Politica Securitatii Informatiei

1.DECLARATIA DE POLITICA

"Este responsabilitatea departamentului de infrastructura IT sa asigure protectia adecvata si confidentialitatea tuturor datelor si sistemelor software ale companiei, sa asigure disponibilitatea continua a datelor si a programelor personalului autorizat si sa asigure integritatea datelor.

Angajatul este responsabil pentru datele pe care le gestioneaza pe statiile si sistemele Creativ Tub in conformitate cu NDA semnat si cu politica actuala."

Sumar al principalelor Politici de Securitate

Pentru sustinerea securitatii infrastructurii IT, politica noastra se concentreaza pe urmatoarele aspecte principale:

1.1 Confidentialitatea tuturor datelor trebuie mentinuta prin discretie.
1.2 Accesul la Internet sau la alte servicii externe este oferit angajatilor Creativ Tub prin intermediul prin controlul si managementuui departamentului de Infrastructura IT.
1.3 Accesul la date pe toate computerele trebuie securizat prin encriptie, pentru a mentine confidentialitatea datelor in cazul pierderii sau furtului echipamentelor.
1.4 Vor fi instalate pe echipamente doar aplicatiile licentiate si aprobate de catre departamentul de Infrastructura IT
1.5 Toate removable media din surse externe vor fi scanate cu antivirusul aprobat in organizatie inainte de a fi utilizate
1.6 Parolele trebuie sa contina un minim de 10 caractere alfanumerice si sa fie unice.
1.7 Parolele trebuie schimbate o data la 3 luni.
1.8 Configuratia statiilor de lucru va fi modificata doar cu suportul departamentului de Infrastructura IT.
1.9 Atunci cand folositi un instrument gratuit, este interzisa partajarea datelor prin intermediul platformei respective.
1.10 Creativ Tub interzice utilizarea echipamentelor personale in interes de munca. Doar echipamentele companiei (calculatoare, hardware si software aprobate) sunt autorizate pentru activitati legate de servicii oferite clientilor Creativ Tub.
1.11 Toate instrumentele de comunicare si operationale trebuie aprobate de companie. Pentru a obtine cea mai buna productivitate, instrumentele aprobate trebuie sa combine securitatea si eficienta.
1.12 Utilizarea echipamentelor companiei in interes personal este strict interzisa.
1.13 Utilizarea necorespunzatoarea a echipamentelor Creativ Tub reprezinta o incalcare a acestei Politici de Securitate si poate atrage masuri disciplinare.

2. PROTECTIA ANTIVIRUS

Declaratiile cheie referitoare la acest aspect sunt enumerate mai jos si trebuie respectate de toti angajatii Creativ Tub, in conformitate cu rolul lor.

2.1 Personalul de Infrastructura IT va avea disponibila o solutie antivirus actualizata pentru scanarea si eliminarea virusilor suspectati. Acest software va fi disponibil pentru toti angajatii Creativ Tub.

2.2 Toate serverele de fisiere ale companiei vor fi protejate cu software de scanare antivirus.

2.3 Toate statiile de lucru trebuie sa aiba instalata si activa solutia antivirus aprobata de Creativ Tub

2.4 Solutia antivirus va fi actualizata cu cele mai recente versiuni in mod regulat pe toate statiile si serverele active.

2.5 Toti angajatii trebuie sa fie atenti la email-urile spam primite. Nu accesati link-uri necunoscute.

2.6 Toate "removable media" aduse din afara organizatie vor fi scanate inainte de utilizare.

2.7 Nu sunt permise aplicatii de tip shareware, acestea fiind una dintre cele mai commune surse de infectie.

2.8 Solutiile software nou-instalate vor fi scanate inainte de utilizare.

2.9 Conducerea companiei sustine cu fermitate politicile antivirus ale Organizatiei si pune la dispozitie resursele necesare pentru implementare.

2.10 Utilizatorii vor fi informati cu privire la procedurile si politicile actuale de catre personalul Administrativ.

2.11 Angajatii vor fi responsabili pentru orice incalcare a politicilor antivirus ale Organizatiei.

2.12 In cazul unei posibile infectii cu virus a unei statii de lucru, utilizatorul trebuie sa informeze imediat departamentul de Infrastructura IT.

3. CONTROLUL ACCESULUI

Mediul de lucru online impune o politica de control a accesului foarte bine definite, aceasta fiind detaliata in paragrafele urmatoare.

3.1 Utilizatorilor li se vor acorda doar drepturile minime suficiene necesare pentru a le permite sa isi desfasoare activitatea asupra sistemelor.

3.2 Accesul la retea / servere se va face prin nume de utilizatori si parole individuale.

3.3 Numele de utilizator si parolele nu vor fi notate. Parolele trebuie stocate in instrumente dedicate gestionarii acestora (ex. KeePass).

3.4 Fiecare utilizator al statiilor de lucru trebuie sa aiba configurata o parola puternica (parola alfanumerica de celputin 10 caractere) pentru a preveni accesul neautorizat.

3.5 Departamentul IT va fi informat in cazurile in care angajatii parasesc Organizatia, pentru a elimina drepturile si accesele din toate sistemele utilizate.

3.6 Parolele de management ale retelei / serverelor vor fi stocate intr-o locatie sigura in caz de urgenta sau dezastru, de exemplu, baza de date KeePass.

3.7 Toate proiectele si datele companiei vor fi stocate pe resurse detinute de Creativ Tub.

4. SECURITATEA RETELEI LOCALE

4.1 Echipamentele LAN vor fi pastrate in incaperi securizate, incuiate in orce moment. Accesul va fi limitat doar personalului Administrativ.

4.2 Utilizatorii trebuie sa se deconecteze sau sa isi blocheze statiile cand pleaca pentru orice perioada de timp.

4.3 Toate statiile de lucru nefolosite trebuie oprite in afara programului de lucru.

4.4 Utilizatorii nu vor plasa sau depozita niciun fel de articol deasupra cablurilor de retea.

4.5 Toate serverele vor fi tinute in siguranta, sub cheie.

4.6 Accesul la consola de sistem si server va fi limitat personalului autorizat Administrativ.

4.7 Toate serverele si echipamentele de retea vor fi echipate cu Uninterruptable Power Supply (UPS).

4.8 Toate UPS-urile vor fi verificate periodic.

4.9 Departamentul Administrativ va tine un inventar complet al tuturor echipamentelor informatice si al software-ului folosit in companie.

4.10 Auditarea hardware si software va fi efectuata periodic.

5. SECURITATEA SERVERELOR

Aceasta sectiune este aplicabila serverelor Windows si Linux.

5.1 Toate sistemele de operare vor fi actualizate periodic.

5.2 Serverele vor fi scanate periodic in vederea eliminarii potentialilor virusi.

5.3 Serverele vor fi stocate in interiorul unei incaperi securizate (incuiate).

5.4 Utilizatorii trebuie sa se deconecteze sau sa blocheze statiile cand pleaca pentru orice perioada de timp.

5.5 Toate conturile vor fi configurate cu parole de minimum 10 caractere.

5.6 Vor fi folosite parole unice.

5.7 Numarul de grace logins va fi limitat la 3.

6. SECURIATEA Wireless LAN – WLAN

6.1 Retelele LAN fara fir vor folosi cele mai sigure facilitate de criptare si autentificare posibile.

6.2 Toate bridge-urile, routerele si gateways vor fi tinute incuiate in interiorul unei incaperi securizate.

7. TRANSFERUL DATELOR SI INFORMATIILOR

7.1 Transferul de date si informatii trebuie sa fie criptat si protejat cu parola; acolo unde criptarea nu este posibila, transferal de date si informatie trebuie sa se face cel putin protejat cu parola.

7.2 Datele cu caracted personal pot fi transferate in afara Uniunii Europene respectand nivelul adecvat de protective ale acestora.