POLITICA DE REALIZARE A COPIERII DATELOR

1. Scop

Politica de copiere a datelor furnizează o documentație cuprinzătoare a reglementărilor aplicabile în companie și măsurile luate pentru back-upul datelor. De asemenea, aceasta servește ca dovada terțelor parți, conform cărora controlul disponibilității legale necesare este efectuat corect.

2. Responsabilități in cadrul companiei

Companiile trebuie să asigure securitatea IT și backup-ul datelor.

Conducerea corporatistă este direct responsabilă pentru acest lucru și este responsabilă personal atunci când este aplicabilă.

3. Condiții legale generale

Legea impune anumite controale prin măsuri tehnice și organizatorice, atât cu prelucrarea datelor în scopuri proprii, cât și cu prelucrarea datelor comandate; în acest context, se aplică, în special, un control al disponibilității.

Verificarea controalelor sau a măsurilor tehnice și organizatorice trebuie, printre altele, să fie oferită clienților în cadrul prelucrării datelor comandate.

4. Riscuri

Eroare umană: funcționare incorectă / accident, sabotaj, atac

Întreruperi tehnice: defecțiuni tehnice, defecțiuni hardware, tulburări de linie

Forță majoră, accidente, catastrofe: apă, incendiu etc.

Posibile efecte existente amenințătoare asupra companiilor

5. Proceduri de backup de date, opțiuni

- Suport complet
- Backup incremental
- Backup diferențial

6. Reglementări tehnice și organizatorice minime

6.1 Reglementări generale

- Suportul de date trebuie să fie efectuat în mod responsabil și competent
- Fără ocolirea accidentală a modelelor de autorizare prin măsuri de salvare a datelor
- Confidențialitatea și obligația de protecție a datelor
- Nominalizarea persoanelor responsabile pentru fiecare domeniu de activitate
- Determinarea nevoii de confidențialitate, integritate și disponibilitate

6.2 Implementarea tehnică

- Crearea planului de salvare a datelor
- Determinați perioada de păstrare și numărul de generații
- Coordonarea cu politica de prevenire a situațiilor de urgență
- Documentație și înregistrare suficientă: în special date de rezervă, domeniu de rezervă, parametri de rezervă
- Aranjați procedura de recuperare
- Crearea directorului de inventar
- Asigurați evaluarea bușteniilor
- Teste privind reconstrucția / restaurarea datelor și exercițiile de urgență
- Configurați comenzile necesare, în special controlul accesului
- Implementarea cerințelor de protecție pentru confidențialitate, integritate și disponibilitate
- Specificați și asigurați căile de transport
- Alocați capacitățile: capacitatea de transfer, volumul, cantitatea de dispozitive de stocare a datelor
- Implementarea cerințelor de copiere de rezervă (calculatoare mobile, PDA / MDA, baze de date, fișiere deschise, date de sistem, date din jurnal etc.)

Asigurați-vă, în special, controlul accesului, controlul permisiunilor de acces, controlul transmisiei, controlul de intrare și controlul separării, inclusiv în ceea ce privește seturile de backup de date.