod nerezonabil accesul altor utilizatori (transmiterea intensivă de emailuri într-un interval scurt de timp care poate bloca serverul de email);
- activități care corup sau distrug datele altor utilizatori;
- activități care afectează activitatea altor utilizatori;
- crearea sau transmiterea de imagini, date sau materiale cu caracter ofensator sau indecent;
- crearea sau transmiterea de materiale care pot cauza iritare, neplăceri sau anxietate;
- crearea sau transmiterea de materiale abuzive sau amenințătoare la adresa altor persoane sau menite să hărțuiască;
- crearea sau transmiterea de materiale discriminatoare sau care încurajează discriminarea pe criterii rasiale, etnice, de gen, orientare sexuală, dizabilități, opinii politice, confesiunea religioasă etc.
- crearea sau transmiterea de materiale defăimătoare;
- crearea sau transmiterea de materiale care includ afirmații false sau de natură a induce în eroare;
- utilizarea limbajului nepoliticos, inclusiv a unor termeni ofensatori sau condescendenți;
- activități care încalcă viața privată a altor utilizatori;
- divulgarea către terți a conținutului unor mesaje confidențiale destinate doar unei anumite persoane, fără consimțământul autorului;
- crearea sau transmiterea de mesaje anonime (fără identificarea explicită a expeditorului);
- crearea sau transmiterea de materiale care pot afecta negativ imaginea Asociației.

VI. Junk Mail-urile

(20) Pot exista situații în care utilizatorii adreselor de email puse la dispoziție de Asociație vor primi mesaje nesolicitate de tip junk mail sau spam, în pofida eforturilor administratorului de rețea de a le filtra din server.

(21) Înainte de comunicarea adresei de email către o terță parte, de pildă prin intermediul unui site web, utilizatorii trebuie să ia în considerare posibilitatea ca aceasta să fie făcută cunoscută (poate chiar vândută sub forma bazelor de date) unei terțe părți necunoscute și să ia în calcul dacă eventualele beneficii compensează potențialele probleme.

(22) Scrisorile înlănțuite nu trebuie redirecționate utilizând sistemele IT sau facilitățile puse la dispoziție de Asociație.

VII. Mărimea căsuței de email

(23) Pentru asigurarea disponibilității serviciului de email și a bunei funcționări a acestuia, este recomandabil ca utilizatorii să evite transmiterea mesajelor inutile, în special a celor cu atașamente de mari dimensiuni (de exemplu, fișiere de tip .ppt sau .pps de peste 1 MB). În mod special, va fi evitată transmiterea unor astfel de mesaje către grupuri de adrese de e-mail, situație care ar putea duce la blocarea serverului pentru un anumit interval de timp.

(24) Utilizatorii au la dispoziție o dimensiune limitată a căsuței de email, pentru a reduce problemele asociate cu capacitatea serverului. Utilizatorii trebuie să își administreze conturile de email pentru a se încadra în limitele dimensiunilor căsuței, asigurându-se că mesajele sunt arhivate sau șterse când nu mai sunt necesare.

(25) Emailurile pot fi folosite ca mijloc de a transfera fișiere sau alte mesaje integrate în corpul mesajului sau atașate mesajului. Atunci când este necesară transmiterea unui document către o altă persoană (în special documente de mari dimensiuni), este de preferat transmiterea unei referințe cu privire la locul în care este disponibil fișierul în locul unei copii a documentului în sine, pentru a evita încărcarea excesivă a sistemului și atingerea limitei maxime de dimensiune a căsuței de email a destinatarului.

VIII. Administrarea și monitorizarea conturilor de email

(26) Utilizarea emailului se înregistrează centralizat, prin intermediul panoului de control al platformei de email, de unde pot fi gestionate redirecționările automate și dimensiunile căsuțelor de email.

(27) În cazul în care utilizarea căsuțelor de email se apropie de capacitatea maximă sau o depășește, administratorul de rețea poate interveni pentru deblocarea conturilor sau pentru a mări dimensiunea acestora.

(28) În aceste situații, administratorul de rețea este posibil să șteargă mesajele de tip spam și junk, fără însă a monitoriza conținutul acestora. Utilizatorii trebuie să fie conștienți de această eventualitate și să prevină acumularea de mesaje până la limita maximă a conturilor de email pentru a evita ștergerea unor mesaje importante care pot ajunge accidental în folderele de spam sau junk, în special în perioada concediilor când se acumulează un volum mare de corespondență în server.

(29) În situații excepționale care ar putea implica investigarea utilizării neautorizate a emailului sau soluționarea unei cercetări întreprinse de către autorități judiciare (poliție, instanțe de judecată, parchete ș.a.), poate fi posibilă monitorizarea traficului aferent unui anumit cont de email (mesajele transmise și primite). Monitorizarea conținutului mesajelor va fi realizată doar de persoane strict desemnate pentru acest scop (administratorul de rețea), conform atribuțiilor prevăzute de fișa postului sau de contractul de prestări servicii, în baza unei solicitări scrise din partea Directorului General.

(30) În orice alte situații, accesul la contul unui utilizator (angajat, membru al Consiliului director sau al grupurilor de lucru) este strict interzis, cu excepția cazului în care acesta și-a dat consimțământul sau dacă emailul trebuie accesat de către superiorii ierarhici pentru scopuri specifice, pe durata absenței utilizatorului (concediu etc.).

(31) În cazurile prevăzute la art. (29) și (30) este necesară transmiterea unei solicitări scrise către administratorul rețelei IT din partea Directorului General pentru a se asigura astfel respectarea drepturilor și libertăților fundamentale ale persoanei. Vor fi deschise doar mesajele care sunt relevante și strict necesare pentru îndeplinirea activităților/scopurilor sau obligațiilor legale ale Asociației.

IX. Confidențialitatea

(32) Toți angajații au responsabilitatea de a păstra confidențialitatea informațiilor la care pot avea acces în exercitarea atribuțiilor lor de serviciu. La această obligație generală se adaugă responsabilitățile specifice care derivă din legislația protecției datelor cu caracter personal. În cazul în care un angajat nu are certitudinea că poate comunica anumite informații, va consulta Directorul General sau responsabilul cu protecția datelor.

(33) Personalul Asociației va depune eforturi pentru a asigura păstrarea confidențialității emailurilor. Angajații trebuie să fie conștienți că un mesaj nu este șters din sistem până când toți destinatarii mesajului sau redirecționărilor nu au șters copiile lor. În plus, confidențialitatea nu poate fi asigurată atunci când mesajele sunt transmise prin intermediul unor rețele externe (cum ar fi internetul) datorită naturii nesigure a acestora.

(34) Se va proceda cu atenție la introducerea adreselor de email în câmpul *"Către"* pentru a preveni astfel transmiterea accidentală către alți destinatari decât cei avuți în vedere, în special în cazul aplicațiilor care completează automat câmpul de adresă atunci când utilizatorul începe să tasteze un nume.

X. Transmiterea din neglijență a virusurilor informatice

(35) Având în vedere că virusurile informatice se transmit cu ușurință prin intermediul emailului sau a descărcărilor de pe internet, va fi utilizat software-ul antivirus pus la dispoziție de Asociație iar orice suspiciune pe care un utilizator o are cu privire la o posibilă infectare a calculatorului va fi raportată administratorului rețelei IT.

(36) Pentru mai multe instrucțiuni în acest sens, utilizatorii vor consulta Politica de securitate a datelor cu caracter personal.

XI. Utilizarea emailului în scop personal

(37) Utilizarea în scop personal a contului de email pus la dispoziție de Asociație este permisă dar se recomandă să fie realizată în limite rezonabile. Accesul la alți furnizori de servicii de email precum Gmail sau Yahoo se va face prin internet, cu respectarea prevederilor din secțiunea B a acestei politici, referitoare la utilizarea în scop personal a internetului. Această facilitate se bazează pe încredere în utilizatori și pe responsabilitate din partea acestora.

SECȚIUNEA B –INTERNETUL

XII. Scopul facilitării accesului la Internet

(38) Serviciul de Internet este pus la dispoziția utilizatorilor (angajații, vizitatorii sediilor ANEVAR etc.) pentru:

- accesarea de informații relevante pentru îndeplinirea activităților și scopurilor Asociației;
- publicarea de informații pe site-urile web ale Asociației și actualizarea acestora;
- posibilitatea de a face achiziții online de bunuri și servicii pentru Asociație.

XIII. Utilizarea în scop personal a serviciului de Internet pus la dispoziție de Asociație

(39) Accesul la Internet în scop personal se poate face în limite rezonabile de durată și grad de solicitare a rețelei, recomandabil în afara programului normal de lucru sau în timpul pauzelor, pentru a nu limita viteza de upload/download în detrimentul altor utilizatori și pentru a nu interfera negativ cu îndeplinirea atribuțiilor de serviciu.

(40) În cazul achizițiilor online de bunuri sau servicii în interes personal, prin intermediul conexiunii de Internet a Asociației, utilizatorii se vor asigura că informațiile necesare derulării tranzacției sunt furnizate în nume propriu și nu în numele Asociației.

(41) Asociația nu își asumă nici o responsabilitate privind eventualele daune, pierderi, distrugeri sau pretenții financiare care ar putea deriva din tranzacțiile respective.

XIV. Administrarea, securitatea și monitorizarea utilizării serviciului de Internet

(42) Facilitatea de acces la Internet aparține Asociației iar traficul general este înregistrat de furnizorul serviciului de Internet și poate fi interogat, atât de provider cât și de administratorul rețelei IT, cu scopul monitorizării utilizării

abonamentului de date, astfel încât să nu existe sincope și/sau o capacitate insuficientă (viteză mică de transfer etc.).

(43) În situații excepționale care ar putea implica prevenirea unor incidente și breșe de securitate (de genul accesării unor site-uri rău intenționate care pot virusa nu doar computerul conectat ci și întreaga rețea IT a Asociației), traficul Internet poate fi monitorizat de către administratorul rețelei IT care, în caz de necesitate, poate bloca accesul unui anumit utilizator (identificat după I.P.) la aceste site-uri.

(44) Utilizatorii trebuie să conștientizeze riscurile la care se expun când accesează site-uri sau link-uri nesigure și să ia act de faptul că istoricul lor de navigare pe Internet ar putea fi monitorizat.

(45) Următoarea listă, cu toate că nu este exhaustivă, oferă exemple de site-uri nepotrivite a căror accesare este descurajată prin această politică:

- pariuri online
- jocuri online
- site-uri cu conținut nepotrivit care poate fi considerat ilegal, obscen sau ofensator
- site-uri care promovează ura, discriminarea și violența
- site-uri care promovează armele și hacking-ul
- dating online etc.

SECȚIUNEA C – COMUNICAȚIILE MOBILE

XV. Serviciile de telefonie mobilă puse la dispoziție de ANEVAR

(46) Acolo unde este necesar pentru îndeplinirea scopurilor și activităților sale, Asociația va pune la dispoziția angajaților, a membrilor Consiliului director și a membrilor consiliilor filialelor telefoane mobile/tablete și cartele sim.

(47) Achiziția și distribuirea dispozitivelor mobile și a cartelelor către utilizatori se face de către un angajat ANEVAR care are prevăzută această atribuție în fișa postului.

(48) În cazul defectării echipamentelor, a pierderii sau furtului acestora, utilizatorii vor notifica de îndată persoana responsabilă. Asociația are responsabilitatea atât pentru apelurile efectuate până în momentul blocării

cartelelor cât și pentru datele cu caracter personal ale contactelor stocate în memoria terminalelor mobile sau pe simuri (nume, numere de telefon, adrese de email).

(49) Terminalele și cartelele defecte, pierdute sau furate vor fi înlocuite, în limita stocului disponibil și într-o perioadă de timp rezonabilă dar cât mai rapid cu putință, pentru a nu afecta activitatea curentă a utilizatorilor.

(50) În eventualitatea pierderii sau furtului telefonului mobil (este cazul telefoanelor inteligente), utilizatorul va proceda, în măsura posibilităților, la ștergerea de la distanță a informațiilor de pe terminal, cu ajutorul aplicațiilor specializate:

- pentru telefoanele cu sistem de operare Android se poate descărca de pe Google Play aplicația *Android Device Manager* care permite localizarea de la distanță și resetarea la valorile din fabrică;
- pentru telefoanele cu sistem de operare IOS, se va proceda la autentificarea în icloud - https://www.icloud.com/#find și la ștergerea de la distanță a datelor stocate pe acestea.

(51) La terminarea relațiilor de muncă, telefonul mobil sau tableta, cartela sim și orice alt accesoriu (încărcător, baterie, dongle etc.) vor fi predate în ultima zi lucrătoare către angajatul care are în atribuții gestionarea echipamentelor mobile. În nici o situație, aceste echipamente nu vor fi transferate unui alt angajat. Echipamentele mobile realocate unui alt utilizator vor fi resetate la valorile din fabrică pentru a fi șterse toate datele cu caracter personal care ar putea fi stocate pe acestea.

XVI. Utilizarea telefoanelor în scop personal

(52) Utilizarea în scop personal a serviciilor de telefonie mobilă puse la dispoziție de Asociație este permisă dar se recomandă să fie realizată în limite rezonabile. În mod similar cu utilizarea emailului, această facilitate se bazează pe încredere în utilizatori și pe responsabilitate din partea acestora.

(53) Monitorizarea apelurilor primite și efectuate de utilizatori nu este permisă, având în vedere că în numeroase situații este foarte dificilă realizarea unei distincții clare între utilizarea serviciilor de comunicații mobile puse la dispoziție de Asociație în interes de serviciu și utilizarea în interes personal (conform Opiniei 2/2017 despre procesarea datelor la locul de muncă emisă de Grupul de lucru WP 249) și că o asemenea monitorizare poate aduce atingere vieții private și drepturilor și libertăților fundamentale ale persoanelor fizice.

SECȚIUNEA D – PAROLELE

XVII. Parolele de acces

(54) Parolele reprezintă un aspect important al securității computerelor. Ele sunt prima linie de protecție pentru conturile de utilizatori. O parolă prost aleasă poate conduce la compromiterea întregii rețele IT a Asociației. Prin urmare, toți angajații și terții care au acces la sistemele IT ale Asociației au responsabilitatea de a urma pașii corespunzători, prezentați în cele ce urmează, pentru a-și alege și securiza parolele.

a) Pentru Staff-ul IT

Toate parolele de sistem (root, administrare servere și site, Windows admin, control panel etc.) vor fi schimbate la maxim șase luni. Parolele vor fi stocate într-o manieră sigură și vor fi disponibile pentru restabilirea în caz de incidente și pentru asigurarea continuității activității.

b) Pentru utilizatori

- parolele de utilizatori (email, acces pe site în contul de utilizator, computer etc.) vor fi schimbate la maxim trei luni.
- conturile de utilizator care au privilegii speciale (de tip administrator) vor avea o parolă distinctă (unică) de celelalte conturi deținute de acel utilizator.
- parolele de acces nu trebuie inserate în cadrul mesajelor transmise prin email sau prin alte forme de comunicare electronică.

XVIII. Îndrumar pentru construirea parolelor

(55) Parolele sunt necesare pentru diferite scopuri. Unele dintre cele mai comune utilizări includ conturile de utilizator, conturile web, conturile de email, protecția ecranului etc. Prin urmare, fiecare utilizator trebuie să știe cum să construiască o parolă puternică.

(56) Parolele slabe au următoarele caracteristici:

- parola conține mai puțin de 7 caractere;
- parola este un nume de familie, prenume etc.;
- parole este un cuvânt comun care figurează în dicționar;
- parola conține data nașterii sau alte date personale care pot fi asociate facil cu utilizatorul ;

- succesiuni sau tipare de litere sau cifre de genul 12345, 123321, qwerty, abcd etc.

(57) Parolele puternice au următoarele caracteristici:

- conțin atât caractere scrise cu litere mici cât și cu majusculă;
- conține semne de punctuație sau simboluri, în combinație cu litere și cifre (de exemplu K_lm&#@0-9);
- cuprind cel puțin 12 caractere alfanumerice;
- nu reprezintă un cuvânt dintr-o limbă, dialect, argou, jargon etc.
- nu se bazează pe date cu caracter personal, nume de familie etc.

(58) Parolele nu trebuie notate sau stocate on-line. Se recomandă alegerea unor parole care să poată fi ușor memorate. O metodă ar fi crearea unei parole bazate pe titlul unui cântec, pe un proverb, o poveste sau o frază. Un exemplu de acest fel poate fi "Albă ca Zăpada și cei Șapte Pitici" iar parola poate fi A1c2Z3&c4S5P6 sau orice altă variație.

(59) Nu vor fi utilizate parole comune pentru conturile Asociației și conturile personale (de exemplu, conturi de email, conturi de utilizator al unui magazin sau serviciu online, de internet banking etc.) întrucât atunci când o parolă este compromisă pot fi afectate toate conturile în care autentificarea se face pe baza acelei parole

(60) Acolo unde este posibil, nu va fi utilizată aceeași parolă pentru conturi diferite ale Asociației (de exemplu, contul de administrare a site-ului și contul de control panel al serverului de email).

(61) Toate parolele vor fi considerate informații confidențiale și nu vor fi comunicate altor persoane, inclusiv colegilor. Nu vor fi date indicii cu privire la formatul parolelor (de exemplu, numele de familie).

(62) Parolele nu trebuie notate sau salvate pe computer în fișiere necriptate.

(63) În cazul în care există suspiciunea că o parolă a fost compromisă, incidentul va fi raportat administratorului rețelei IT iar parolele vor fi schimbate deîndată.

SECȚIUNEA E – UTILIZAREA MEDIILOR DE STOCARE MOBILE

XIX. Mediile de stocare mobile

(64) Mediile de stocare mobile reprezintă un mijloc flexibil de transfer al datelor însă, ca orice alte echipamente, și acestea trebuie gestionate în mod corespunzător, astfel încât să fie asigurată securitatea informațiilor. Un mod inadecvat de utilizare și control al acestor medii de stocare poate duce la compromiterea întregii rețele IT a Asociației și la pierderi de date.

(65) Mediile de stocare mobile includ, fără a se limita la acestea, următoarele tipuri de suporturi:

- Discuri optice (CD-uri, DVD-uri+R/RW, discuri BluRay, Minidiscuri etc.)
- Hard-disk-uri externe
- Memorii USB Flash
- Carduri de memorie (SD Card, inclusiv Mini și Micro SD, xD Card etc.)
- Microcipuri încorporate (inclusiv Smart Carduri și cartele SIM)
- Playere audio și video (MP3, MP4)
- Camere digitale
- Benzi audio (inclusiv roboți telefonici și reportofoane)
- Telefoane mobile etc.

XX. Securitatea datelor de pe mediile de stocare mobile

(66) Datele stocate într-un singur loc și într-un singur format sunt mult mai expuse riscului de a deveni indisponibile sau corupte în urma pierderii, distrugerii sau defectării echipamentului pe care sunt păstrate față de datele pentru care se fac frecvent copii de siguranță. Prin urmare, mediile de stocare mobile nu trebuie să fie unicul loc în care sunt păstrate date importante prelucrate de Asociație. Copiile datelor salvate pe mediile de stocare mobile trebuie păstrate pe sistemul / computerul sursă sau pe un server de rețea până în momentul în care datele sunt transferate cu succes pe computerul de destinație.

(67) Documentele păstrate pe mediile de stocare mobile care conțin date cu caracter personal trebuie protejate cu parolă.

XXI. Măsuri antivirus și Malware

(68) Înainte de utilizare, toate echipamentele mobile vor fi scanate împotriva amenințărilor de tip virus informatic sau malware, folosind versiunile actualizate ale programelor antivirus instalate pe computerele Asociației.

(69) În cazul în care nu este disponibil un program antivirus și există suspiciuni că suportul de date ar putea fi infectat, va fi contactat administratorul rețelei IT care va proceda la o scanare amănunțită a dispozitivului, utilizând un computer care nu este conectat la rețea.

XXII. Eliminarea mediilor de stocare scoase din uz

(70) Toate echipamentele de stocare mobile care nu mai sunt necesare sau care s-au defectat vor fi returnate administratorului rețelei IT pentru eliminarea în siguranță a acestora. În scopul prevenirii scurgerii de date, conținutul anterior al acestor medii de stocare va fi șters pentru a preveni eventualitatea nedorită în care datele șterse să poată fi recuperate folosind un software specializat.

XXIII. Responsabilitatea utilizatorilor

(71) Prevederile acestei politici se aplică în toate situațiile în care sunt utilizate mediile de stocare mobile în derularea activităților Asociației. La folosirea stick-urilor USB, a CD-urilor, DVD-urilor sau cardurilor de memorie se va acorda o atenție specială următoarelor aspecte:

- mediile de stocare mobile utilizate în conexiune cu echipamentele sau rețeaua Asociației sau utilizate pentru a stoca informații necesare activităților oficiale ale Asociației vor fi achiziționate și instalate prin intermediul serviciilor IT;
- datele stocate pe mediile mobile vor fi parolate sau criptate, în măsura posibilităților;
- la conectarea mediilor mobile la un computer, se va proceda mai întâi la scanarea antivirus și antimalware pe un sistem dedicat, neconectat la internet sau rețeaua locală, pentru a nu compromite alte computere și integritatea datelor stocate pe acestea ;
- mediile de stocare mobile nu vor fi utilizate pentru arhivarea înregistrărilor ca alternativă la alte medii de stocare;

- mediile de stocare mobile nu vor fi lăsate la vedere. Se recomandă ca acestea să fie tratate ca un portofel – ținut într-un loc sigur atunci când nu este folosit;
- se recomandă minimizarea cantității de date stocate pe medii mobile și a perioadei de timp în care datele sunt păstrate pe acestea;
- mediile de stocare mobile sunt în responsabilitatea utilizatorilor și nu vor fi împrumutate sau oferite altor persoane;
- se vor lua măsuri pentru protecția fizică a mediilor de stocare mobile și pentru a preveni pierderea, alterarea și furtul datelor.

XXIV. Validitatea politicii (versiunea 1 – 2019)

Această politică a intrat în vigoare la data de ..... și va fi verificată și actualizată periodic de responsabilul cu protecția datelor.