**ANEXA 20 - CONDITII DE SECURITATE CIBERNETICĂ**

Contractantul poate accesa sistemele Achizitorului numai dacă este autorizat de Achizitor. Contractantul este responsabil pentru activitățile desfășurate în sistemele Achizitorului prin utilizarea identității sale digitale, care ar trebui să fie protejată în orice moment. În desfășurarea acestor activități, Contractantul trebuie să respecte următoarele reguli de conduită:

* + 1. a) să nu dezvăluie și să nu furnizeze niciodată datele de autentificare nimănui;
    2. b) să nu introducă parole în mesajele de e-mail sau în alte forme de comunicare electronică și să nu le dezvăluie nimănui la telefon;
    3. c) să nu memoreze niciodată parolele pentru a accesa aplicațiile Achizitorului prin intermediul browserului prin intermediul funcționalității „remember password” (memorarea parolei);
    4. d) să verifice dacă nu-l urmărește nimeni atunci când tastează acreditările pentru a accesa dispozitivele sau sistemele IT, pentru a preveni furtul datelor de autentificare;
    5. e) să nu utilizeze niciodată aceeași parolă pentru autentificarea la sisteme diferite;
    6. f) accesul la sistemele informatice se limitează la programele/instrumentele furnizate special pentru desfășurarea activităților necesare; este interzisă utilizarea serviciilor de rețea sau a conexiunilor în scopuri care nu au legătură cu activitățile care trebuie desfășurate;
    7. g) nicio tranzacție desfășurată prin intermediul sistemelor Achizitorului nu trebuie să încalce legea;
    8. h) postul de lucru utilizat (permanent sau temporar) nu trebuie să se conecteze la alte servicii de internet decât cele furnizate sau autorizate de Achizitor și trebuie să aibă instalat antivirusul necesar. Se iau toate măsurile necesare pentru a preveni răspândirea virușilor, a programelor malițioase sau a oricăror programe ilicite care pot provoca întreruperi ale serviciului sau pierderi de date;
    9. i) toate conturile de e-mail, platformele de stocare a fișierelor sau de comunicare (inclusiv rețelele de socializare) trebuie să fie furnizate sau autorizate în mod explicit de Achizitor;
    10. j) datele sensibile se stochează, se transmit sau se anulează cu ajutorul unui software de codare adecvat;
    11. k) este interzisă modificarea configurației sistemului pentru a evita controalele de securitate;
    12. l) pentru a preveni dezvăluirea de informații către persoane neautorizate, se acordă atenție documentelor tipărite, hard disk-urilor detașabile, dispozitivelor de stocare amovibile și ecranelor video.