Instruirea angajaților cu privire la modul de utilizare şi exploatare a tehnicii de calcul şi a aplicatiilor software, în scopul evitării apariţiei incidentelor de securitate

Privind respectarea prevederilor *Regulamentului (UE) 2016/679 al Parlamentului European şi al Consiliului din 27 aprilie 2016 privind protecţia persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal şi privind libera circulaţie a acestor date şi de abrogare a Directivei 95/46/CE (Regulamentul general privind protecţia datelor) pus în aplicare prin Legea nr.190/2018* .

1. Reguli

Trebuie (Este permis)

a). Echipamentele trebuie scoase de sub tensiune la sfarsitul fiecarei zile de lucru, daca nu este specificat altfel;

b) La inchiderea sesiunii de lucru tehnica de calcul va fi oprita folosind pasii standard ai sistemului de operare si nu deconectandu-le brusc de sub tensiune;

c) Intretinerea tehnicii de calcul trebuie facuta de catre persoane autorizate;

d) In cazul in care constatati o functionare anormala a unui echipament trebuie sa anuntati persoana desemnata pentru intretinerea acesteia: responsabilul cu mentenanta; in nici un caz nu se admite dezasamblarea sau desigilarea tehnicii de calcul de catre utilizatori in vederea detectarii/ remedierii problemei aparute;

e) Cand terminalele nu sunt folosite temporar, acestea trebuie protejate printr-un mecanism de incriptare a ecranului si a tastaturii cu parola, similar mecanismului de autentificare a utilizatorului;

f) Periodic, tehnica de calcul se va sterge de praf la exterior si in zonele accesibile.

Nu trebuie (Nu este permis)

a) Nu este permisa scoaterea brusca de sub tensiune a tehnicii de calcul;

b) Nu este permis consumul de alimente si bauturi in apropierea tehnicii de calcul;

c) Nu este permisa schimbarea configuratiei tehnicii de calcul fara acordul persoanelor autorizate (conducerea SNSPA)

2. Alegerea parolelor

Parolarea se poate realiza atat pentru accesul la tehnica de calcul (computer) , cat si pentru aplicatii si documente.

Pentru a nu facilita aflarea parolelor de catre alte persoane, utilizatorii trebuie sa tina cont de urmatoarele **recomandari**:

a) **Nu folositi cuvinte uzuale** – cuvintele uzuale sunt usor de descoperit;

b) Numele dvs., al prietenilor, al partenerilor, datele aniversare, numerele de masina, numerele de telefon sunt primele incercate pentru a descoperi parolele;

c) Alegeti parole de minimum 8 caractere;

d) **Trebuie utilizate acronime, litere aleatorii, etc, sau inserate caractere alfanumerice in interiorul cuvintelor, inlocuiti litere cu numere** (O cu 0, i cu 1, e cu 3, etc). ;

e) Utilizati **cOmBiNaTiI** de litere mici si MARI;

f) **Includeti o cifra** (0-9) in parola;

g) Daca este posibil, **includeti un simbol in parola** (!@#$%^&*()_+=.,;\<> etc);

h) Cand schimbati o parola schimbati cel putin doua caractere;

i) **Alegeti o parola pe care o puteti tine minte**;

j) **Este interzisa notarea parolelor pe biletele, post-it-uri si pastrarea la vedere a acestora** (monitoare, tastaturi), telefoane mobile, etc;

k) **Nu divulgati parola dvs. si nu permiteti nimanui sa se logheze cu userul si parola dvs.;**

l) Evitati sa lasati alte persoane sa priveasca cand introduceti parola;

m) Schimbati parola la 60 de zile.

3. E-mail

Fiecare utilizator este responsabil pentru securitatea informatiilor primite si transmise. Securitatea este responsabilitatea fiecaruia.

Fiecare utilizator este obligat sa verifice confidentialitatea datelor primite sau transmise.

Utilizatorii trebuie sa foloseasca posta electronica a organizatiei numai in beneficiul SNSPA.

Daca se observa ceva neobisnuit (neconformitate, potential risc, incident), utilizatorul trebuie sa anunte seful direct.

Cand angajatii SNSPA utilizeaza posta elecronica trebuie sa respecte urmatoarele reguli:

Trebuie (este permis):

a) Se va verifica frecvent e- mailul, pentru a vedea daca sunt mesaje noi;

b) Toate mesajele transmise vor avea in campul „SUBIECT„ un subiect, care sa faca referire la continutul mesajului;

c) Inainte de a transmite un mesaj, utilizatorii vor verifica daca adresa la care doresc sa transmita acel mesaj este a persoanei potrivite;

d) Utilizatorii vor sterge mesajele care nu necesita a fi pastrate, pentru a nu ocupa spatiul alocat primirii informatiilor;

e) Utilizatorii vor folosi semnatura standard a companiei pentru a semna toate e-mailurile de serviciu.

Nu este permis:

a) Listarea e-mailurilor, decat daca acest lucru este absolut necesar;

b) Utlizarea e-mailului in scopuri personale;

c) Trimiterea e-mailurilor cu atasamante foarte mari;

d) Transmiterea e-mailurilor ce contin materiale pentru adulti, continut pedofilic sau ce contin informatii despre droguri, rasism, terorism, violent;

e) Incercarea logarii cu ID-ul si parola altcuiva;

f) Folosirea conturilor de mail internet base (gen gmail, hotmail, yahoo).

4. Utilizare Internet

Trebuie (Este permis):

a) Trebuie folosit internetul doar in interes de serviciu;

b) Trebuie verificat daca orice informatie folosita este corecta, actuala si completa;

c) Trebuie verificat daca informatia gasita este valida;

d) Trebuie respectate legile dreptului de autor referitoare la informatia, software-ul, etc gasite si utilizate

Nu trebuie (Nu este permis):

a) Nu este permisa folosirea internetului in scop personal;

b) Nu este permis accesul la site-uri cu continut pentru adulti, continut pedofilic sau ce contin informatii despre droguri, rasism, terorism, violenta, etc.;

c) Nu este permisa down-loadarea (descarcarea) si instalarea pe calculator a software-lor (programelor) de pe internet;

d) Nu este permisa utilizarea computerelor apartinand SNSPA, pentru accesul neautorizat in alte calculatoare sau retele;

e) Nu este permisa utilizarea identitatii altei persoane (nu va dati drept altcineva).

5. Responsabilitatea Utilizatorilor

Accesul la internet, daca ai adresa de e-mail @snspa.ro. Sunt urmarite aspectele:

f) Fiecare utilizator este responsabil pentru securitatea informatiilor si datelor pe care le detine si utilizeaza. Securitatea este responsabilitatea fiecaruia;

g) Fiecare utilizator este obligat sa verifice confidentialitatea datelor. Pentru siguranta, se intreaba seful ierarhic, pentru ca informatia este o resursa, uneori o resursa nepretuita (poate implica costuri sau castiguri foarte mari) ;

h) Utilizatorii trebuie sa foloseasca resursele puse la dispozitie numai in beneficiul SNSPA;

i) Fiecare utilizator este responsabil pentru ceea ce face in cadrul sistemului informatic;

j) Daca se observa ceva neobisnuit (neconformitate, potential risc, incident) , utilizatorul trebuie sa anunte pe seful direct.

Când utilzati resursele informatice apartinand SNSPA trebuie sa respectati urmatoarele reguli:

Trebuie (Este permis):

a) Trebuie sa alegi o parola ce va fi greu de intuit;

b) Trebuie sa blocati sa sa va delogati inainte de a parasi statia de lucru;

c) Trebuie sa protejati echipamentele contra furtului si sa le tineti la distanta de alimente si bauturi;

d) Trebuie sa va asigurati ca peiodic sunt facute copii de siguranta . Solicitati asistenta companiei daca nu stiti sa faceti copii de siguranta;

e) Sa va asigurati ca toate mediile de stocare sunt scanate antivirus inainte de utilizare in cadrul SNSPA;

f) Trebuie sa informati persoanele responsabile in domeniu, din cadrul SNSPA, daca considerati ca o statie de lucru poate fi virusata.

Nu trebuie (Nu este permis):

a) Nu trebuie sa va notati parolele;

b) Nu trebuie sa spuneti parola;

c) Nu trebuie sa permiteti altora sa priveasca atunci cand lucrati cu informatii confidentiale;

d) Nu trebuie sa folositi aplicatii shareware (aplicatii de pe internet, CD/DVD-urile diverselor reviste) ;

e) Nu trebuie sa copiati aplicatiile software;

f) Nu trebuie sa instalati orice software pe computer si nu modificati configuratia acestuia.

6. Securitatea fizica si a mediului de lucru

Fiecare utilizator al echipamentului informatic trebuie sa respecte urmatoarele reguli:

a) Sunteti responsabil pentru securitatea bunurilor, informatiilor si datelor pe care le detineti si utilizati. Securitatea este responsabilitatea fiecaruia;

b) Trebuie sa intelegi ca tu esti responsabil pentru ceea ce faci;

c) Daca observi ceva neobisnuit anunta-l pe seful direct.

In acest sens trebuie sa aveti in vedere:

Trebuie (Este permis):

a) Vizitatorii trebuie sa se inregistreze la receptie si trebuie sa fie insotiti;

b) Se inregistreaza data si ora de sosire si plecare al vizitatorilor;

c) Trebuie sa se ia masuri de precautie suplimentare pentru accesul la zonele unde exista informatii sensibile, trebuie controlat si limitat;

d) Toti angajatii, partenerii, vizitatorii trebuie sa poarte elemente vizibile de identificare (legitimatii);

e) Daca intalnesc persoane care nu poarta elemente vizibile de identificare trebuie sa informeze persoana responsabil cu securitatea sau seful direct;

f) Birourile si incaperile trebuie securizate prin incuiere;

g) Echipamentele ce contin informatiile de siguranta (back-up) trebuie amplasate in locatii sigure (la distanta suficient de mare de amplasamentul principal, de exemplu seif banca, pentru a preveni pierderea acestora in cazul uni incendiu, inundatie, explozie);

h) Nu este permisa utilizarea echipamentelor de inregistrare audio, video, foto decat daca sunt autorizate;

i) Echipamentele trebuie montate astfel incat sa fie minimizat riscul potentialelor amenintari fizice cum ar fi: inundatiile, praful, vibratiile, furtul, focul etc.;

j) Vizitatorii nu trebuie sa vada ecranele calculatoarelor cu excepţia cazului în care în mod specific sunt instalate pentru a asista clientul;

k) Calculatoarele personale şi staţiile de lucru trebuie să fie alimentate doar pana la sfârşitul fiecărei zile, dacă nu există alte instrucţiuni;

l) Echipamentele critice trebuie prevazute cu unitati de alimentare, cu energie electrica fara intrerupere (UPS);

m) Documentele continand informatii personale, confidentiale si sensibile trebuie sa fie distruse folosind echipamente dedicate, utilizand tehnici specifice care sa faca imposibila recuperararea

datelor de pe mediile de stocare magnetice sau optice. Acest lucru poate fi realizat si prin intermediul unui partener;

n) Este interzisa utilizarea functiunilor standard de stergere sau formatare astfel incat sa nu fie recuperate prin procedee speciale de restaurare a informatiei;

o) Vor fi inregistrate echipamentele cand sunt mutate in afara locatiei si inregistate din nou cand sunt returnate;

p) Interventiile asupra echipamentelor (intretinerea, service-ul) vor fi realizate numai de persoane autorizate;

q) Nu vor fi lasate informatii sensibile sau importante pe birouri, in imprimante, fax-uri