**Anexa 2**

Cerinţe de securitate cibernetică

Modernizare sisteme de stingere incendiu în spațiile tehnice de nivel central

1. Cerinţe software

Executantul va asigura documentarea programelor software/firmware instalate pe computerele de monitorizare livrate, fişiere de configuraţie runtime, baze de date, etc. Listing-ul va include toate porturile şi serviciile autorizate pentru operare.

1. Controlul accesului

Executantul va asigura conturi de utilizatori cu acces configurabil şi privilegii diferite pentru grupuri de utilizatori creaţi conform sarcinilor din organizaţie.

Executantul va asigura un mecanism de administrare pentru efectuarea modificărilor de privilegii pentru diferiţi utilizatori/grupuri de utilizatori.

Executantul va verifica şi va documenta faptul că nu sunt instalate dispozitive de înregistrare/ raportare (ex. key loggere, camere web, microfoane etc.).

1. Managementul conturilor de utilizator

Executantul va documenta toate conturile de utilizatori (incluzându-le, dar fără a se limita la cele generice şi/sau prestabilite) ce necesită activare pentru funcţionarea normală a produselor livrate.

Executantul va modifica setările conturilor de utilizatori astfel încât parolele asociate să îndeplinească cerinţele Beneficiarului: minim 8 caractere, minim o majusculă, minim o cifră, parola să difere de ultimele 5 de parole utilizate.

1. Managementul sesiunilor

 Executantul nu va permite logarea simultană a mai multor utilizatori folosind aceleaşi date de autentificare, memorarea informaţiilor de login de către aplicaţii, completarea automată în timpul logării sau logării de tip anonim.

 Executantul va asigura configurarea delogării automate a conturilor sau grupurilor de utilizatori în cazul deconectării sesiunilor de comunicaţie sau a expirării timpului alocat.

1. Politici şi management de autentificare/parolare

Executantul va documenta nivelurile și metodele de autentificare și autorizare. Executantul va livra un produs ce aderă la protocoalele de autentificare standard.

 Executantul va asigura un sistem configurabil de management a parolelor conturilor utilizatorilor, astfel încât să permită cel puţin următoarele:

* modificări de parole (inclusiv parole implicite);
* selecţia numărului de caractere al parolelor;
* frecvenţa modificărilor;
* setări a complexităţii necesare a parolelor;
* număr de încercări de autentificare până la blocarea contului respectiv;
* delogare pentru sesiuni inactive;
* blocarea ecranului de către aplicaţie;
* comparare cu o bibliotecă/bază de date de şiruri de caractere interzise;
* utilizare derivată a numelui de utilizator;
* interzicerea folosirii repetate a aceleiaşi parole sau a parolelor folosite anterior.

 Executantul va asigura posibilitatea unui management al conturilor atât local, cât şi centralizat.

1. Detectarea malware-urilor şi protejarea la acestea

 Executantul va asigura sau va preciza modalitatea de implementare a funcţiei de scanare automată a tuturor dispozitivelor mobile ce intră în contact cu produsele livrate.

1. Accesul fizic la sisteme

 Executantul va asigura facilităţi de închidere sau blocare a accesului fizic la produsele livrate şi la sistemele ce conduc/supervizează accesul fizic al acestora.