



**GEWISS ROMANIA SRL
CODUL DE CONDUITĂ IT**

Julie 2014

SUMAR

INTRODUCERE	3
1. DEFINIȚII	3
2. SISTEMELE INFORMATICE ALE COMPANIEI – REGULI GENERALE	3
3. FOLOSIREA ECHIPAMENTELOR DE TEHNOLOGIE A INFORMAȚIEI	4
4. PAROLE	5
5. FOLOSIREA REȚELEI LAN A COMPANIEI.....	5
6. FOLOSIREA REȚELEI DE INTERNET ȘI A SERVICIILOR AFERENTE.....	5
7. FOLOSIREA POȘTEI ELECTRONICE.....	6
8. CONTROLURI	7
9. NE-RESPECTAREA INSTRUCȚIUNILOR ȘI SANȚIUNILOR.....	7

INTRODUCERE

Răspândirea progresivă de noi tehnologii ale informației pot face ca GEWISS să se confrunte atât cu riscuri la adresa proprietății cât și cu riscuri penale, creând între timp probleme pentru imaginea și securitatea corporației, în cazul în care echipamentele de tehnologie a informației sunt folosite într-un mod incorect sau pentru acțiuni criminale.

Importanța în creștere a informațiilor confidențiale din cadrul activelor companiei și folosirea corectă a avantajelor competitive pentru aceasta au convins-o să se doteze cu toate măsurile de protecție adecvate pentru prevenirea răspândirii de date și informații confidențiale, care pot cauza răspunderi civile și criminale pentru persoana care încalcă secretul corporativ.

De aceea, compania dorind să-și protejeze informațiile confidențiale, este recomandabil să fie dotată cu măsuri pozitive (de exemplu măsuri de securitate) pentru protejarea naturii confidențiale a informațiilor.

În plus, referitor la procesarea de date personale, GEWISS a oferit explicații și instrucțiuni adecvate pentru toți „utilizatorii corporatiști” care sunt interesați de măsurile specificate mai sus deoarece lucrează cu instrumente informative.

Deoarece folosirea de informații corporative și resurse telematice se va face întotdeauna conform principiilor de corectitudine și caracter echitabil, atitudini ce trebuie păstrate întotdeauna în cursul lucrului, este utilă adoptarea în continuare a unui regulament de comportament intern pentru mediul informatic, cu scopul de evita orice comportament în necunoștință de cauză și/sau incorect.

1. DEFINITII

În cadrul acestui Cod de conduită IT, sensul specificat pentru fiecare termen și expresie specificate mai jos este valabil pentru termenul/expresia respectivă, după cum urmează:

- „**COD DE CONDUITĂ IT**”: acest document;
- „**COMPANIE**”: compania GEWISS ROMANIA SRL;
- „**COMPANIA-MAMĂ**”: compania GEWISS S.P.A.;
- „**DIRECTOR DE SECURITATE**”: persoană însărcinată cu procesarea datelor personale din cadrul GEWISS S.P.A., cu transferul de date și comunicații, precum și cu măsurile de securitate aferente, conform legislației în vigoare.
- „**ECHIPAMENTE DE TEHNOLOGIE A INFORMAȚIEI**”: orice echipament non-hârtie folosit de fiecare utilizator corporativ pentru a-și îndeplini sarcinile, printre care se numără, ca exemplu, computerele personale, atât cele desktop cât și cele portabile, PDA sau telefoane inteligente, fixe și mobile;
- „**SISTEM INFORMATIC**”: resurse, date, aplicații și programe pentru echipamentele de IT și/sau dispozitivele de stocare a datelor;
- „**UTILIZATOR CORPORATIV**”: orice utilizator, chiar dacă nu este angajat al COMPANIEI, care a primit unul sau mai multe ECHIPAMENTE DE TEHNOLOGIE A INFORMAȚIEI și/sau a primit acces la sistemul informatic al companiei.

2. SISTEMELE INFORMATICE ALE COMPANIEI – REGULI GENERALE

Toate ECHIPAMENTELE INFORMATICE, programele respective și/sau toate aplicațiile, acordate UTILIZATORILOR companiei sunt considerate instrumente de lucru. De aceea:

- 2.1 Aceste instrumente trebuie păstrate în mod adecvat;
- 2.2 Aceste instrumente trebuie folosite numai în scop profesional (adiacente în mod evident îndatoririlor personale) și nu în scop personal, și în orice caz nu în scop criminal;
- 2.3 Este interzis împrumutul sau distribuirea către terțe părți a oricăror ECHIPAMENTE DE TEHNOLOGIE A INFORMAȚIEI;
- 2.4 Este interzisă scoaterea semnelor de identificare de pe ECHIPAMENTELE DE TEHNOLOGIE A INFORMAȚIEI;
- 2.5 Orice furt, avariere sau pierdere a computerelor va fi imediat raportată companiei și Departamentului de care ține persoana respectivă. În plus, în cazul în care echipamentele respective de computer sunt furate sau pierdute, persoana implicată sau persoana care a primit ECHIPAMENTE DE TEHNOLOGIE A INFORMAȚIEI de orice tip, îi va remite companiei exemplarul original al raportului înaintat Autorității publice de securitate în termen de 24 de ore;

- 2.6 Este interzisă introducerea și/sau păstrarea în cadrul companiei, în orice capacitate și din orice motiv, (prin intermediul instrumentelor informatice, hardware și pe hârtie), a oricăror materiale și/sau documente IT confidențiale și terțe, fără autorizația proprietarului anterior. Se înțelege că, în cazul încălcării acestei reguli, se va aplica răspunderea personală civilă și criminală a angajatului respectiv, precum și sancțiuni disciplinare impuse de companie;
- 2.7 Este interzisă scoaterea din companie și/sau transmiterea de fișiere, documente, schițe, proiecte sau orice alte documente confidențiale ale COMPANIEI, prin intermediul computerului, mijloacelor hardware și pe hârtie, cu excepția cazului în care acest lucru se face în scopuri care privesc în mod strict executarea sarcinilor personale și, în orice caz, sub rezerva autorizației Directorului de departament relevant;
- 2.8 Este absolut interzisă partajarea în zonele comune (ca de exemplu directoarele Workspace/LAN etc.) sau, în orice caz, transmiterea de documente și informații din cadrul companiei, care nu sunt relevante pentru activitățile profesionale ale expeditorului sau destinatarului, prin intermediul oricăror instrumente IT, hardware și pe hârtie;
- 2.9 Este interzisă înregistrarea în SISTEMUL INFORMATIC al companiei a unor documente jignitoare și/sau discriminante referitoare la sex, limbaj, religie, rasă, origine etnică, opinie și calitate de membru de sindicat și/sau politică;
- 2.10 În cazul în care contractul de angajare este reziliat din orice motiv, UTILIZATORII companiei trebuie să restituie toate ECHIPAMENTELE DE TEHNOLOGIE A INFORMAȚIEI și instrumentele de lucru acordate acestora și condițiile de utilizare. Ștergerea tuturor datelor scrise pe aceste ECHIPAMENTE DE TEHNOLOGIE A INFORMAȚIEI și pe instrumentele de lucru se va face întotdeauna în prezența companiei, de către persoana responsabilă;
- 2.11 În orice caz, compania are dreptul de a folosi în mod diferit ECHIPAMENTELE DE TEHNOLOGIE A INFORMAȚIEI acordate UTILIZATORILOR CORPORATIVI, de a solicita restituirea imediată a acestora și/sau de a verifica dacă sunt utilizate corect.

3. FOLOSIREA ECHIPAMENTELOR DE TEHNOLOGIE A INFORMAȚIEI

În scopurile specificate mai sus, orice acțiune sau atitudine care intră în contradicție cu instrucțiunile anterioare este interzisă. Mai jos sunt prezentate exemple în scop de indicație:

- 3.1 Pentru a împiedica pericolul unui virus de computer și de avariere a stabilității computerelor personale și aplicațiilor acestora, utilizatorii au dreptul de a instala programe externe numai cu autorizația explicită a COMPANIEI.
- 3.2 Este interzisă instalarea și folosirea de programe care nu sunt autorizate de companie, iar aceasta își va da acordul dacă sunt îndeplinite obligațiile impuse prin lege privind drepturile de copyright și protecția legală a produsului software.
- 3.3 Este interzisă modificarea configurațiilor setate pe ECHIPAMENTELE DE TEHNOLOGIE A INFORMAȚIEI fără autorizația anterioară a COMPANIEI.
- 3.4 Este interzisă instalarea pe și/sau conectarea la ECHIPAMENTELE DE TEHNOLOGIE A INFORMAȚIEI a oricăror dispozitive periferice suplimentare care nu sunt autorizate de COMPANIE.
- 3.5 Pe un sistem PC dotat cu dispozitive audio și/sau player CD/DVD, este interzisă audierea de fișiere audio sau muzicale sau vizionare de clipuri video și de filme dacă acest lucru nu este în legătură directă cu postul respectiv.
- 3.6 Utilizatorii nu își vor lăsa propriile ECHIPAMENTE DE TEHNOLOGIE A INFORMAȚIEI nesupravegheate și/sau accesibile altora. În cursul unor absențe îndelungate de la birou, se va activa funcția de Blocare PC/echipamente.
- 3.7 Este interzisă lăsarea oricăror ECHIPAMENTE DE TEHNOLOGIE A INFORMAȚIEI portabile (laptop-uri, PDA-uri, telefoane inteligente și mobile, proiectoare video, etc.) nesupravegheate și/sau accesibile altor persoane în cursul transferurilor (de exemplu în zonele de parcare etc.), călătoriilor de afaceri (de exemplu: aeroporturi, stații, etc.), sau, în cazul absenței din companie (concedii, în week-end sau pe timpul nopții).

4. PAROLE

- 4.1 Parolele care permit accesul la rețeaua LAN a companiei vor rămâne secrete; de aceea întreg personalul va păstra secretul parolelor.
- 4.2 Parolele nu se vor acorda nimănui. Etichetele și/sau biletele care conțin numele de utilizator și/sau parolele nu pot fi expuse pe PC.
- 4.3 Parolele trebuie să aibă 8 caractere, nu trebuie să conțină referințe la utilizator, trebuie să fie modificate de către utilizator la prima accesare și trebuie să fie modificate cel puțin o dată pe trimestru.
- 4.4 Este absolut interzisă folosirea parolelor care aparțin altor UTILIZATORI CORPORATIVI, chiar dacă acces se face către zone protejate în numele aceluiași UTILIZATORI CORPORATIVI, cu excepția cazului în care acest lucru este autorizat în mod explicit de directorul UTILIZATORULUI și de DIRECTORUL DE SECURITATE.

5. FOLOSIREA REȚELEI LAN A COMPANIEI

- 5.1 Unitățile de rețea și zona Workspace sunt zone partajate care conțin informații strict profesionale, care nu pot fi folosite în alte scopuri.
Modurile operaționale pentru a avea acces în mod corect la datele electronice sunt specificate în detaliu în Instrucțiunile procedurale/de operare adoptate de companie și de COMPANIA-MAMĂ, care fac parte integrală din acest document.
Compania are dreptul de a modifica autorizațiile de acces la rețeaua LAN a companiei și la aplicațiile relevante, în cazul în care integritatea tuturor datelor și informațiilor companiei este riscată, chiar și potențial.
- 5.2 Niciun fișier care nu este relevant pentru activitățile profesionale nu va fi introdus, nici măcar pe timp scurt, în SISTEMUL INFORMATIC al companiei și în ECHIPAMENTELE DE TEHNOLOGIE A INFORMAȚIEI.
- 5.3 Accesul fiecărui angajat la orice resurse care țin de SISTEMUL INFORMATIC al companiei (directoare din rețeaua LAN a companiei, zonele compune etc.) trebuie autorizat de Directorul relevant în baza sarcinilor alocate fiecărui angajat; astfel, fiecare UTILIZATOR CORPORATIV va folosi rețeaua LAN a companiei în scopuri strict legate de sarcinile sale, în conformitate cu baza în care a fost acordată autorizația.
- 5.4 Fiecare UTILIZATOR CORPORATIV va proteja natura confidențială a datelor pe care le procesează, acordând atenție specială datelor partajate și oricăror copii pe hârtie ale datelor electronice, eliminându-le în același timp, când aceste date nu mai sunt necesare; în special este recomandat să se protejeze cu parolă toate documentele care sunt puse temporar în zonele partajate la care au acces toți UTILIZATORII CORPORATIVI.
- 5.5 În orice moment, compania are dreptul de a elimina orice fișier sau aplicație considerată periculoasă pentru securitatea sistemului și orice fișier sau aplicație a cărei obținere și/sau instalare încalcă prezentul Cod de conduită IT; în special, compania are dreptul de a șterge datele salvate în zonele partajate comune pentru toți UTILIZATORII CORPORATIVI în termen de 24 de ore de la salvarea acestora.
- 5.6 Este interzisă instalarea și folosirea de software și/sau hardware pentru a intercepta conversații (de orice formă, conversație prin telefon, sms, e-mail etc.) și a falsifica, modifica sau șterge conținutul comunicatelor și /sau documentelor IT ale companiei.
- 5.7 Este interzisă conectarea la rețeaua LAN a companiei a oricărui sistem PC sau dispozitiv de tehnologie a informației care nu îi aparține companiei, cu excepția cazului în care acest lucru este autorizat în mod explicit de companie.

6. FOLOSIREA REȚELEI DE INTERNET ȘI A SERVICIILOR AFERENTE

Compania garantează, dar numai acelor UTILIZATORI care au nevoie de aceasta, accesul la internet de la propriul loc de muncă. Conexiunea la internet va fi păstrată numai atâta timp cât este necesar pentru a efectua activitățile legate de utilizarea internetului. De aceea:

- 6.1 Este interzisă navigarea către site-uri care nu sunt legate de activitățile profesionale;

- 6.2 Este interzisă descărcarea și stocarea de documente neautorizate și de documente jignitoare/discriminante despre sex, limbă, religie, rasă, origine etnică, opinie și calitatea de membru la sindicat și/sau politică;
- 6.3 Este interzisă executarea oricăror tranzacții financiare, inclusiv operațiuni de banking la distanță, achiziții on-line și operațiuni similare, cu excepția acelor cazuri prevăzute de procedurile companiei privind achizițiile companiei;
- 6.4 Este interzisă descărcarea de pe site-uri de internet a oricărui tip de software, cu excepția cazului în care acest lucru este autorizat în mod explicit de COMPANIE;
- 6.5 Este interzisă efectuarea oricărei înregistrări pe site-uri al căror conținut nu este relevant pentru activitățile profesionale ale angajatului respectiv;
- 6.6 Este interzisă folosirea și consultarea, din motive personale, a unor servicii ca forumuri, rețele sociale, linii de chat, grupuri de știri, buletine electronice de notificare sau altele și înregistrarea în cărțile de oaspeți, chiar folosind porecle;
- 6.7 Este interzisă înregistrarea pe forumuri, linii de chat, bloguri, buletine de știri sau site-uri web de pe internet relevante pentru activitățile profesionale, folosind adresa de email a companiei, cu excepția cazurilor când acest lucru este autorizat specific, anterior, de către Directorul relevant de departament. În orice caz, fiecare este direct responsabil pentru folosirea corectă și legitimă a adresei de e-mail a companiei, precum și conținutul declarațiilor și informațiilor transmise;
- 6.8 Singura conexiune autorizată la internet este la rețeaua LAN a companiei; orice alte conexiuni, de exemplu cele folosind liniile telefonice ale companiei, sunt deci neautorizate;
- 6.9 În orice moment, compania și COMPANIA-MAMĂ au dreptul de a activa filtre privind navigarea pe internet, blocând accesul la site-uri care nu sunt relevante pentru activitatea profesională, la site-uri periculoase sau la site-uri care pot cauza o încălcare a acestui Cod și a procedurilor/instrucțiunilor relevante adoptate de companie și DE COMPANIA-MAMĂ, conform legislației în vigoare.

7. FOLOSIREA POȘTEI ELECTRONICE

COMPANIA oferă, în funcție de necesitățile UTILIZATORILOR care au nevoie de aceasta, o căsuță personală de e-mail, alocată în mod inechivoc. De asemenea, căsuța de e-mail reprezintă un instrument de lucru disponibil pentru îndeplinirea activităților relevante pentru sarcinile alocate, de aceea adresa atribuită s UTILIZATORILOR companiei este personală dar nu privată. Fiecare persoană este direct responsabilă în fața comitetului disciplinar și a legii pentru conținutul propriei sale căsuțe poștale și a mesajelor expediate.

Folosirea căsuțelor poștale se va face cu respectarea procedurilor interne și a acestor reguli:

- 7.1 Este interzisă folosirea poștei electronice, atât interne cât externe, din motive fără legătură cu activitățile profesionale;
- 7.2 Este interzisă trimiterea sau înregistrarea oricăror mesaje, interne sau externe, de natură jignitoare și/sau discriminantă referitoare la sex, limbă, religie, rasă, origine etnică, opinie și calitate de membru de sindicat și/sau politică;
- 7.3 Toate mesajele externe, trimise sau primite, pot și partajate și vizualizate în cadrul companiei;
- 7.4 Este interzisă folosirea poștei electronice aparținând altor UTILIZATORI CORPORATIVI pentru trimiterea de mesaje în nume propriu sau în numele acestor alți utilizatori, cu excepția cazurilor în care există autorizația explicită a utilizatorului respectiv. În cazul unei absențe plănuită a angajatului, se recomandă ca UTILIZATORUL companiei să își partajeze căsuța poștală, activând un răspuns automat (așa-numitul „mesaj de absență”) cu indicarea posibilă a persoanelor de referință care trebuie contactate în caz de urgență și a datelor de referință electronice și/sau telefonice ale acestora. Mesajul „de absență” trebuie activat atât pentru expeditori interni și externi;
- 7.5 Accesul la căsuța poștală a unui UTILIZATOR CORPORATIV absent și cunoașterea tuturor mesajelor necesare poate avea loc în conformitate cu prevederile legislației în vigoare și conform instrucțiunilor menționate în procedurile specifice adoptate de companie;

- 7.6 Căsuțele poștale personale sunt create și alocate fără nicio configurare pentru partajare și/sau reguli. Fiecare UTILIZATOR CORPORATIV este deci responsabil pentru orice partajare și/sau regulă aplicată căsuței sale poștale electronice. În plus, se aplică și regulile conform alineatului 2.8 privind partajarea documentelor și informațiilor în zonele comune;
- 7.7 Este interzisă crearea, consultarea și folosirea de căsuțe poștale private în cadrul căsuțelor poștale electronice alocate UTILIZATORILOR companiei de către companie;
- 7.8 În orice caz, compania a pus la dispoziție unele adrese partajate de mai mulți UTILIZATORI CORPORATIVI, anulând natura non-confidențială a acestor mesaje. Aceste adrese corespund în general unor căsuțe poștale de serviciu sau funcționale. Toate comunicatele externe, trimise sau primite prin intermediul acestor adrese, vor fi înregistrate.

8. CONTROLURI

- 8.1 Cu respectarea reglementărilor legale, compania va verifica periodic ECHIPAMENTELE DE TEHNOLOGIE A INFORMAȚIEI ale companiei alocate utilizatorilor (inclusiv telefoanele celulare), modul de folosire a acestora și programele și/sau aplicațiile aferente, pentru a detecta orice eventual virus de computer, a garanta integritatea și securitatea sistemului, a le verifica folosirea corectă și a împiedica orice acțiune sau comportament care poate periclita integritatea tuturor datelor companiei.
- 8.2 Cu respectarea prevederilor legislației în vigoare, compania va organiza verificări specifice dar nu regulate privind folosirea e-mail-ului și internetului prin analizarea datelor agregate, pentru a verifica folosirea corectă a serviciilor și a preveni orice eventual comportament care poate periclita integritatea tuturor datelor companiei.
- 8.3 Dacă în angajat este autorizat să acceseze anumite informații privind SISTEMUL INFORMATIC al companiei, această autorizație va fi considerată strict limitată la executarea sarcinilor profesionale, cu respectarea formularelor de autorizație emise anterior. Compania, cu asistența eventuală a COMPANIEI-MAMĂ, va executa verificări specifice, dar nu regulate, conform legislației în vigoare, asupra profilurilor UTILIZATORILOR, pentru a verifica accesul la și managementul datelor companiei, precum și consistența sarcinilor alocate, profilul și autorizațiile acordate, a descoperi orice comportament care poate periclita integritatea tuturor datelor companiei.
- 8.4 Datele analizate în cursul acestor verificări nu sunt asociate automat sau sistematic unor UTILIZATORI CORPORATIVI identificați, dar ca urmare a naturii acestora pot identifica acești utilizatori prin procesarea și asocierea acestora cu alte date.
- 8.5 În cazul în care se analizează profilele de autorizație de acces, compania va avea dreptul de a lua toate măsurile necesare pentru a se proteja, considerând aceste încălcări ca o gravă ne-respectare a legii și a contractului de angajare.
- 8.6 Eventualele date de internet și analiza acestora se va folosi numai pentru a extrage informații statistice despre folosirea site-urilor și de asemenea pentru a verifica periodic folosirea corectă a acestora, aceste date fiind păstrate pentru o perioadă de timp limitată, conform legislației în vigoare.
- 8.7 Toate aceste date pot fi folosite pentru a verifica răspunderea în cazul unor eventuale ofense informaționale la adresa companiei, precum și în caz de litigii.
- 8.8 Fiecare angajat trimite notificări cu privire la orice încălcare a acestui COD DE CONDUITĂ IT la adresa de e-mail ia-odv@gewiss.com, conform prevederilor din „Politica de denunțare” disponibilă pe site-ul web și pe avizierul companiei.
- 8.9 Compania promovează respectarea standardelor de comportament incluse în acest document și îi va raporta imediat Directorului de audit intern corporativ, prin intermediul Directorului de securitate sau a oricărei alte persoane responsabile, cu privire la orice încălcare a regulilor din acest Cod.

9. NE-RESPECTAREA INSTRUCȚIUNILOR ȘI SANCTIUNILOR

- 9.1 Ne-respectarea regulilor specificate în acest COD DE CONDUITĂ IT va face obiectul unei evaluări disciplinare conform legislației în vigoare, aplicabil și în domeniul juridic.

- 9.2 Compania va solicita compensații din partea persoanelor responsabile de eventuale daune rezultate din folosirea necinstită sau incorectă a regulilor din acest COD DE CONDUITĂ IT.
- 9.3 În conformitate cu legea, utilizatorii companiei pot fi chemați să răspundă și din punct de vedere disciplinar, în caz de furt, pierdere și orice eventuală avariere suferită de echipamentele de tehnologie a informației ca urmare a folosirii necinstite a acestora; suma aferentă acestor daune poate fi taxată pe statele de plată.