Politica de securitate fizică

1. Introducere

1) Protecția mediului fizic este una dintre cele mai importante sarcini în domeniul securității informațiilor. Lipsa controlului accesului fizic poate determina inutilitatea celor mai atente precauții tehnice și poate pune în pericol securitatea informațiilor confidențiale.

2) Instituția se angajează să asigure siguranța angajaților săi, a cetățenilor, a contractanților și a bunurilor și acordă o foarte mare importanță problemei securității fizice. Această politică ce stabilește principalele măsuri de precauție care trebuie luate, împreună cu documentele prezentate, formează un întreg care cuprinde setul de măsuri al securității informațiilor.

3) Aceste măsuri se aplică tuturor sistemelor, persoanelor și proceselor care intră în legătură cu sistemele informatice ale organizației, inclusiv membrii consiliului administrativ, directorii, angajații, furnizorii și alte părți terțe care au acces.

2. Zone securizate

1) Informațiile sensibile trebuie să fie stocate în siguranță. În ideea identificării unui nivel necesar de protecție care trebuie pus în aplicare pentru asigurarea stocării informațiilor, este imperios necesară efectuarea unei evaluări a riscurilor.

2) Securitatea fizică trebuie să pornească de la însăși protecția clădirii și trebuie efectuată o evaluare a vulnerabilității perimetrului. O clădire trebuie să dispună de mecanisme adecvate de control pentru păstrarea în siguranță a informațiilor confidențiale și a echipamentelor care sunt stocate în cadrul acesteia.

3) Acestea pot include cele de mai jos, lista nefiind exhaustivă:

a) Alarme montate și activate în afara programului de lucru
b) Blocări pentru ferestre și uși
c) Mecanisme de control al accesului montate pe toate ușile accesibile (unde sunt utilizate codurile, acestea trebuie schimbate în mod regulat și cunoscute numai de persoanele autorizate să acceseze zona / clădirea)
d) Camere CCTV
e) Zonă de recepție personală
f) Protecție împotriva deteriorării - de ex. incendiu, inundații, vandalism

1) Personalul care lucrează în zone sigure trebuie să restricționeze accesul persoanelor neautorizate.

2) Instrumentele de identificare și de acces (de exemplu, insigne, chei, coduri de intrare etc.) trebuie să fie deținute numai de persoane autorizate să acceseze zonele respective și nu trebuie împrumutate / furnizate nimănui altcuiva.

3) Vizitatorii în zonele securizate sunt obligați să declare ora de sosire și plecare și trebuie să poarte o insignă de identificare.

4)Cheile către toate zonele securizate care găzduiesc echipamente tehnice și departamentele tehnice sunt păstrate în condiții de maximă securitate.

5) În cazul în care există încălcări ale măsurilor sau un angajat și-a depășit competențele încredințate, toate instrumentele de identificare și de acces (de exemplu, insigne, chei etc.) trebuie recuperate de la angajat și toate codurile de acces trebuie schimbate imediat.

3. Securitatea documentelor și echipamentelor

(1) Documentele care conțin informații confidențiale (altele decât cele electronice) trebuie protejate prin măsuri adecvate precum:

a) Zone de depozitare blocate;
b) Seifuri încuiate;
c) Stocarea într-o zonă sigură cu acces neautorizat.

2) Toate echipamentele informatice trebuie amplasate în locații fizice adecvate care:

a) Limitează riscurile cauzate de pericolele de mediu - de ex. căldură, foc, fum, apă, praf și vibrații;
b) Limitează riscul de furt - de exemplu dacă elementele necesare, cum ar fi laptopurile, trebuie atașate fizic la birou;
c) Permit posturilor de lucru care manipulează date sensibile să fie poziționate astfel încât să elimine riscul ca datele să fie văzute de persoane neautorizate.

3) Documentele trebuie să fie stocate și electronic. Acest lucru
asigură că informațiile pierdute, furate sau deteriorate prin acces neautorizat pot fi restaurate și integritatea lor este menținută.

4) Toate serverele situate în afara centrului de date trebuie amplasate într-un mediu sigur din punct de vedere fizic.
5) Sistemele critice pentru întreprinderi trebuie să fie protejate de o sursă de alimentare continuă pentru a reduce riscul de corupție a sistemului de operare și a datelor din cauza unor defecțiuni de alimentare.
6) Toate echipamentele trebuie înregistrate într-un inventar. Este necesară existența unor proceduri pentru a garanta faptul că inventarul este actualizat de îndată ce activele sunt primite sau eliminate.
7) Toate echipamentele trebuie să fie denumite și să aibă un număr unic alocat. Acest număr de activ trebuie înregistrat în inventar.
8) Sistemele care transportă trebuie să fie protejate împotriva interceptării neautorizate sau deteriorării.
9) Cablurile de alimentare trebuie să fie separate de cablurile de rețea. Cablurile de rețea trebuie să fie protejate prin conducte și, acolo unde este posibil, să se evite rutele prin zone publice.

4. Gestionarea ciclului de viață al echipamentelor

1) Furnizorii de servicii trebuie să se asigure că toate echipamentele informatice ale instituției sunt menținute în conformitate cu instrucțiunile producătorului și cu toate procedurile interne documentate pentru a se asigura că acestea rămân în stare de funcționare eficientă.

2) Personalul implicat în întreținere trebuie să:

a) Păstreze toate copiile instrucțiunilor producătorului
b) Identifice intervalele și specificațiile recomandate
c) Activeze un proces de apel în caz de eșec
d) Să se asigure că numai tehnicienii autorizați finalizează orice lucrare cu privire la echipament
e) Înregistreze detaliile tuturor lucrărilor de remediere efectuate
f) Identifice cerințele de asigurare
g) Înregistreze detaliile defecțiunilor și acțiunilor necesare

3) Trebuie să se păstreze o evidență a istoricului de funcționare a echipamentului, astfel încât să se poată lua decizii cu privire la momentul oportun al înlocuii acestuia.
4) Instrucțiunile de întreținere ale producătorului trebuie să fie documentate și disponibile pentru ca personalul de asistență să le poată utiliza la efectuarea reparațiilor.
5) Utilizarea echipamentelor în afara amplasamentului trebuie să fie aprobată oficial de către managerul de linie al utilizatorului.

6) Echipamentele care trebuie reutilizate sau eliminate trebuie să aibă toate datele șterse/ distruse. În cazul în care echipamentul urmează să fie transferat către o altă organizație (de exemplu returnat în baza unui contract de leasing), eliminarea datelor trebuie realizată utilizând instrumente software aprobate, în mod corespunzător, în siguranță.
7) Zona de încărcare și instalațiile de depozitare trebuie să fie protejate în mod corespunzător împotriva accesului neautorizat.
8) Îndepărtarea ulterioară a echipamentului trebuie să se realizeze printr-un proces formal.
9) Modalitățile de securitate a informațiilor trebuie să facă obiectul unor audituri regulate și independente.

5. Consecințe

1) Nerespectarea prezentei Politici de către angajații instituției sau alți colaboratori externi poate conduce către sancțiuni disciplinare (inclusiv încetarea contractului de muncă), rezilierea contractelor și, în funcție de circumstanțe, acționarea în instanță pentru recuperarea integrală a prejudiciilor aduse ca urmare a nerespectării prezentei Politici.

2) Când există suspiciunea unor activități ilegale (cum ar fi, exemplificativ, sustragerea documentelor, copierea, distribuirea, transferul bazelor de date), instituția va denunța activitatea infracțională organelor legii pentru tragerea la răspundere penală a făptuitorului.

3) Prezenta Politică va fi adusă de către conducere la cunoștința tuturor angajaților, colaboratorilor, partenerilor de afaceri sau a altor terți