ROMÂNIA
JUDEŢUL BRAŞOV
PRIMĂRIA ORAŞULUI GHIMBAV
str. Lungă nr. 2, Ghimbav, cod 507075, jud. Bra;ov, România
Tel./Fax: 40-268-258006 / 40-0268-258355
www.primaria-ghimbav.ro e-Mail: relatiipublice@primaria-ghimbav.ro

POLITICA DE SECURITATE
A ORAŞULUI GHIMBAV

Oraşul Ghimbav se angajează să asigure siguranţa angajaţilor, a contractanţilor şi a bunurilor şi acordă o foarte mare importanţă problemei securităţii. Aceste măsuri se aplică tuturor sistemelor, persoanelor şi proceselor care intră în legătură cu sistemele informatice ale unităţii.

Această procedură este destinată utilizării de către Primăria Ghimbav, atunci când o persoană vizată exercită unul sau mai multe drepturi în temeiul **Regulamentului (UE) 679/2016**.

Scopul acestei politici este de a menţine un nivel adecvat de securitate pentru a proteja datele cu caracter personal, precum şi sistemele informatice împotriva accesului neautorizat.

Această politică defineşte regulile necesare pentru a asigura această protecţie şi pentru a asigura o funcţionare sigură şi fiabilă a sistemelor informatice din primărie. Numai utilizatorii autorizaţii au acces la sistemele informatice, acţiunile lor asupra documentelor fiind permise prin aplicaţii specifice şi aprobate cu diferite niveluri de acces.

Accesul la sistemul informatic se realizează pe baza unui ID unic pentru fiecare utilizator.

Această politică se aplică tuturor calcuatoarelor, dispozitivelor şi sistemelor informatice deţinute sau operate de Oraşul Ghimbav. Această politică se aplică tuturor sistemelor de operare şi tuturor sistemelor de aplicaţii.

Orice utilizator care trebuie să acceseze reţelele şi sistemele informatice ale unităţii, trebuie să treacă prin procesul de autentificare. Nivelul de autentificare trebuie să fie ridicat. Autentificarea va include, dar nu se va limita la:

- un identificator unic pentru utilizator;
- deconectare automată.

Parolele utilizate sunt şiruri de caractere, adecvate din punct de vedere al securităţii ca lungime şi caractere speciale. Parolele nu sunt afişate pe monitor. Acestea se schimbă la 3 luni.

Accesul la informaţii:

- mijloace de autentificare în sistem;
- este strict interzisă utilizarea credenţialelor ce aparţin altui angajat;
- fiecare angajat va fi responsabil să menţină securitatea informaţiilor şi să le protejeze de accesul neautorizat (furt, distrugere);
- trebuie obţinută aprobarea din partea proprietarului informaţiei înainte de crearea, modificatrea sau ştergerea unei autorizaţii de acces;
- este interzisă copierea de fişiere electronice;
- este interzisă navigarea prin fişierele persoanelor sau prin conturile altor angajaţi;
- personalul care asigură suportul tehnic nu va avea acces la date cu caracter personal.

Accesul la sistem:

- Notarea sau stocarea parolelor pe orice suport fizic este strict interzisă;

- Sistemul trebuie blocat ori de câte ori angajatul părăseşte biroul;
- După terminarea programului, calculatoarele vor fi închise.

Este interzisă utilizarea PrintScreen-ului, sau fotografierea monitorului cu telefonul pentru a salva datele cu caracter personal.

Listarea documentelor ce conţin date cu caracter personal se va realiza doar de către utilizatorii autorizaţi.

Nivelul de protecţie şi securitate al prelucrărilor de date cu caracter personal trebuie să fie proporţional cu nivelul riscului pe care îl comportă prelucrarea datelor respective cu caracter personal faţă de drepturile şi libertăţile persoanelor.

Zone securizate

Informaţiile sensibile trebuie să fie stocate în siguranţă. Securitatea fizică trebuie să pornească de la însăşi protecţia clădirii şi trebuie efectuată o evaluare a vulnerabilităţii perimetrului. Acestea pot include:

- alarme;
- blocări pentru ferestre şi uşi;
- mecanisme de control al accesului montate pe toate uşile;
- protecţie împotriva deterirorării (incendiu, inundaţii);
- instrumentele de identificare şi de acces (chei, coduri de intrare), trebuie să fie deţinute numai de persoanele autorizate să acceseze zonele respective.

Securitatea documentelor şi echipamentelor

Documentele care conţin confidenţialitate trebuie protejate prin măsuri adecvate:

- zone de depozitare blocate;
- seifuri încuiate;
- stocarea într-o zonă sigură de acces neautorizat.

Documentele trebuie să fie stocate şi electronic. Acest lucru asigură faptul că informaţiile pierdute, furate sau deteriorate prin acces neautorizat, pot fi restaurate şi integritatea lor este menţinută.

Scopul prelucrării prin mijloace video

Primăria Ghimbav, prelucrează date cu caracter personal, respectiv imaginea prin intermediul sistemelor video, în scopul monitorizării accesului persoanelor în instituţie.

Amplasarea camerelor de supraveghere a fost realizată în conformitate cu legislaţia în vigoare.

Se supraveghează prin mijloace video:

- zonele de acces şi spaţiile destinate publicului;
- zonele cu acces restricţionat.

Inspector
Clarisa DOBRIN
SPCLEP Ghimbav

PRIMAR
Ionel FLIUNDRA