*Traducere din limba italiană*

**Protecția Datelor și Reguli de Securitate**

FOGLIANI SA – FUTURTEC SRL

FOGLIANI ROMANIA

**CONTROL DOCUMENT**

|  |  |  |  |
| --- | --- | --- | --- |
| Cod DOCUMENT | nivel de Revizie1.0 | Data emiterii7 martie 2019  | TIP de DOCUMENTPOLItica |

***Cuprins***

[1 INTRODUCERE 3](#_Toc6243133)

[1.1 SCOP 3](#_Toc6243134)

[1.2 DESTINATARI 3](#_Toc6243135)

[1.3 REVIZII ȘI ACTUALIZĂRI ALE DOCUMENTULUI 3](#_Toc6243136)

[2 REFERINȚE LEGISLATIVE 4](#_Toc6243137)

[2.1 Legislația privind protecția datelor personale (Regulamentul European 2016/679) 4](#_Toc6243138)

[2.2 Modificări și completări ale codului penal și ale codului de procedură penală privind infracționalitatea informatică, Legea n. 547 din 1993 6](#_Toc6243139)

[2.3 Legislația privind drepturile de autor (Legea 633/41) 6](#_Toc6243140)

[2.4 Răspunderea Administrativă a Organizațiilor (Decr.leg. 231/2001) 7](#_Toc6243141)

[2.5 nerespectarea prezentelor norme de comportament 7](#_Toc6243142)

[3 ACCEPTAREA POLITICII 8](#_Toc6243143)

[3.1 Politica generală de securitate a datelor 8](#_Toc6243144)

[4 REGULI SPECIFICE 11](#_Toc6243145)

[4.1 Accesul fizic și logic 11](#_Toc6243146)

[4.2 instrumente de securitate 12](#_Toc6243147)

[4.3 îngresitrarea și stocarea datelor 15](#_Toc6243148)

[4.4 Gestionarea datelor pe suport de hârtie 16](#_Toc6243149)

[5 POLITICA DE FOLOSIRE A PAROLELOR DE ACCES 17](#_Toc6243150)

[5.1 Autentificare 17](#_Toc6243151)

[5.2 POLITICA de E-MAIL 20](#_Toc6243152)

[6 POLITICA de INTERNET 22](#_Toc6243153)

[7 VERIFICARE ȘI CONTROL 23](#_Toc6243154)

[7.1 Moduri de verificare 23](#_Toc6243155)

[7.2 Informații conf. art. 13 Regulamentul UE 23](#_Toc6243156)

[7.3 Sancțiuni 24](#_Toc6243157)

# INTRODUCERE

Acest document reprezintă regulamentul companiei Fogliani precum și a societăților/ filialelor acesteia, privind confidențialitatea și securitatea datelor cu caracter personal.

Pentru compania Fogliani securitatea informațiilor este o condiție necesară în atingerea obiectivelor instituției: protecția datelor companiei și a sistemelor informatice aferente permite companiei Fogliani să ofere servicii de calitate care să asigure fiabilitatea serviciului oferit.

Prin intermediul sistemelor informatice ale companiei, o serie de date cu caracter personal sunt tratate în raport cu legislația italiană și europeană privind confidențialitatea datelor și necesită punerea în aplicare a măsurilor tehnice și organizatorice de securitate, precum și implicarea activă a tratamentului respectiv, pentru asigurarea protecției adecvate a acestora.

Protecția datelor corporative depinde, în mod substanțial de respectarea normelor de comportament pentru a proteja confidențialitatea, integritatea și disponibilitatea în același timp (criteriul RID).

## SCOPUL

Întrucât aceasta este o politică și nu o procedură, nu sunt raportate activități și fluxuri de operațiuni specifice. Obiectivul principal al acestei politici este acela de a se asigura că toți utilizatorii își adaptează comportamentul în conformitate cu indicațiile detaliate de mai jos.

Acest lucru va contribui la atingerea obiectivelor de siguranță, rezumate în trei aspecte distincte:

* **Confidențialitatea,** cu scopul de a asigura prevenirea accesului ilegal sau neautorizat la informații, servicii și la sisteme
* **Integritatea**, cu scopul de a garanta că informațiile nu sunt alterate accidental sau abuziv.
* **Disponibilitatea** , cu scopul de a garanta accesul la informații și la serviciile din rețea de către personalul desemnat în raport cu nevoile de lucru.

## DESTINATARI

Prezentul document este destinat tuturor angajaților și colaboratorilor interni a societății FOGLIANI Spa, FUTURTEC Srl, FOGLIANI ROMANIA Srl

## REVIZII ȘI ACTUALIZĂRI ALE DOCUMENTULUI

Revizia și actualizarea prezentului document cade în sarcina Direcției Administrative și IT, care se bucură de sprijinul tuturor celorlalte structuri corporative în raport cu domeniile de competență.

# REFERINȚE LEGISLATIVE

Legislația italiană în ultimii ani a adoptat un set de reguli menite să ghideze companiile în realizarea unui echilibru între ceea ce tehnologiile se pot face și necesitatea de a proteja datele, care de multe ori nu aparțin persoanelor care le conduc.

Îndeplinind legislația cu privire la mijloacele de securitate a informațiilor, prin urmare, pentru a evita riscul legal sau de a suporta sancțiuni penale/administrative ca urmare a nerespectării legilor sau reglementărilor.

Referitor la subiectul siguranței datelor în companie, este posibilă sintetizarea reglementărilor legislative italiene și europene de referință, astfel:

* Regulamentul (UE) 2016/679 din 27 aprilie 2016, al Parlamentului și Consiliului European, referitor la protecția persoanelor fizice, cu referire la tratamentul datelor cu caracter personal.
* Codul de procedură privind protecție a datelor personale (Decretul Legislativ 196 din 30 iunie 2003), abrogat parțial și modificat cu Decretul 101/2018.
* Măsuri de respectare a Confidențialității
* Modificări și completări ale normativelor Codului penal și al Codului de procedură penală privind infracționalitatea informatică, Legea nr. 547 din 1993
* Legislația asupra drepturilor de autor (Legea 633/41)
* Decretul Legislativ 231 din 08/06/2001 asupra Responsabilității Administrative a Organizațiilor.

## Legislația privind protecția datelor personale (Regulamentul European 2016/679)

***General Data Protection Regulation (GDPR)***, sau Regulamentul UE nr. 679/2016 privind protecția datelor cu caracter personal (sau Politica de confidențialitate), a intrat în vigoare 24 mai 2016, și a devenit pe deplin eficient din 25 mai 2018, abrogând Directiva 95/46/CE, din care au rezultat în ultimii ani diferite legi naționale (inclusiv Codul de confidențialitate italian - Decretul Legislativ 196/2003).

Regulamentul privind protecția persoanelor fizice cu privire la prelucrarea datelor cu caracter personal și libera circulație a acestor date, prin care se înțelege că „orice informație referitoare la o persoană fizică identificată sau identificabilă.“

Nu mai este vorba doar o normă exclusiv legală, ci și de un impact economic, deoarece legiuitorul a intenționat să introducă normele necesare pentru a pune ordine în economia digitală, dominată de giganții web.

**Principii generale**

În fond, așa cum deja sancționează Decretul legislativ 196/2003, Regulamentul garantează că „protecția persoanelor fizice cu privire la prelucrarea datelor cu caracter personal este un drept fundamental.“

Legiuitorul are drept scop standardizarea aplicării protecției datelor cu caracter personal în cadrul Uniunii, pentru a asigura un nivel consecvent și ridicat de protecție a drepturilor și libertăților fundamentale ale persoanelor fizice, precum și pentru a elimina obstacolele din calea fluxurilor de date cu caracter personal în interiorul Uniunii.

Orice prelucrare a datelor cu caracter personal ar trebui să fie legală și corectă. Ar trebui să fie transparente pentru persoanele fizice, modurile în care sunt colectate, utilizate sau accesate toate datele cu caracter personal , inclusiv măsura în care datele personale sunt sau vor fi tratate.

Principiul de transparență impune ca informațiile și comunicările referitoare la tratamentul acestor date personale să fie accesate și înțelese cu ușurință, folosindu-se un limbaj simplu și clar.

Regulamentul European prevede printre pilonii săi principali și principiul **Responsabilității**  (care ar putea fi tradus ca „responsabilitatea și obligativitatea răspunderii “) referitor la toate subiectele.

Titularul datelor trebuie să fie în măsură să demonstreze că a adoptat un proces global juridic, organizatoric și tehnic, pentru protecția datelor cu caracter personal, inclusiv prin dezvoltarea unor modele specifice de organizare pentru a demonstra într-un mod pozitiv și pro-activ că prelucrarea datelor efectuate sunt adecvate și conforme.

**Noutăți din Europa**

Pe lângă principiul menționat deja și fundamental al Responsabilității, cu Regulamentul European au fost introduse unele noutăți interesante referitor la protecția datelor personale:

* „***Privacy Impact Assessment***" (evaluări preventive ale impactului asupra protecției datelor), în cazul unor tratamente riscante devine necesară o analiză detaliată a riscurilor. Textul Regulamentului menționează în mod expres parametrii de gravitate și probabilitatea evenimentului.
* Numirea unui „***Data Protection Officer****“* (responsabil pentru protecția datelor cu caracter personal), care trebuie să fie competent, independent și nu neapărat un intern al Organizației/Întreprinderii. Numirea acestuia este obligatorie în unele cazuri (de exemplu: tratamentele cu risc al datelor cu caracter personal), dar toate organizațiile au dreptul de a desemna această persoană pentru gestionarea corectă și eficientă a unui sistem de confidențialitate.
* “***Joint controllers****”* (Co-proprietarii) se vor putea împărți sau pot să împartă responsabilitatea confidențialității printr-un contract special, de care va trebui să se țină cont în cazul unor inspecții sau dispute. Această informație ar putea fi utilă, în special, în domeniul *cloud computing* (pana acum dificil încadrat în vechile tipare proprietar/responsabil).
* Conceptul de ”sediu principal” al titularului, pentru a evita ca o întreprindere activă în mai multe țări din UE să trebuiască să se ocupe de îndeplinirile naționale ale fiecărui stat în parte.
* Rolul de "*Lead Authority*", pentru a se asigura că există doar un singur Garant, la rândul său responsabil de procedurile care au un impact multi-stat.
* **Penalități** mult mai grele decât în ​​trecut: până la 4% din volumul de afaceri globale al unei întreprinderi. Scopul este în mod clar acela de a face ca protecția datelor să fie o problemă sensibilă, în special pentru marile companii multinaționale (cum ar fi *Google, Facebook, Microsoft*)
* Obligația de a urmări, în proiectarea de noi produse sau servicii, principiile „***Data Protection by Design***“ și „**Data Protection by *Default*** “, adică aplicarea protecției datelor din faza de proiectare a oricărui tratament.
* Dreptul de a uita, astfel încât orice parte interesată să poată solicita eliminarea datelor lor cu caracter personal din motive legitime (de exemplu, putem cere să fie „uitate“ on-line).
* ***Data Breach***, sau notificarea unei încălcări autorității, dacă este posibil, în termen de 72 de ore, și comunicarea acesteia celor interesați.

**Impactul asupra siguranței tratamentului**

La nivel comunitar normele privind securitatea datelor este menținută în forma sa generală; cu toate acestea, se introduce însă, o mai mare atenție la așa-numita *risk-based approach* și se precizează, în mod mai descriptiv și exemplificativ unele dintre cele mai importante tipuri de măsuri tehnice și organizatorice.

În plus, se acordă o mare importanță recunoașterii eficacității măsurilor de securitate adoptate (articolul 32, litera d.) și mai ales evaluării impactului (cunoscut sub numele de DPIA - *Data Protection Impact Assessment*) ca un instrument fundamental în cunoașterea situației actuale și a marjei de îmbunătățire a sistemului de confidențialitate. În general, se reafirmă unul dintre conceptele fundamentale ale securității informațiilor: asigurarea confidențialității, integrității și disponibilității (cunoscute sub acronimul RID).

Cum se pot urmări toate acestea? Regulamentul UE prevede responsabilitatea operatorilor de date sau a responsabililor, care au obligația de a adopta și menține documentația similară cu Documentul de politică de securitate, prevăzut de Decretul Legislativ 196/2003.

De exemplu există obligația de a ține un registru al activităților de tratament a datelor personale, care să conțină o descriere generală a măsurilor tehnice și organizatorice de siguranță, adoptate.

Formal, companiile mici care nu prezintă risc de tratament pot fi exceptate de la această cerință; este recomandabil însă, să se adopte astfel de înregistrări, care să permită oricărei situații să demonstreze în mod clar tipul de date cu caracter personal gestionate.

Rezumând, titularul și responsabilii tratamentului de date sunt obligați să ia măsuri organizatorice și tehnice de securitate pentru reducerea riscului, în conformitate cu o abordare pro-activă (*accountabilty*), identificând riscurile asociate tratamentului (c*.d. risk-based approach*), precum și adoptând măsuri adecvate care să țină seama de principiile transparenței, precum și de principiile confidențialității *by design (*confidențialitatea începând de la proiectare*)* și *by default*.

## Modificări și completări ale Codului penal și a Codului de procedură penală privind infracționalitatea informatică, Legea nr. 547 din 1993

Legea 547/93 a introdus conceptul de criminalitate informatică în cadrul normelor prevăzute de Codul penal și de Codul de procedură penală. În acest sens, a făcut posibilă urmărirea unor infracțiuni informatice, în același mod cu cel tradițional, prevăzând penalizări variabile până la maximum cinci ani de închisoare. Infracțiunile informatice și articolele din codul penal care au fost înlocuite sunt enumerate mai jos, după cum urmează:

* Atac în sistemele informatice de utilitate publică (art. 420)
* Falsificarea documentelor informatice (art.491, lit.b)
* Accesul abuziv în sistemul informatic sau telematic (art. 615, lit.c)
* Deținerea și difuzarea abuzivă a codurilor de acces în sistemele informatice sau telematice (art. 615 lit.d)
* Difuzarea de programe direcționate să distrugă sau să întrerupă un sistem informatic (art. 615 lit.e)
* Violarea corespondenței telematice (art. 616-617 lit.f)
* Interceptarea e-mailurilor (art. 617 lit.d)
* Deteriorarea sistemelor informatice și telematice (art. 635 lit.b)
* Frauda informatică (alterarea integrității datelor cu scopul de a obține foloase necuvenite (art. 640 lit.c)

Cunoașterea infracțiunilor, enumerate mai sus, permite utilizatorilor să prevină un posibil comportament infracțional în timpul utilizării instrumentelor informatice dar și să înțeleagă mai bine necesitatea de a aplica unele din regulile descrise mai jos.

## Legislația privind drepturile de autor (Legea 633/41)

Legea nr.633 din 22 aprilie 1941 care reglementează „Protecția drepturilor de autor și a altor drepturi referitoare la exercitarea ei“, revizuită prin Legea nr. 248 din18 august 2000 și cu ulteriorul Decret Legislativ n. 68 din 9 aprilie 2003, instituie sancțiuni administrative și penale pentru cei care încalcă drepturile de autor.

Conform acestei legi în cazul în care se constată folosirea ilicită a produselor software în către companie, poate fi tras la răspundere reprezentantul legal al companiei și eventual responsabilul serviciului informatic. În cazul în care se stabilește că infracțiunea a fost făcută direct de către companie, aceasta este responsabilă pentru utilizatorul final, în cazul în care se stabilește că acesta din urmă a introdus copii ilegale pe care le folosește în activitatea sa fără știrea companiei sau în contrast cu regulamentul în vigoare din cadrul companiei acesta va răspunde.

Utilizarea abuzivă de software implică astfel două tipuri de riscuri, una tehnică și una juridică:

* Riscuri de natură tehnică: utilizarea de programe contrafăcute în cadrul rețelei companiei poate duce la răspândirea virușilor și proasta funcționare a sistemelor companiei (pierderi de date și de funcționare) datorate copiilor incomplete și incompatibile între ele;
* Riscuri de natură juridică: în calitatea lor de lucrări de concepție, produsele software sunt protejate de regimul juridic ale dreptului de autor. Copierea și utilizarea produselor software fără a obține autorizația necesară din partea deținătorului drepturilor constituie o infracțiune. Riscurile juridice la care este expusă o astfel de infracțiune include sancțiuni civile și penale.

În ceea ce privește, însă, duplicarea ilegală a programelor de calculator, cei care comit această infracțiune riscă sancțiuni penale la care se poate adăuga și amenda, sau o amendă de până la de două ori prețul de piață al software-ului copiat ilegal.

FOGLIANI oferă utilizatorilor săi toate instrumentele software necesare pentru desfășurarea activității și asigură conformitatea acestora cu reglementările privind drepturile de autor. Prin urmare, utilizatorii trebuie să respecte cu strictețe normelor privind folosirea de software în cadrul companiei, cu scopul de a evita riscurile asociate introducerii unor programe neautorizate sau rău intenționate.

## Răspunderea Administrativă a Organizațiilor (Decr. Leg. 231/2001)

Decretul 231/2001 a introdus în legislația italiană răspunderea administrativă a organizațiilor pentru anumite infracțiuni și contravenții care, deși realizate material de persoane aflate în poziție de conducere sau angajați ai companiei pot fi trași la răspundere în mod direct atunci când au ”comis infracțiunile sau contravenții în interes personal”

Tipuri de infracțiuni prevăzute de Decr. Leg. 231/2001:

* Infracțiuni împotriva administrației publice
* Infracțiuni ale asociaților
* Infracțiuni cu bancnote false, cărți de credit sau bonuri valorice
* Infracțiuni de *insider trading* și *market abuse*
* Infracțiuni în scopuri de terorism

Pentru infracțiunile prevăzute în prezentul Decret, societatea este răspunzătoare numai în cazul în care comiterea infracțiunii a fost făcută din neglijență în conducere sau lipsa de supraveghere a activității. E exclusă omiterea acestor obligații în cazul în care, înainte de infracțiunea comisă, instituția a adoptat și a pus în mod eficient în aplicare o politică de management și control adecvat cu scopul de prevenire a circumstanțelor care au condus la infracțiune.

## Nerespectarea regulilor de conduită.

FOGLIANI își rezervă dreptul, în limitele permise de lege, să verificate aderarea la standardele actuale de verificare a funcționării corecte a activității sistemelor.

FOGLIANI își rezervă dreptul de a revoca autorizarea accesului la Internet și poșta electronică în cazul nerespectării normelor mai sus menționate și, de asemenea, afirmă că, în baza legislației specifice, accesul nepermis la sistemul informativ al companiei cât și menținerea conexiunii nepermise la sistemul menționat, chiar dacă accesul a fost obținut inițial, poate constitui infracțiune penală (art. 615 Cod penal, lit.b) și mai mult, constituie o încălcare relevantă a obligațiilor contractuale din punct de vedere disciplinar.

De asemenea, de reținut faptul că în Codul penal (art. 615 lit.d) este prevăzut în mod expres că se pedepsesc cu închisoare persoanele care „cu scopul de realiza profit, pentru ei înșiși sau pentru alții, sau pentru a provoca daune altora, sau dacă se procură și/sau se produc, ilegal, coduri de livrare, cuvinte cheie sau alte mijloace de acces la un sistem informatic sau telematic, protejate prin măsuri de securitate, sau furnizează indicații sau instrucțiuni în acest scop. "

# ACCEPTABLE USE POLICY

Securitatea sistemului informațional al companiei FOGLIANI este o condiție fundamentală pentru asigurarea fiabilității informațiilor prelucrate, precum și eficacitatea și eficiența serviciilor Grupului. Securitatea sistemului informatic are ca obiectiv principal protecția datelor și elementele prin care sunt gestionate datele.

Protecția datelor și elementelor asociate este garantată dacă este păstrată:

* **rezervarea:** asigură faptul că datele sunt accesibile doar celor autorizați să aibă acces.
* **integritatea:** garantează modul complet de transfer al datelor.
* **disponibilitatea:** asigură faptul că utilizatorii autorizați au acces la date și la elementele pe care le tratează, atunci când este nevoie

Lipsa unui nivel adecvat de securitate a datelor, în ceea ce privește Rezervarea, Disponibilitatea și Integritatea, poate avea drept consecință pierderea avantajului competitiv, a imaginii, a clienților, a veniturilor, rezultând o pierdere financiară semnificativă. La toate acestea trebuie să adăugăm, de asemenea, riscul de a suporta penalități legate de încălcarea legilor în vigoare.

Prin urmare, securitatea sistemului informatic se obține prin punerea în aplicare a unor serii de măsuri adecvate de securitate sau de proceduri, mecanisme tehnice sau practici care reduc riscurile la care este expus patrimoniul informativ, în ansamblu.

FOGLIANI direcționează propria sa activitate de a se conforma legislației în vigoare, în special la Codul privind protecția datelor cu caracter personal, nu numai pentru a evita riscul de implicare a unei companii, dar mai ales pentru a asigura un nivel adecvat de securitate a datelor cu caracter personal companiei și sistemului de informații acesteia.

## Politici generale di securitate a datelor

În prezentul paragraf sunt indicate principii fundamentale care se inspiră din normele de securitate a datelor Companiei FOGLIANI.

### Sistemul informatic al companiei

Sistemul de informatic al companiei este compus dintr-un set de unități de server central și PC client, conectat la o rețea locală (LAN), care folosește diferite sisteme de operare și aplicații.

FOGLIANI furnizează propriilor angajați și colaboratori interni toate instrumentele necesare desfășurării activităților atribuite. Instrumentele și aplicațiile software furnizate de companie sunt instrumente de lucru considerate a fi datele companiei, deci proprietatea companiei. Prin urmare compania poate dispune de toate acestea în mod complet, iar utilizatorii nu pot avea așteptări privind confidențialitatea cu privire la informațiile trimise, primite sau stocate.

De reținut că utilizarea necorespunzătoare a sistemelor companiei include procesarea, trimiterea, recuperarea, accesarea, afișarea, stocarea, tipărirea, și în general difuzarea materialelor și informaților frauduloase, hărțuitoare, amenințătoare, ilegale, rasiste, de orientare sexuală, obscene, intimidante, defăimătoare sau orice alt mod contradictoriu unei conduite profesionale.

Prin urmare, nici un fel de date de acest fel nu vor putea fi prezente în rețeaua companiei FOGLIANI, pe PC, în aplicații (cum ar fi e-mail, portaluri intranet, etc.) și în folderele de rețea, personale sau partajate.

Mai mult decât atât, utilizatorii de sisteme ale companiei nu trebuie să utilizeze infrastructura pentru a face afaceri, pentru a vinde produse, sau pentru alte activități comerciale, altele decât cele prevăzute în mod expres de conducerea companiei.

### Accesul la informații

Accesul la informații, de către fiecare utilizator individual, trebuie să se limiteze numai la informațiile de care au nevoie pentru a-și îndeplini sarcinile (principiul *need to know*). Divulgarea și transmiterea informațiilor atât în interior, cât și spre exterior, trebuie să se bazeze pe același principiu.

### Personalul și siguranța

În programul companiei se desfășoară activități de formare și informare a personalului, acordând o atenție deosebită securității informațiilor și utilizarea corespunzătoare a echipamentelor companie.

Trebuie solicitat personalului companiei să asigure un nivel minim de securitate echipamentelor alocate. Furtul, deteriorarea sau pierderea instrumentelor de lucru trebuie să fie raportate cu promptitudine.

Personalul (inclusiv consultanții și colaboratorii externi) trebuie să semneze clauze de confidențialitate care trebuie reînnoite la momentul încetării raportului de muncă.

Nerespectarea informațiilor indicate în acest document, precum și a oricăror alte informații care decurg din acesta constituie „neglijarea materialelor companiei“ și sunt supuse sancțiunilor disciplinare în conformitate indicațiile prevăzute de articolul 7 din Legea 300/70 și de Contractul Colectiv Național de munca.

### Incidente și deficiențe

Toți angajații sunt obligați să detecteze și să informeze personalul IT referitor la orice probleme legate de securitatea companiei

### Securitatea fizică

Accesul în clădirile și în locațiile importante pentru protecția bunurilor și a datelor trebuie să aibă loc numai după identificarea părților autorizate. Identificarea și proiectarea contramăsurilor de securitate fizică trebuie să țină cont atât de posibilitatea materializării amenințărilor fizice, cât și de legislația în vigoare. Întreținerea echipamentelor trebuie să fie efectuată în conformitate cu instrucțiunile producătorului sau prin proceduri documentate, pentru a asigura disponibilitatea serviciului și a integrității.

### Securitatea informatică

Proiectarea și implementarea planului de securitate informatică trebuie să țină cont atât de posibilitatea de concretizare a tentativelor de acces neautorizat intern și extern, cât și de legislația în vigoare și de alte constrângeri legate de procesele companiei, certificărilor în domeniu, reglementări.

Utilizatorii nu trebuie să profite de eventualele puncte slabe sau deficiențe ale sistemului de securitate informatică pentru a compromite sistemele sau datele, în a obține resurse pentru care nu sunt autorizate, redirecționarea resursele altor utilizatori sau să aibă acces la sisteme pentru care nu sunt necesare autorizații.

### Verificări

Sistemele informative trebuie să fie controlate periodic, astfel cum este prevăzut în normele de aplicare a procedurilor operative.

Principiile exprimate în politicile generale de securitate găsesc aplicații specifice în cadrul normelor generale de siguranță și în cele specifice la prelucrarea datelor prezentate în capitolele următoare.

Personalul desemnat care lucrează în funcția de IT a fost autorizat să efectueze operațiuni în sistemul informatic al companiei menite să asigure siguranța și securitatea sistemului în sine, precum și întreținerea tehnică

 și/sau suplimentară (de ex. Upgrade/înlocuire/implementare a programelor, întreținere hardware, etc.).

Aceste intervenții, luând în considerare normele detaliate ulterior cu privire la utilizarea de e-mail și Internet, vor implica, de asemenea, accesul în orice moment, la datele prelucrate de către fiecare, inclusiv arhivele de poștă electronica, site-urile de Internet accesate de utilizatorii autorizați pentru de navigarea externă.

Aceeași intervenție, tot în scopul asigurării securității sistemului dar și a funcționării normale a companiei, se aplică și în cazul absenței prelungite sau al unui impediment al utilizatorului.

Personalul IT desemnat , care are puterea de a se conecta și de la distanță și de a vizualiza prin telecomandă desktop-uri de PC-uri individuale cu scopul de a asigura asistența tehnică și cursul normal al operațiunilor de securitate maximă împotriva virușilor, *spyware, malware-ului*, etc.

Intervenția se face exclusiv în urma apelului utilizatorului sau, în caz de necesitate obiectivă, ca urmare a unor probleme tehnice detectate în sistemul informatic și telematic. În acest din urmă caz, acesta va fi notificat cu privire la necesitatea acestui lucru, cu condiția de a nu se afecta în mod negativ promptitudinea și eficiența intervenției.

# REGULI SPECIFICE

## Accesul fizic și logic

### Accesul în sedii

Accesul în sedii este permis cu condiția identificării colaboratorilor interni și a vizitatorilor. Este necesar ca reprezentantul intern al vizitatorului să îl însoțească tot timpul pe durata prezenței acestui a în sediul FOGLIANI.

### Accesul la datele tehnice locale și în sălile CED

Accesul în aceste locații se limitează doar persoanelor autorizate. În cazul personalului serviciului de întreținere tehnică în sălile CED, personalul extern trebuie să fie însoțit de un reprezentant intern FOGLIANI.

### Managementul acreditărilor accesului fizic la birouri, spații și arhive

 Aceste autorizații de acces sunt atribuite de către Conducere și/sau a persoanelor cu funcții delegate în mod specific, cu dreptul de acces al personalului. Predare este înregistrată în scris, astfel încât să știe întotdeauna calificarea fiecărui angajat în parte sau a colaboratorilor interni, pentru a gestiona posibila restituire a acestora (de exemplu, în cazul cheilor fizice) odată ce autorizația persoanei în cauză se încheie.

Se verifică periodic existența condițiilor referitoare la drepturile de acces.

### Gestionarea autorizațiilor de acces la sistemele informatice

Aceste autorizații de acces sunt atribuite de responsabilii IT la cererea diviziile individuale ale companiei și al Biroului Personal. Fiecare utilizator de acces la sistemele informatice cu drepturi definite în ceea ce privește sarcina atribuită (de ex. Utilizarea resurselor specifice, cum ar fi aplicațiile și folderele de rețea). Aceste drepturi sunt revizuite în timpul schimbării locului de muncă sau încetarea raporturilor de muncă.

Cu scopul menținerii la zi a profilurilor autorizate, utilizatorii Biroului Personal au sarcina de a comunica fiecare schimbare organizatorică a funcțiilor IT.

În cazul în care un utilizator nu mai trebuie să aibă acces, operatorii IT încep procedura de încetare care include dezactivarea accesului, cu scopul de a evita atribuirea unui nou acces pentru alte persoane. În cazul neutilizării autorizațiilor de acces pe o perioadă mai mare de 6 luni, acestea vor fi dezactivate automat, atunci când sistemul informatic permite acest lucru, sau vor fi dezactivate manual de către personalul IT.

În cazul în care inactivitatea pe termen lung a persoanei în cauză este cunoscută în prealabil (de exemplu, concediu medical pe termen lung sau de maternitate), Biroului Personal are obligația de a comunica acest fapt la IT.

### Reparațiile de întreținere și prevenția sistemelor

Sistemele trebuie să fie actualizate pentru a preveni eventuale vulnerabilități.

În acest scop, funcțiile IT monitorizează starea vulnerabilităților cunoscute și a actualizărilor de instalare, care se vor face, acolo unde este posibil în mod automat sau manual notificând utilizatorii asupra activităților pe care urmează să le facă în vederea menținerii eficienței sistemelor întotdeauna actualizate.

### Furnizori

Atunci când FOGLIANI face se folosește de companii externe pentru managementul securității informațiilor și de întreținere a sistemului, aceste persoane vor fi autorizate în mod oficial desemnate și își vor asuma rolul, sau dacă este cazul, administratorul de sistem sau responsabilul pentru tratamentul extern.

### Utilizarea sistemelor de către terți

Agenții/consultanții/furnizorii externi, care pe durata relației de colaborare trebuie să aibă acces la sistemele companiei, sunt autorizați, în mod oficial de către Responsabilul din zona de competență. Operatorii IT se ocupă de pregătirea accesului acestora în sistem, în baza profilului pe care consultantul îl va avea în conformitate cu indicațiile Biroului Personal și/sau a responsabilului intern, menționat mai sus.

Înafara documentației contractuale, toate persoanele externe autorizate să aibă acces la rețeaua companiei, trebuie să primească și să semneze prezentul regulament de informare.

De asemenea, în cazul în care o persoană externă utilizează PC-ul pentru a se conecta la rețeaua *Guest* a companiei, trebuie să se asigure că a instalat cea mai recentă versiune a software-ului antivirus și un sistem de protecție de comunicații (de ex. VPN), în cazul în care trebuie să se conecteze la rețeaua lor corporative sau în alt mod aplicație externă.

PC-urile care nu sunt proprietatea FOGLIANI nu se pot conecta la sursele de rețea ale companiei, atât prin cablu cât și prin WiFi.

Persoanele care nu sunt angajatele companiei, cele angajate temporar, consultanții sau agenții nu trebuie să știe sau să aibă *user-id –* ul utilizatorilor interni, și, la fel, nu trebuie să facă uz de privilegiile acordate de sistemul companiei, cu excepția unor situații specifice, în mod special autorizate, legate de întreținerea aplicațiilor de management sau a altor sisteme informatice.

## Securitatea instrumentelor

### Protecția stațiilor de lucru

* Utilizatorii ar trebui să evite să lase nesupravegheate stațiile de lucru, cu sesiunea deschisă și activă (*login* efectuat) sau ecrane care conțin date confidențiale.
* Fiecare utilizator trebuie să introduce blocarea sistemului (cu *CTRL-ALT-DEL+ Block*), în momentul în care se îndepărtează de stația de lucru; reactivare este controlată prin parola (la fel ca și accesul la sistemul companiei).
* De asemenea, fiecare utilizator va trebui să se asigure că stația este protejată prin sistemul de blocaj al ecranului, care intră în funcțiune automat după o perioadă definită de inactivitate (10-15 minute); nu este permisă schimbarea sau dezactivarea acestei configurații. Acest tip de măsuri previne ca stația de lucru ( și deci, aplicația deschisă) să poate fi folosită de alții în absența sa.
* La încheierea programului de lucru, toate aplicațiile trebuie închise, conform regulilor prevăzute de aplicația respectivă. Închiderea necorespunzătoare poate provoca pierderea datelor sau accesul la acestea de către persoane neautorizate.
* Închiderea PC la sfârșitul zilei (cu excepția cazului în care se prevede altfel de IT pentru activități de întreținere) sau în cazul unei absențe mai îndelungate, pentru că a lăsa un computer nesupravegheat și conectat la rețea poate fi utilizat de către terți, chiar în mod ilicit.

###  Utilizarea corectă a echipamentului electronic

* Este interzisă instalarea programelor provenite din exterior, care nu sunt autorizate în mod expres de către IT.
* Nu este permisă utilizarea programelor pentru care compania nu a cumpărat și nu deține licență corespunzătoare.
* Nu este permisă utilizarea echipamentelor electronice ale companiei pentru copierea, multiplicarea și/sau divulgarea materialelor protejate de drepturi de autor sau brevete.
* Nu este permisă modificarea configurației setate a PC-ului.
* Nu este permisă instalarea și utilizarea programelor de software și/sau hardware, făcute pentru a intercepta, falsifica, altera sau o suprima conținutul di comunicațiilor și/sau documentelor informatice.
* Nu este permisă instalarea pe propriul computer a mijloacelor de comunicare diferite de cele puse la dispoziție de companie.
* Evitarea lăsării nesupravegheate a suporturilor detașabile (CD-uri, DVD-uri, casete, chei USB) care conțin date ale companiei, pe birouri sau în alte locuri în care acestea ar putea fi îndepărtate cu ușurință de către terțe persoane neautorizate. Toate suporturile care poate fi ușor de copiat, de desigilat sau de ascuns, atunci când nu sunt utilizate, ar trebui să fie depozitate în dulapuri, rafturi sau sertare închise cu cheie.

### O mai mare atenție pentru laptop-uri și alte tipuri de “unelte mobile”

* Un laptop, o tabletă și un telefon mobil pot fi autorizate de către companie pentru a fi utilizate de către personalul desemnat care în timpul deplasărilor are nevoie să dispună de fișiere electronice, suport de automatizare și/sau pentru a accesa rețeaua organizației.
* Din cauza vulnerabilității informațiilor conținute pe dispozitivele mobile, ar trebui să se acorde o atenție deosebită acestor tipuri de sisteme, și limitarea maximă a utilizării acestora.
* Nu lăsați niciodată dispozitivul nesupravegheat; dacă vă aflați în sediul altor companii, puteți utiliza sistemele de protecție cum sunt cablurile de siguranță pentru PC portabile.
* În timpul călătoriilor păstrați întotdeauna instrumente cu dumneavoastră. Niciodată nu lăsați laptop-ul în mașină, chiar dacă se află în portbagaj, sau la vedere într-o cameră de hotel, în holuri de hotelului sau în săli de așteptare din gări și aeroporturi.
* Dacă nu este posibilă o conexiune sigură la sistemul companiei, executați *backup* zilnic tuturor datelor confidențiale pe dispozitive portabile utilizând dispozitive externe, cum ar fi *stick-uri USB* pe care personalul IT vi-l poate pune la dispoziție (la cerere)
* În caz de furt sau pierdere, faceți plângere la autoritățile competente și notificați imediat compania (funcționarii Biroului Personal și IT), care va efectua, după caz, ceea ce este necesar pentru a preveni utilizarea ilegală a configurărilor de pe dispozitiv.

### Utilizarea telefonului mobil/smartphone-ului personal

În timpul programului de lucru, inclusiv în pauze, persoanelor desemnate li se permite folosirea telefonului mobil personal numai pentru comunicațiile de urgență sau legate de mediul de lucru.

În cazul deplasărilor de serviciu, telefonul personal să fie pornit, pentru a facilita comunicarea cu compania, când este necesar.

Și în acest caz, vă rugăm a nu se folosi telefonul mobil în scopuri personale, în special în prezența clienților sau furnizorilor.

Persoanele desemnate, care nu sunt angajați ai companiei (consultanți, agenți, colaboratori externi), pot utiliza telefoanele lor mobile/smartphone-uri pentru a stoca datele companiei numai în cazul în care sunt în mod expres autorizate și asumându-și întreaga responsabilitate pentru tratamentul acestora.

Aceste telefoane mobile/smartphone-uri trebuie să fie în prealabil verificate și să prezinte măsuri de securitate adecvate.

### Atenția la sistemele di comunicare!

Comunicațiile în rețea cel mai des folosite, prin mijloace diferite de poșta electronică sunt: *software instant* de mesagerie, rețele sociale și alte sisteme.

 Vă rugăm să rețineți că de cele mai multe ori aceste instrumente nu sunt în măsură să protejeze comunicațiile care se transmit.

De exemplu, este foarte ușor să se folosească contul unui alt utilizator, cu nume complet; de multe ori lipsa utilizării protocolului HTTPS facilitează atacurile malware iar lipsa unor tehnologii avansate pentru comunicații criptate permite identificarea frazelor cu o precizie extraordinară.

Se recomandă deci transmiterea documentelor companiei să se facă prin intermediul unor astfel de sisteme, cu excepția cazului în care aplicația este verificată și autorizată de către companie.

### Antivirus

Prezența unui software anti-virus este o măsură de securitate esențială și un instrument de protecție foarte util. Eficacitatea sa depinde în mod esențial de actualizarea acestuia, în ceea ce privește computerele utilizatorilor, aceasta se face automat in timp activității.

Proprietarii de computerelor portabile ar trebui să se asigure că antivirus-ul este tot timpul actualizat, în acest scop este pur și simplu necesar să fie conectați frecvent la rețeaua companiei sau la site-ul producătorului, beneficiind astfel de serviciul de actualizare automată. Instrucțiuni detaliate sunt disponibile la IT.

Dată fiind complexitatea considerabilă atinsă de viruși, utilizatorii nu ar trebui să încerce să le șteargă fără ajutorul unui expert. Sistemul anti-virus este configurat pentru a șterge în mod automat orice virus găsit.

Dacă suspectați o situație mai complexă, sau în cazul în care virusul este în carantină, deoarece este imposibil să se elimine, trebuie să deconectați imediat calculatorul de la rețea, opriți-l și contactați profesioniștii IT.

Acest mod de acțiune va contribui la limitarea daunelor cauzate fișierelor și software-ului și, în același timp, asigură faptul că informațiile necesare pentru a identifica o nouă infecție sunt înregistrate.

### Restituirea echipamentelor

Ca urmare a încetării contractului de muncă sau de consultanță a utilizatorilor cu compania, sau orice alt mod de absență a raporturilor cu aceasta, la decizia incontestabilă a companiei privind valabilitatea condițiilor de utilizare a echipamentelor acordate, persoanele desemnate au următoarele obligații:

1. Să restituie imediat echipamentele folosite
2. Este absolut interzisă formatarea, modificarea sau distrugerea dispozitivului atribuit sau schimbarea inteligibilă a datelor în acestea, prin orice proces manual sau automat.

## Memorarea și disponibilitatea datelor

* Datele necesare pentru desfășurarea activității proprii (documente, imagini legate de afaceri, e-mail) trebuie să fie salvate pe resursele rețelei puse la dispoziție de către companie, pentru a permite astfel *backup*-ul centralizat automat. Persoanele desemnate care lucrează în afara companiei și care nu au posibilitatea de a utiliza resursele de rețea, trebuie să se adreseze IT pentru a li se atribui o memorie externă atunci când au nevoie să facă backup datelor aflate pe PC-ul local (mai mult detalii mai jos).
* Si recomanda să:
	+ se salveze datele în folderul de rețea, cel mai potrivit, în funcție de tipul de document și modul utilizat de grupul de lucru din care face parte utilizatorul
	+ să nu se păstreze în rețea mai multe versiuni ale aceluiași document, și mai ales, odată salvat, să se șteargă versiunile anterioare, astfel încât să nu ocupe în mod inutil resursele discului.
	+ Să se evite mutarea sau eliminarea dosarelor necunoscute, și în orice caz să notifice prompt IT în cazul în care operațiunile de încheiere sunt incorecte sau nereușite.
* Utilizatorii nu trebuie să fie stocheze în rețea, în folderele comune și pe PC-urile companiei documente personale sau care nu sunt legate de activitatea profesională, atât pentru a proteja viața privată a fiecăruia cât și pentru a ocupa inutile resursele de pe disc.

**Prin urmare, orice fișier care nu este legat de activitatea profesională (de ex. fotografii personale, muzică, videoclipuri) nu pot fi salvate pe resursele companiei (unități de rețea, *storage* partajat, PC-ul utilizatorului), NICI chiar și pentru perioade scurte de timp. Compania își rezervă dreptul de a proceda imediat la eliminarea fiecărui fișier sau aplicație pe care le consideră a fi periculoase pentru siguranța sistemelor sale sau, în cazul în care se constată că astfel de cereri au fost dobândite sau instalate prin încălcarea prezentului Regulament.**

* Nu este permisă stocarea sau difuzarea de informații de natură scandaloasă și/sau documente discriminatorii legate de sex, religie, rasă, origine etnică, apartenența la un sindicat, și/sau politic.
* Non este permisă arhivarea documentelor companiei în serviciile *Cloud* neautorizate de IT (ex. *Apple iCloud, Dropbox, Google Drive personale, One Drive personale,* etc.)
* Persoanele desemnate care funcționează în afara companiei și care nu au posibilitatea de a utiliza resursele din rețea, trebuie să solicite operatorului IT atribuirea unei memorii externe (cheie USB, hard disk extern, card de memorie) pe care să copieze temporar date care urmează să fie utilizate pentru *backup* de date la nivel local pe laptop-ul sau *desktop-ul* PC-ului. Operatorul IT va evalua nevoile utilizatorului și va atribui tipul de echipament pe care îl consideră cel mai potrivit. Utilizatorul trebuie să urmeze instrucțiunile furnizate de operatorul IT în utilizarea memoriei, în special pentru operațiunile de *backup.* Aceste dispozitive trebuie să fie, de asemenea, păstrate cu mare atenție, atât în ​​timpul deplasării, cât și în ​​timpul utilizării la locul de muncă; ar trebui să fie folosite numai de către persoanele cărora le-au fost atribuite și, acestea nu trebuie să fie date spre folosință altor terți. Eventualele pierderi de date legate de lipsa efectuării *backup* cade în responsabilitatea utilizatorului căruia îi este atribuit dispozitivului.

## Gestionarea datelor pe suport de hârtie

### Gestionarea corecta a documentelor pe suport de hârtie

Persoanele desemnate cu tratamentul documentelor, care conțin date cu caracter personal, trebuie să păstreze aceste documente luând toate măsurile de precauție necesare pentru a le stoca în baza de date (inclusiv orice copie) la sfârșitul operațiunilor.

Si recomanda:

* Verificarea și funcționarea închizătorilor cu chei, ale dulapurilor și cutiilor de arhivare care conțin date de natură specială (chiar și numai pentru păstrarea temporară a acestor documente)
* Înmânarea cheilor de la dulapuri/cutii de arhivare numai personalul autorizat, care va proteja aceste spații cu atenție
* Nu se vor lăsa documente în interiorul imprimantelor, fotocopiatoarelor sau fax-urilor.
* Nu se vor lăsa documente la vedere pe birouri (*clean desk policy*) la îndepărtarea sau ieșirea din încăpere sau în timpul unor întâlniri.
* În cazul în care în care beneficiați de un birou personale închideți cu cheia încăperea când ieșiți din birou pentru pauze, ședințe, alte obligații în exteriorul companiei; iar ca alternativă încuiați arhiva, sertarele, etc.

### Documentele confidențiale

**Documentele din hârtie care conțin informații personale sensibile, juridice sau considerate importante ar trebui să fie protejate iar libera circulație a acestora ar trebui să fie limitată.**

Utilizatorii autorizați cu gestionarea acestor documente pe suport de hârtie, care conțin date personale mai speciale (ex date sensibile), juridice sau considerate ca foarte importante ar trebui să se asigure că aceste documente nu pot fi vizualizate de către persoane neautorizate, chiar și în timp ce se află la locul de muncă, căutând să nu le lase nesupravegheate sau în imprimante, copiatoare și faxuri și să le depoziteze în dulapuri încuiate. Circulația acestor documente se limitează numai peroanelor autorizate.

### Sfaturi practice

Câteva exemple și sfaturi practice pentru utilizatorii din toate sediile. Se recomandă prestarea unei atenții speciale celor care lucrează în filiale, în cazul în care camerele sunt mai mici și sunt folosite în comun, pentru nevoi diferite.

* Utilizați sala de ședințe, în cazul în care aceasta există, pentru a primi clienții și furnizorii
* Dacă persoanele externe trebuie să fie primite pentru a folosi PC-ul, pe biroul dumneavoastră asigurați-vă că nu lăsați documente confidențiale (oferte, liste de prețuri, contracte, caiete de sarcini, etc.) la vedere
* În general, sfârșitul zilei de muncă, puneți documentele comerciale în dulapuri, sertare, arhive
* Atenție la datele cu caracter personal care sunt notate pe ambalaje (numere de telefon, etc.). introduceți doar informațiile necesare pentru livrarea acestora.
* Pe mesele de livrare nu trebuie să fie lăsate liste cu date de contact, e-mail, etc.
* Gestionați acordând confidențialitatea necesară propunerilor, caietelor de sarcini, documentelor lăsate de instalatori pentru pregătirea unui proiect și devizelor.

# PASSWORD POLICY – USER ACCESSES

## Autentificarea

### Compoziția autorizațiilor de acces.

Fiecare utilizator, pentru a avea acces la sistemele de informații corporative trebuie să fie mai întâi identificat și autentificat, prin verificarea autorizațiilor de acces. Datele de autorizare constau în:

* identificativul unic al utilizatorului (user-id)
* parola secretă (password).

Autorizațiile sunt confidențiale și strict personale și sunt atribuite fiecărui angajat care trebuie să utilizeze un terminal, conectat la rețeaua companiei, ca un instrument de muncă. Cuvintele cheie (*password*) sunt „măsuri de securitate“, întocmite în conformitate cu cerințele legale specifice. Din acest motiv, comunicarea acestora este interzisă oricui; nu există excepții de la această regulă, chiar și față de șefii direcți. Interdicția se referă la orice formă posibilă de comunicare autorizațiilor de autentificare, atât oral cât și în scris (telefon, e-mail, etc.).

Vă rugăm să rețineți că utilizarea sistemului informatic al companiei, și prin urmare, accesul la date, la programe și la toate resurse informatice ale companiei este permisă doar în scopul îndeplinirea sarcinilor și/ sau obligațiilor atribuite și doar pe timpul necesar pentru a îndeplinirea aceste sarcini și obligații.

### Reguli de compunere a parolelor

În perioada de valabilitate a parolei proprii, în unele cazuri, raportate automat, fiecare utilizator va trebui, în funcție de modul de utilizare, să actualizeze parola, în conformitate cu următoarele reguli:

* să adopte o combinație de cifre și litere (alfanumerice), cu o lungime de cel puțin 8 caractere; Se recomandă, de asemenea, utilizarea combinată de caractere mari, mici și speciale
* nu ar trebui să se bazeze pe informații personale (nume de familie, numărul de licență auto, data nașterii, o parte din numele său/prenumele, locul de origine geografică, etc.)
* să nu utilizeze un acronim, un mod comun de a spune, un cuvânt în dialect sau în argou
* nu ar trebui să fie o secvență de caractere comune, cum ar fi 123456, aaabbb, qwerty, etc .
* nu ar trebui să se bazeze pe o terminologie a unei companii, ușor de identificat, cum ar fi numele companiei și produsele sale sau codul/numele produsului.

În general, parola trebuie să fie suficient de puternică în ceea ce privește combinația de caractere, dar trebuie să fie ușor de memorat/amintit de către utilizator.

O posibilă tehnică este utilizarea secvențelor de caractere, fără un fel de evident, dar cu caractere individuale care fac o frază ușor de depozitat, ca titlul unui film, o carte sau o melodie. Ex: I7N0m3de88aR% s = Numele trandafirului.

### Confidențialitatea parolei

Toți utilizatorii trebuie să asigure de confidențialitatea strictă a parolei; toate parolele trebuie să fie tratate ca informații sensibile și confidențiale de către companie și, prin urmare, trebuie să respecte următoarele indicații:

* nu se spune nici unei alte persoane;
* nu se dezvăluie parolele prin mesajele sau e-mail sau în alte forme electronice de comunicare
* nu divulga parola prin telefon niciunei persoane
* se evită evidența scrisă a acesteia
* se introduce întotdeauna având grijă să nu fie văzut de oricine
* se iau măsuri imediate pentru a o actualiza în cazul unei încălcări a confidențialității, chiar și doar în cazul unei suspiciuni

### Actualizarea parolei.

Este necesar să se facă actualizarea parolei în următoarele cazuri:

* În momentul primei conectări la sistemul informatic (de exemplu, rețea și server ale companiei, aplicații) pentru înlocuirea parolei „inițiale“ atribuite, care este de obicei temporară;
* atunci când se semnalează în mod automat de către sistem (sau cel puțin o dată la 90 de zile dacă este gestionată manual de către utilizator);
* de fiecare dată când există suspiciunea sau se constată că parola nu mai este confidențială.

Se reamintește că, în efectuarea operațiunii de actualizare a parolei, cea nouă va trebui să se facă în cadrul normelor definite anterior.

Actualizarea parolei trebuie să fie efectuată pe toate sistemele de operare sau aplicații care necesită utilizarea autorizărilor, indiferent de prezența unui sistem de expirare automată a acestuia.

### Dezactivarea autorizării utilizatorului

Autorizările de acces la domeniu sau la aplicații vor fi dezactivate în caz de neutilizare a acestora pentru o perioadă mai mare de șase luni. În cazul lipsa utilizării este legată de o mai lungă absență (de maternitate sau concediu de sănătate), Biroul Personal va trebui să informeze operatorul IT de acestea.

Utilizatorul trebuie să ceară ulterior, în conformitate cu procedurile aflate în vigoare, reactivarea autorizării acestuia, la serviciul IT.

### Dezactivarea autorizării unui utilizator

Accesul la autorizare în sistemului informatic este dezactivat în cazul în care utilizatorul nu mai are nevoie de acces la anumite informații sau servicii, în scopul de a asigura corespondența între sarcinile organizatorice efectuate și dreptul de acces la date.

### Accesul la date în caz de nevoie

În caz de nevoie (de exemplu, absență neașteptată și prelungită), este de așteptat ca parolele utilizatorului să fie resetate și înlocuite pentru a permite accesul la date unei alte persoane autorizate. Acest lucru se comunicată titularului autorizației de acces, care va trebui ulterior să furnizeze, în conformitate cu normele în vigoare, actualizarea acesteia.

### Gestionarea încetării raportului de muncă

Biroul Personale trebuie să comunice toate schimbările semnificative ale sarcinilor utilizatorului și/sau a statutului său de angajat, operatorului IT, pentru ca acesta să poată efectua toate operațiunile necesare utilizării.

Prin urmare la încetarea raportului de muncă se va proceda la următoarele activități:

* Se dezactivează *user-id* în Sistemul Informativ al companiei
* Căsuța de poșta electronica (dacă este nominală) se dezactivează și se elimină conținutul său în termen de maxim cincisprezece zile de la încetarea raportului de muncă; va fi necesar pentru a anunța și pentru returna eventualele mesaje și pentru a face comunicările necesare în afara companiei (dacă e cazul), cu referire la noi interlocutori.
* Dacă utilizatorul care a plecat a utilizat o căsuță de e-mail funcțională/generic, aceasta va fi făcută disponibilă noii persoane desemnate.
* conținutul echipamentului de lucru folosit, poate fi evaluat de către responsabilul utilizatorului, care trebuie să decidă rapid dacă acesta poate fi refolosit și deci reatribuit, sau trebuie mai înainte de orice curățat, comunicând aceasta birourilor competente.

Se recomandă utilizatorului care părăsește compania să nu șteargă datele propriei companii din calculatorul personal, în timp ce este necesar ca orice date cu caracter personal (care nu sunt de natură profesională) să nu fie prezente în echipamentele companiei, ce urmează să fie returnate.

### Control de siguranță

În sfera activităților legate de protecția securității infrastructurii tehnologice, compania ar putea face analiza periodică ale parolelor utilizatorilor, cu scopul de a verifica robustețea acestora, politica de gestiune, și durata, informând în prealabil despre acestea utilizatorii.

În cazul în care la audit, printre rezultatele posibile, se constată că parola este slabă, aceasta este blocată, iar persoana desemnată va fi obligat să o înlocuiască cu alta parolă mai puternică.

##  E-MAIL POLICY

### E-mailuri – Reguli Generale

* E-mailul este un mijloc de comunicare deținut de companie, atribuit persoanei responsabile pentru a-și îndeplini sarcinile.
* În general, un mesaj de e-mail trimis de la o adresă de e-mail autorizată prenume.name@numecompanie sau funcție@numecompanie este perceput ca mesaj ce conține informații, știri, opinii cu caracter oficial provenit de la companie. În consecință, utilizarea e-mailului trebuie să fie luată în considerare la fel ca utilizarea antetului companiei.
* Fiecare persoană este responsabilă pentru conținutul comunicărilor sale, inclusiv în ceea ce privește confidențialitatea datelor prelucrate în acestea: divulgarea neadecvată ar putea fi considerată o încălcare a secretului companiei sau o încălcare a reglementărilor actuale.
* Utilizarea personală a căsuței de e-mail a companiei nu este permisă. Orice informații cu caracter personal nu trebuie să treacă prin serverele de e-mail ale companiei, care pot fi supuse verificărilor în timpul activităților de întreținere sau în caz de anomalii, defecțiuni sau intervenții legate de siguranță; ca atare, utilizatorii nu vor putea avea așteptări de confidențialitate cu privire la informațiile trimise, primite sau stocate. În caz de primire a mesajelor personale în căsuța de e-mail a companiei, utilizatorul trebuie să șteargă imediat fiecare mesaj.
* Vă amintim faptul că compania oferă adrese de e-mail „funcționale” partajate de mai mulți lucrători, alături de cele individuale. Vă recomandăm utilizarea acestora pentru a gestiona toate acele comunicări care trebuie partajate în cadrul grupului de lucru.

### E-mailuri – Securitate

* + Nu este autorizată configurația e-mailului personal pe calculatorul companiei (de ex. pe clientul dvs. *Outlook, Mozilla*, etc.). În schimb, puteți consulta căsuța personală de e-mail prin intermediul aplicațiilor *Webmail* (de ex. *Gmail, Yahoo, Libero, Fastweb*, etc.), respectând metodele de utilizare a rețelei definite în această procedură. De asemenea, este permisă accesarea contului dvs. de e-mail prin intermediul smartphone-ului companiei (sau dispozitivelor similare), numai în limite minime, care să nu afecteze activitatea profesională, eficiența și productivitatea personală. Se reamintește că e-mailul personal NU trebuie NICIODATĂ utilizat pentru procesarea datelor companiei.
	+ Compania poate adopta numeroase sisteme de protecție a e-mailului împotriva virușilor și activităților de *spamming*. Cu această ocazie vă amintim unele reglementări fundamentale pentru utilizarea corectă a e-mailului:
	1. Utilizatorii nu trebuie să deschidă atașamentele din e-mailurile al căror expeditor nu este cunoscut cu certitudine sau despre care apar chiar și cele mai mici îndoieli.
	2. Nu transmiteți nimănui mesajele care conțin știri false despre alarme sau apeluri pentru care se solicită divulgarea.
	3. Nu creați, stocați și nu trimiteți mesaje publicitare sau promoționale care nu au legătură cu derularea activităților profesionale în cadrul și în afara domeniului companiei
	4. Nu efectuați comunicări masive prin intermediul clientului dvs. de e-mail, ci utilizați numai instrumentele speciale dedicate marketingului prin e-mail (contactați funcția IT în caz de nevoie)
	5. Nu răspundeți la mesajele care provin în aparență de la expeditori considerați „siguri” (de ex. bancă, poștă, furnizori de marfă, etc.) și, mai ales, nu furnizați date personale solicitate în cadrul acestor e-mailuri **și nu vă conectați la eventuale link-uri propuse în mesaj**.
* În toate situațiile descrise mai sus, dacă există vreo îndoială cu privire la modul de gestionare a mesajului, vă amintim să nu deschideți mesajul și eventualul atașament și să contactați funcțiile IT.
* Este necesar să arhivați în mod sigur mesajele din e-mailurile care pot angaja compania cu terți sau care au orice valoare legală. Vă amintim că este posibil să păstrați aceste mesaje pe serverul de e-mail, dar această practică nu garantează caracteristicile autenticității, integrității, fiabilității. În aceste cazuri, vă recomandăm să contactați funcțiile IT pentru a evalua eventuala necesitate a unor sisteme mai adecvate pentru stocarea în condiții de siguranță, cum ar fi gestionarea documentelor.

### E-mailuri – Gestionarea absențelor

Pe baza celor explicate anterior, vă precizăm următoarele:

* 1. Conținutul mesajelor din e-mailuri la intrare/ieșire ar putea fi vizualizat de către Controlorul de date (prin personalul special însărcinat), în cazul absenței neprevăzute și prelungite a lucrătorului, dacă acest lucru ar fi necesar pentru continuitatea activității profesionale.
	2. În cazul absenței prelungite și prevăzute, ar fi o bună practică activarea serviciului de mesagerie automată. Compania a pus la dispoziția fiecărui lucrător niște funcții speciale (așa-numitele alerte „nu sunt la birou” sau „regula nu sunt la sediu”) prin care pot fi trimise automat informațiile (telefonice sau electronice) unui coleg sau ale unei structuri alternative la care să se apeleze. Prin urmare, toți utilizatorii sunt rugați să utilizeze aceste servicii, împiedicând astfel posibilitatea ca e-mailul acestora să fie consultat de alte persoane.
	3. În mod alternativ și în toate cazurile în care este necesară păstrarea căsuței de e-mail din motive specifice operaționale ale companiei, utilizatorul poate identifica un „mandatar” care, în absența sa, poate verifica e-mailurile și transmite conținutul necesar către persoanele care au urgențe.
	4. În cazul în care nu este identificat mandatarul, managerul ierarhic este autorizat să acceseze conținutul mesajelor sau să procedeze la configurarea mesageriei automate, prin personalul special însărcinat. Utilizatorul va fi informat cu privire la accesul la căsuța de e-mail, cu prima ocazie.
	5. În cazul în care e-mailul dvs. a fost consultat de terți în timpul absenței dvs. (așa cum am explicat mai sus), parola de acces trebuie schimbată de utilizator la întoarcerea la companie.

# INTERNET POLICY

### Internet – Reguli Generale

Conectivitatea sistemelor la rețelele publice este asigurată pentru desfășurarea activității profesionale în cele mai bune condiții.

Utilizarea personală sporadică este acceptată numai în orele în care nu se lucrează (de ex. în pauza de masă), în limite minime de timp, comparabile cu alte practici de comunicare de la locul de muncă și în conformitate cu aceste orientări, a tuturor celorlalte proceduri și politici ale companiei și ale legislației actuale.

### Internet – Reguli de navigare în siguranță

După cum prevede legislația privind protecția datelor cu caracter personal, compania trebuie să promoveze orice măsură organizatorică și tehnologică adecvată, menită să prevină riscul unei utilizări necorespunzătoare a sistemelor companiei. În general, prevenirea abuzurilor trebuie considerată mai importantă decât identificarea lor și, prin urmare, trebuie preferate măsurile de PREVENIRE față de următoarele acțiuni REPRESIVE.

Având în vedere aceste principii, compania a adoptat unele măsuri de securitate organizațională și tehnologică și, în special:

1. Sunt identificate tipurile de utilizatori cărora li se acordă, pentru nevoile legate de profesia lor, utilizarea e-mailului și/sau a internetului.
2. Unele dispozitive informatice instalate de mai mult timp, permit reducerea riscului de încălcare a condițiilor de accesare a rețelei proprii din exterior
3. Dispozitive instalate care limitează și contracarează orice utilizare necorespunzătoare sau periculoasă a „navigării” pe internet. În special, site-urile periculoase sunt întotdeauna blocate, cu referire la liste negre care sunt actualizate constant și includ categorii precum pornografie, pedofilie, violență, piraterie software, încălcarea drepturilor de autor, *hacking* și *cracking, peer-to-peer*, etc. În plus, în timpul programului de lucru, poate fi restricționat accesul la anumite categorii de site-uri care nu sunt relevante pentru activitatea profesională și care poate influența semnificativ eficiența benzii *(web mail, social network, shopping, instant messaging).*

Sistemele utilizate garantează un nivel bun de protecție a rețelei companiei în ceea ce privește comportamentul ilegal; în orice caz, amintim câteva reguli fundamentale:

1. Este interzisă conectarea la site-uri precum *WebChat*, site-uri care oferă software protejat de drepturi de autor și activități ilegale în general.
2. Este interzis să descărcați și/sau să instalați independent pe stația dvs. software de orice fel.
3. Este interzisă navigarea pe site-uri care pot dezvălui păreri politice, religioase, sindicale și de sănătate ale utilizatorului, deoarece ar putea fi în măsură să dezvăluie date cu caracter sensibil.
4. Nicio formă de înregistrare nu este permisă pentru site-urile al căror conținut nu este legat de activitățile profesionale; nu este permisă participarea, din motive non-profesionale, la forumuri, chat-uri sau grupuri de discuții.
5. Este interzisă efectuarea oricăror tranzacții financiare cu caracter personal, inclusiv operațiunile de servicii bancare la distanță, achiziții online și altele asemenea, cu excepția cazurilor autorizate direct de către Controlorul de date și în conformitate cu procedurile normale de achiziție.

Utilizatorii care beneficiază de serviciul de conectivitate și navigare pe internet al companiei sunt totuși informați despre faptul că FOGLIANI dispune de instrumentele necesare pentru securitatea sistemelor informatice, a datelor și a cunoștințelor, care înregistrează adresele site-urilor vizitate și adresa stației (IP-ul) și, prin urmare, ar putea fi utilizat pentru a constata eventuale comportamente contrare politicilor de utilizare a internetului și a instrumentelor companiei.

# VERIFICĂRI ȘI CONTROALE

FOGLIANI și celelalte societăți controlate, în calitate de titular a datelor și echipamentelor informatice utilizate în tratament, își rezervă dreptul de a efectua controale ce se consideră oportune cu următoarele scopuri:

1. Protejarea securității rețelei companiei și integritatea echipamentelor informatice și a datelor. 2. Evitarea comiterii ilegalităților, prin punerea în aplicare a măsurilor de prevenție sau de apărare 3. Verificarea funcționalității sistemului și a echipamentelor informatice

Activitățile de control pot apărea, de asemenea, și prin auditul tehnic sau proces, sau prin intermediul evaluării *Vulnerability Assesment* a sistemului informatic. Pentru aceste controale, organizația își rezervă dreptul de a folosi personal extern.

Se precizează totuși că, organizația nu adoptă „dispozitive în scopul controlului de la distanță a lucrătorilor“ (art. 4, primul paragraf, Legea 300/1970), în care se include si echipamentele hardware software orientate către controlul utilizatorului.

## Modalități de verificare

În cazul în care un eveniment dăunător sau o situație periculoasă pentru securitatea companiei nu a fost blocată de caracteristicile tehnice adoptate, compania poate lua toate măsurile necesare pentru a verifica dacă nu există un comportament anormal.

Controalele vor respecta însă principiile fundamentale de relevanță și nu de limitare, și se va face o regula în acest mod:

1. detectarea evenimentului dăunător 🡪 verificarea anonimă asupra datelor cumulate 🡪 avizarea generală (a companiei sau a grupului de lucru)
2. repetarea evenimentului dăunător 🡪 verificarea grupurilor de postare/nominal 🡪 avizarea/avertizarea grupului controlat
3. repetarea evenimentului dăunător 🡪 verificarea individuală 🡪 avizarea/avertizarea nominală

Informațiile înregistrate sau înregistrabile automat de către sisteme (logarea la navigarea pe Internet sau la serverul de poștă electronică) sunt accesibile numai operatorilor IT ale companiei FOGLIANI, autorizate în mod oficial.

Persoanele desemnate vor desfășura doar operații strict necesare în scop tehnic și de siguranță.

## Informații conform art. 13 din Regulamentul UE

Orice date cu caracter personal, sau care aparțin unei anumite categorii, găsite pe echipamentele electronice deținute de companie, chiar au fost deținute sau păstrate prin încălcarea prezentului regulament vor fi în continuare prelucrate în conformitate cu criteriile de confidențialitate stabilite prin lege, exclusiv în scopul activităților de control aferente și/sau pentru asigurarea unei eventuale protecții juridice a companiei

Sistemele software sunt configurate astfel încât să poată șterge periodic și în mod automat datele cu caracter personal referitoare la acces și la traficul pe Internet, a căror păstrare nu este necesară. O posibilă prelungire a timpilor de stocare este evaluată ca excepțională și ar trebui să aibă loc numai referitor la:

1. Cerințele tehnice sau de securitate cu totul speciale;
2. Indispensabilitatea faptelor pentru a se stabili sau apăra o revendicare în sfera juridică;
3. Obligație de a păstra sau de a difuza datele pentru îndeplinirea unei cereri specifice a instanței sau a poliției judiciare.

## Sancțiuni

Fiecare este responsabil personal, în cazul încălcării deliberate a acestor norme, în conformitate cu legislația în vigoare și a obligațiilor contractuale și de natură disciplinară

Eventuale sancțiuni:

1. Avertisment verbal
2. Avertisment în scris;
3. Amendă ;
4. Suspendarea retribuției financiare și din funcție;
5. Concedierea disciplinară cu alte urmări legale;

Pentru personalul de conducere se va aplica legislația în vigoare și/sau contractual colectiv, cu condiția ca, în cazul celor mai grave încălcări, Organizația va putea proceda la demiterea managerului care a comis infracțiunea.