

Politica privind utilizarea dispozitivelor de supraveghere si inregistrare video

PRIMARIA COMUNEI GÂRLENI

1. Introducere

Dispozitivele de supraveghere si inregistrare video reprezintă o componentă tot mai des intalnita in viata de zi cu zi a unei localitati. Pe măsură ce capacitățile de supraveghere si de stocare a imaginilor cresc, în mod evident, cresc și riscurile.

Ca exemple de locuri in care aceste dispozitive sunt amplasate, putem enumera:

- Primarie.
- Institutii de invatamant.
- Strazi.
- Parcuri si locuri de joaca
- Cimitire.
- Alte institutii publice aflate in subordinea primariei (biblioteci, politie locala, cluburi sportive etc).

Scopul acestei politici este de a stabili măsurile care trebuie să fie utilizate atunci când se utilizează dispozitivele de supraveghere si inregistrare video. Se intenționează să se reducă următoarele riscuri:

- Pierderea sau furtul dispozitivelor de supraveghere si inregistrare video, inclusiv datele pe care acestea le conțin.
- Compromiterea informațiilor clasificate prin acces neautorizat.
- Introducerea în rețea a virusilor sau a programelor malware.
- Pierderea reputației.

Este important ca măsurile stabilite în această politică să fie respectate în orice moment în utilizarea și functionarea dispozitivelor de supraveghere si inregistrare video.

Această politică se aplică tuturor departamentelor, persoanelor și proceselor care constituie sistemele dispozitivelor de supraveghere si inregistrare video, precum si sistemelor informatice ale organizației, inclusiv membrii consiliului, directorii, angajații, furnizorii și alte părți terțe care au acces la sistemele si dispozitivele instituției.

2. Politica privind securitatea informației colectata si stocata cu ajutorul dispozitivelor de supraveghere si inregistrare video

1. Accesul la echipamentele organizației de către terți se va face sub supraveghere. În contractele cu terți se vor include clauze privind măsurile de protecție a datelor și, în special, a datelor cu caracter personal;
2. Informațiile vor avea diferite grade de sensibilitate și importanță, informațiile personale (datele cu caracter personal) necesitând un nivel suplimentar de protecție (fisier video);
3. Responsabilitatea angajaților privind securitatea va fi implementată încă din etapa recrutării și inclusă în contractele de muncă sau fișă a postului și monitorizată permanent;
4. Parolele utilizate pentru autentificare sunt șiruri de caractere, adecvate din punct de vedere al securității ca lungime și compoziție, conținând majuscule și caractere speciale și sunt formate din cel puțin 8 caractere. Acestea sunt schimbate periodic, cel puțin o dată la două luni. Schimbarea periodică a parolelor se face numai de către utilizatori autorizați.
5. Angajații instituției sau alte terțe părți care au acces la dispozitivele instituției ar trebui să semneze un contract de confidențialitate;
6. Angajații ar trebui să fie instruiți cu privire la Securitatea Informațiilor;
7. Toate incidentele de Securitate vor fi raportate conducerii, pentru a decide dacă este cazul ca acestea să fie raportate Autorității de Supraveghere și/sau persoanelor vizate. Se va implementa în acest sens o Politică privind managementul adecvat al incidentelor de Securitate;
8. Dispozitivele de supraveghere și înregistrare video vor fi protejate împotriva amenințărilor de Securitate și se vor implementa măsuri de securitate pentru a preveni și detecta accesul neautorizat la acestea și asupra datelor colectate.
9. Trebuie să se introducă proceduri pentru efectuarea de back-up strategic, simularea periodică a restaurării de pe copii realizate, logarea evenimentelor și a defectelor, acolo unde este posibil și monitorizarea permanentă a echipamentelor critice.
10. Utilizarea oricărui dispozitiv de supraveghere și înregistrare video va fi conformă legislației în vigoare cât și a normelor interne.
11. Este strict interzisă orice modificare neautorizată a echipamentelor utilizate;
12. Este strict interzisă conectarea echipamentelor personale de orice fel (hard-diskuri interne sau externe, memory stick, laptop etc) la orice dispozitiv de supraveghere și înregistrare video al organizației. (Nerespectarea acestei reguli aduce după sine posibilitatea desfacerii contractului de muncă sau alte măsuri disciplinare.
13. Este strict interzisă utilizarea dispozitivelor de supraveghere și înregistrare video în alte scopuri decât îndeplinirea atribuțiilor de serviciu.
14. Este interzisă orice intervenție asupra dispozitivelor de supraveghere și înregistrare video de către personal neautorizat de către instituție în mod scris.
15. Fiecare angajat va fi responsabil să mențină securitatea oricărei informații, și în special informațiilor personale (datelor cu caracter personal) și să le protejeze de acces neautorizat (vizualizare, alterare, furt sau distrugere).

16. Pentru copierea fișierelor electronice, instituția își rezervă dreptul de a depune plângere penală împotriva angajatului și de a-l acționa pe acesta la instanțele civile pentru acoperirea oricărui prejudiciu adus instituției.
17. Personalul care asigură suportul tehnic nu va avea acces la date cu caracter personal, decât în situații excepționale și, în toate cazurile, cu respectarea tuturor obligațiilor impuse de Regulamentul (EU) 679/2016 persoanelor împuternicire și, în special, existența unor clauze contractuale exprese privind protecția datelor.
18. Nu se va elimina niciun semn de identificare de pe dispozitiv, cum ar fi o etichetă a instituției sau o serie. Se vor lua măsuri ca dispozitivul să fie inaccesibil publicului larg și protejat
19. Dispozitivele nu trebuie să fie conectate la rețele publice, cum ar fi wireless sau Internet, cu excepția cazului în care este utilizată o rețea VPN (Virtual Private Network/Rețea Virtuală Privată).
20. Aceste aspecte trebuie luate în considerare atunci când se evaluează caracterul adecvat al oricărui dispozitiv de a stoca datele confidențiale ale organizației.
21. Este politica instituției să evalueze fiecare cerere de acces la datele colectate prin dispozitivele de supraveghere și înregistrare video în mod individual, pentru a stabili:
 - identitatea persoanei care face cererea
 - motivul cererii
 - datele care vor fi păstrate sau procesate
 - dispozitivul specific care va fi utilizat
22. Pentru a asigura că datele sale sunt protejate în mod adecvat, este important ca instituția să poată monitoriza și să verifice nivelul de conformitate cu această politică. Nivelul de monitorizare și de audit va fi adecvat clasificării informațiilor deținute pe dispozitiv.
23. În cazul în care dispozitivul este deteriorat sau furat, personalul responsabil trebuie să informeze conducerea cât mai curând posibil, oferind detalii despre circumstanțele pierderii și sensibilitatea informațiilor stocate pe acesta.

3. Consecințe

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 instituției ca urmare a nerespectării prezentei Politici. 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.

Prezenta Politică va fi adusă de către conducerea instituției la cunoștința tuturor angajaților, colaboratorilor sau a altor terți.