

**Aprobat
Presedintele Consiliului de
Administratie**

Gheorghe Nicolae

**Reguli si proceduri pentru securitatea si controlul sistemelor informatice,
pentru a stoca documentele transmise si primite prin INTERNET si pentru asigurarea confidentialitatii
si pastrarea in siguranta a datelor si informatiilor stocate, inclusiv recuperarea acestora in caz de dezastru**

În acord cu prevederile din prezentele reguli si proceduri, sistemele informatice sunt bunuri strategice ale SSIF ROMBELL SECURITIES SA care sunt administrate in scopul asigurarii confidentialitatii informatiilor stocate, a fisierelor si a bazelor de date.

Politica de Securitate si Control a Resurselor Informatice se aplică nediscriminatoriu tuturor persoanelor care au acces la orice resursă informatică și de comunicații a societatii.

Următoarele entități și utilizatori sunt vizați în mod distinct de prevederile Politicii:

- angajații cu contract de muncă pe perioadă determinată sau nedeterminată care au acces la sistemul informațional și de comunicații;
- colaboratorii societatii care au acces la Resursele Informatice și de Comunicații;
- furnizorii societatii care au acces la Resursele Informatice și de Comunicații;
- alte persoane, entități sau organizații care au acces la Resursele Informatice și de Comunicații.

Scop

Politica de Securitate si Control a Resurselor Informatice și de Comunicații are ca scop asigurarea integrității, confidențialității și disponibilității informației.

Integritatea se referă la măsurile și procedurile utilizate pentru protecția datelor împotriva modificărilor sau distrugerii neautorizate.

Confidențialitatea se referă la protecția datelor împotriva accesului neautorizat. Fișierele electronice create, trimise, primite sau stocate pe sistemele de calcul aflate în proprietatea, administrarea sau în custodia și sub controlul societatii, sunt proprietatea SSIF ROMBELL SECURITIES SA în condițiile legilor si regulamentelor în vigoare din piata de capital. Utilizatorul răspunde personal de confidențialitatea datelor încredințate prin alocarea de parole si coduri de acces la Resursele Informatice și de Comunicații.

Disponibilitatea se asigură prin funcționarea continuă a tuturor componentelor Resurselor Informatice și de Comunicații. Diverse aplicații au nevoie de nivele diferite de disponibilitate în funcție de impactul sau daunele produse ca urmare a nefuncționării corespunzătoare a Resurselor Informatice și de Comunicații.

Politica de Securitate si Control are ca scop, de asemenea, stabilirea cadrului necesar pentru elaborarea regulamentelor și procedurilor de securitate. Acestea sunt obligatorii pentru toți utilizatorii Resurselor Informatice și de Comunicații.

Atribuții și Responsabilități

Departamentul de Tehnologia Informatiei respectiv administratorii de rețea/sistem/baze de date:

- asigura existența jurnalelor și a traseelor pentru orice tip de acces în sistem;
- asigura activarea tuturor mecanismelor de securitate;
- elaborează și propune modificări ale Politicii de Securitate si Control a sistemului informatic;

- elaborează și propune pentru aprobare regulamentele și procedurile de securitate a Resurselor Informatice și de Comunicații în conformitate cu Politica de Securitate și Control a acestora;
 - elaborează proceduri pentru identificarea utilizatorilor;
 - tratarea incidentelor de securitate în scopul minimizării efectului distructiv al acestora asupra Resurselor Informatice și de Comunicații;
 - asigură accesul la sistemele informatice de înregistrare electronică a tranzacțiilor, de evaluare a portofoliului și a evidenței investitorilor de către utilizatori individualizați, pe bază de parolă, care au drepturi predefinite de consultare și/sau de modificare în funcție de atribuțiile fiecărui angajat conform reglementărilor interne ale societății;
 - păstrează înregistrări de rezervă (de back-up) ale informațiilor stocate în sistemele electronice pentru evidența tranzacțiilor și a investitorilor și pentru evaluarea portofoliului;
- Reprezentanții compartimentului de control intern au drepturi de consultare a sistemelor informatice.
- Atribuții ale utilizatorilor:*
- Să cunoască și să respecte prevederile politicii de securitate și control.
 - Să cunoască și să respecte prevederile tuturor Regulamentelor și/sau Procedurilor privind securitatea Resurselor Informatice și de Comunicații.
 - Să răspundă direct de securitatea și conținutul informațiilor și de Resursele Informatice și de Comunicații încredințate direct sau indirect.
 - Trebuie să accepte și să respecte prezentele reguli și proceduri și regulamentele specifice privind Resursele Informatice și de Comunicații.

Confidențialitate

- Fișierele electronice create, trimise, primite sau stocate folosind Resursele Informatice și de Comunicații administrate sau în custodia și sub controlul societății nu au caracter personal și pot fi accesate oricând de către angajații autorizați din cadrul societății.
- În scopul administrării Resurselor Informatice și de Comunicații și pentru asigurarea securității acestora, personalul autorizat poate revizui sau utiliza orice informație stocată sau transportată pe/prin sistemele Resurselor Informatice și de Comunicații în conformitate cu legile și regulamentele în vigoare din piața de capital. În aceleași scopuri, este posibilă monitorizarea activității utilizatorilor.
- Utilizatorii trebuie să raporteze orice slăbiciune în sistemul de securitate al calculatoarelor din cadrul societății, orice incident de posibilă întrebuițare greșită sau încălcare a acestei proceduri.
- Un mare număr de utilizatori (inclusiv clienții societății), pot accesa informații din exteriorul sistemului de comunicații al societății. În aceste condiții este obligatorie păstrarea confidențialității informațiilor transmise din exteriorul societății și a informațiilor obținute din interiorul instituției.
- Utilizatorii nu trebuie să încerce să acceseze informații sau programe pentru care nu au autorizație sau consimțământ explicit.
- Nici un utilizator al Resurselor Informatice și de Comunicații nu poate divulga informațiile la care are acces sau la care a avut acces ca urmare a unei vulnerabilități a sistemelor ce compun Resursele Informatice și de Comunicații. Această regulă se extinde și după ce utilizatorul a încheiat relațiile cu societatea.
- Confidențialitatea și integritatea informațiilor transmise prin intermediul resurselor de comunicații se poate asigura folosind tehnici de criptare. Utilizatorii sunt obligați să se asigure că toate informațiile confidențiale ale societății se transmit în așa fel încât să se asigure confidențialitatea și integritatea acestora.

Furnizorul de servicii internet a fost ales după criteriile bine stabilite, ținând cont de specificul acestei activități. Soluția aleasă include o linie principală pe fibra optică și una secundară tot pe fibra optică, astfel încât coeficientul de acoperire a timpului de conectare să fie aproape de 100%. Banda metropolitană care poate fi alocată poate atinge pragul de 10MB/s, asigurând astfel un număr mare de conexiuni simultane în condiții optime de desfășurare.

Toate resursele hardware prezente sunt alese din rândul celor mai renumiți producători, astfel încât stabilitatea sistemului este garantată.

Computerul pe care ruleaza serverul aplicatiei si al bazei de date este un superserver multiprocesor ce foloseste o solutie mirroring de gestionare a informatiei stocate, reducand astfel riscul de pierdere a informatiei.

Procedura de back-up se efectueaza zilnic pe baza unor script-uri de arhivare zilnica a informatiei implementate in server.

Politica de firewall implementata este una stricta, cu reguli bine definite care minimizeaza posibilitatea atacurilor din exterior. In acelasi timp protectia din interior este structurata prin definirea clara a responsabilitatilor in administrarea resurselor alocate.

Angajatii SSIF ROMBELL SECURITIES SA sunt obligati sa ia la cunostinta si sa aplice prevederile prezentelor reguli si proceduri interne.

Reprezentantul compartimentului de control intern va urmari aplicarea prezentei proceduri si, in caz de incalcare sau abatere, va raporta consiliului de administratie informand imediat conducatorii si auditul intern.

Membrii consiliului de administratie/conducatorii si auditorii interni ai SSIF ROMBELL SECURITIES SA vor notifica cu maxima urgenta CNVM si entitatile pietei de capital implicate situatia constatata si masurile adoptate.

Orice modificare si revizuire intervenite in continutul prezentelor reguli si proceduri proceduri va fi adusa imediat la cunostinta angajatilor SSIF ROMBELL SECURITIES prin grija reprezentantului compartimentului de control intern.

Regulile si procedurile pentru securitatea sistemului informatic, asigurarea confidentialitatii si pastrarea in siguranta a datelor si informatiilor stocate, inclusiv recuperarea acestora in caz de dezastru se modifica si se actualizeaza numai cu aprobarea Departamentului de Tehnologie Informatiei.

Prezentel reguli si proceduri se completeaza de drept cu celelalte prevederi din Legea nr. 297/2004, Regulamentul CNVM nr. 32/2006, precum si orice alte prevederi legale inci

Compartimentul de Control Intern

Gheorghe Nicolae