# Scop, domeniu de aplicare și utilizatori

Scopul acestui document este de a defini norme clare pentru utilizarea sistemului informațional și a altor active informaționale în RENOMIA SRBA.

Utilizatorii acestui document sunt toți angajații RENOMIA SRBA.

# Reguli de bază de securitate

## Definiții

**Sistemul informațional** – include toate serverele și sistemele client, infrastructura rețelei, software-ul de sistem și de aplicație, datele și alte subsisteme informatice și componente care sunt deținute sau utilizate de către organizație sau care se află sub responsabilitatea organizației. Utilizarea unui sistem informațional include, de asemenea, utilizarea tuturor serviciilor interne sau externe, ar fi accesul la internet, e-mail, etc.

**Active informatice** – în contextul acestei politici, termenul *active informatice* este aplicat sistemelor informaționale și altor informații/echipamente, inclusiv documente de hârtie, telefoane mobile, computere portabile, suporturi de stocare a datelor etc.

## Utilizare acceptabilă

Activele informatice pot fi utilizate numai pentru nevoile afacerii în scopul executării sarcinilor legate de organizație.

## Responsabilitatea pentru active

Fiecare activ informatic are un proprietar desemnat în inventarul activelor. Proprietarul activului este responsabil pentru confidențialitatea, integritatea și disponibilitatea informațiilor din activul în cauză.

## Activități interzise

Este interzisă utilizarea activelor informative într-un mod care să preia în mod inutil capacitatea, să slăbească performanța sistemului de informații sau să constituie o amenințare de securitate. De asemenea, este interzisă:

* descărcarea imaginilor sau a fișierelor video care nu au un scop de afaceri, trimiterea scrisorilor de e-mail lanț, jucarea jocurilor, etc
* instalarea software-ului pe un computer local fără permisiune explicită de la [job title]
* utilizarea aplicațiilor Java, controalelor Active X sau a unui alt cod mobil, cu excepția cazului în care sunt autorizate de către [job title]
* utilizarea de instrumente criptografice (criptare) pe un computer local, cu excepția cazurilor descrise în politica de protecție a datelor personale sau aprobate de către [job title]
* instalarea sau utilizarea de dispozitive periferice, cum ar fi modemuri, carduri de memorie sau alte dispozitive pentru stocarea și citirea datelor (de exemplu, unități flash USB) fără permisiune explicită de la [job title];

## Preluarea activelor în afara RENOMIA SRBA

Echipamentele, informațiile sau software-ul, indiferent de forma sau mediul de stocare, nu pot fi scoase din sediile RENOMIA SRBA fără permisiunea scrisă primită de la [job title].

Atâta timp cât activele sunt în afara organizației, acestea trebuie să fie controlate de către persoana care a primit permisiunea pentru îndepărtarea lor.

## Restituirea activelor la rezilierea contractului

La rezilierea contractului de muncă sau a altui contract pe baza căruia sunt utilizate diverse echipamente, software sau informații în format electronic sau de hârtie, utilizatorul trebuie să returneze toate aceste active informatice la [titlu Job].

## Procedura de copiere de rezervă

Utilizatorul trebuie [specifica metoda de procedura de backup] toate informațiile sensibile stocate pe calculatorul său cel puțin o dată pe zi.

## Protecție antivirus

[nume de software antivirus] trebuie să fie instalat pe fiecare computer cu actualizări automate activate.

## Autorizații pentru utilizarea sistemului informațional

Utilizatorii sistemului de informații pot accesa doar acele active ale sistemului de informații pentru care au fost autorizați în mod explicit de către proprietarul activului.

Utilizatorii pot utiliza sistemul informațional numai în scopurile pentru care au fost autorizați, adică pentru care li s-au acordat drepturi de acces.

Utilizatorii nu trebuie să ia parte la activități care pot fi utilizate pentru a ocoli controalele de securitate ale sistemului de informații.

## Responsabilitățile contului de utilizator

Utilizatorul nu trebuie, direct sau indirect, să permită altei persoane să-și folosească drepturile de acces, adică numele de utilizator și nu trebuie să utilizeze numele de utilizator și/sau parola altei persoane. Utilizarea numelor de utilizator de grup este interzisă.

Proprietarul contului de utilizator este utilizatorul său, care este responsabil pentru utilizarea sa și pentru toate tranzacțiile efectuate prin intermediul acestui cont de utilizator.

## Responsabilitățile parolei

Utilizatorii trebuie să aplice bune practici de securitate la selectarea și utilizarea parolelor:

* parolele nu trebuie divulgate altor persoane, inclusiv administratorilor de management și de sistem
* parolele nu trebuie să fie scrise pe hârtii, cu excepția cazului în care o metodă sigură a fost aprobată de către [job title]
* parolele generate de utilizator nu pot fi distribuite prin intermediul oricărui canal (utilizând distribuția orală, scrisă sau electronică etc.)
* parolele trebuie modificate dacă există indicii că parolele sau sistemul ar fi putut fi compromise – în acest caz trebuie raportat un incident de securitate
* trebuie selectate parole puternice, în felul următor:
	+ utilizarea a cel puțin douăsprezece caractere
	+ utilizarea a cel puțin unui caracter numeric
	+ utilizarea a cel puțin unei majuscule și a cel puțin unui caracter alfabetic minuscul
	+ folosind cel puțin un caracter special
	+ o parolă nu trebuie să fie un cuvânt din dicționar, dintr-un dialect sau jargon din orice limbă, sau oricare dintre aceste cuvinte scrise înapoi
	+ parolele nu trebuie să se bazeze pe date cu caracter personal (de exemplu, data nașterii, adresa, numele membrului familiei etc.)
	+ ultimele trei parole nu trebuie să fie re-utilizate
* parolele trebuie schimbate la fiecare 3 luni
* parola trebuie să fie schimbat la primul log-on la un sistem
* parolele nu trebuie stocate într-un sistem de log on automatizat (de exemplu, macrocomandă sau browser)
* parolele utilizate în scopuri private nu trebuie utilizate în scopuri de afaceri

## Utilizarea internetului

Internetul poate fi accesat numai prin intermediul rețelei locale a organizației, cu o infrastructură adecvată și protecție firewall. Accesul direct la internet prin modemuri, Internet mobil, rețea wireless sau alte dispozitive de acces direct la internet este interzis.

[Job title] poate bloca accesul la unele pagini de Internet pentru utilizatorii individuali, grupuri de utilizatori sau toți angajații organizației. În cazul în care accesul la unele pagini web este blocat, utilizatorul poate trimite o cerere în scris la [job title] pentru autorizarea de a accesa astfel de pagini. Utilizatorul nu trebuie să încerce să ocolească această restricție în mod autonom.

Utilizatorul trebuie să considere informațiile primite prin intermediul unui site neverificat ca fiind nesigure. Aceste informații pot fi utilizate în scopuri de afaceri numai după ce a fost verificată autenticitatea și corectitudinea acestora.

Utilizatorul este responsabil pentru toate consecințele posibile care decurg din utilizarea neautorizată sau necorespunzătoare a serviciilor de Internet sau a conținutului.

## E-mail și alte metode de schimb de mesaje

Metodele de schimb de mesaje, altele decât poșta electronică, includ, de asemenea, descărcarea fișierelor de pe Internet, transferul de date prin intermediul [furnizează nume de sisteme de comunicare specializate], telefoane, faxuri, trimiterea mesajelor SMS mesaje text, medii portabile și forumuri și rețele sociale.

 [Job title] determină canalul de comunicație care poate fi utilizat pentru fiecare tip de date, precum și posibilele restricții, adică definește ce activități sunt interzise.

Utilizatorii pot trimite doar mesaje ce conțin informații adevărate. Este interzis a trimite materiale deranjante, neplăcute, sexual explicite, nepoliticoase, calomnioase sau având orice alt conținut inacceptabil sau ilegal. Utilizatorii nu trebuie să trimită mesaje de spam persoanelor cu care nu s-a stabilit nicio relație de afaceri sau persoanelor care nu au solicitat astfel de informații.

În cazul în care un utilizator primește un e-mail de spam, el/ea trebuie să informeze [titlu Job].

Dacă trimiteți un mesaj cu o etichetă de confidențialitate, utilizatorul trebuie să îl protejeze.

Utilizatorul trebuie să salveze fiecare mesaj care conține date semnificative pentru activitatea organizației utilizând metoda specificată de [job title].

Fiecare mesaj de poștă electronică trebuie să conțină un disclaimer, cu excepția mesajelor trimise prin sisteme de comunicații determinate de [titlul funcției]. În cazul în care un utilizator postează un mesaj pe un sistem de schimb de mesaje (rețele sociale, forumuri etc.), el/ea trebuie să precizeze fără echivoc că nu reprezintă punctul de vedere al organizației.

## Copyright

Utilizatorii nu trebuie să facă copii neautorizate ale software-ului deținute de organizație, cu excepția cazurilor permise de lege, de către proprietar sau [job title].

Utilizatorii nu trebuie să copieze software-ul sau alte materiale originale din alte surse, și sunt răspunzători pentru toate consecințele care ar putea apărea sub legea proprietății intelectuale.