REGULI SI PROCEDURI PENTRU SECURITATEA SI CONTROLUL SISTEMELOR INFORMATICE

Număr cod intern: P – 03 ed.2, rev. 5
Număr cod ASF: 0003

Exemplarul nr. _
☐ Exemplar controlat
☐ Exemplar necontrolat

APROBAT - Director General – Adrian SIMIONESCU

REVIZUIT - Ofiţer Conformitate – Andi BRĂDICEANU

Data intrării în vigoare: 01.04.2019

LISTA DE CONTROL A REVIZIILOR

Identificarea documentului:

1	Denumire	***REGULI SI PROCEDURI pentru securitatea şi controlul sistemelor informatice***
2	Cod	***P – 03***
3	Ediţie	***2***
4	Revizie	***5***

Nr. Editie /Nr. Revizie	Dată finalizare revizie	Pagini revizuite	Revizuit de:	Aprobat de :	Conţinutul reviziei
2/4	04/04/2018	34	Miu Mihaela	Adrian Simionescu	Revizie periodică: - introducere Listă de control a reviziilor; - revizuire conţinut, fără modificări de Procedură.
2/5	27.02.2019	integral	Brădiceanu Andi	Adrian Simionescu	Revizie periodică: - actualizare reglementări incidente; - revizuire conţinut Procedură.

1. SCOP

Procedura stabileşte regulile și procedurile pentru securitatea și controlul sistemelor informatice, pentru îndeplinirea obligaţiilor de confidenţialitate şi păstrare în siguranţă a datelor şi informaţiilor trimise sau obţinute de la clienţi, prin internet şi stocate, precum şi a celor ce decurg din activitatea aferentă fiecărei funcţii.

2. DOMENIU DE APLICARE

Procedura este aplicabilă activităţilor din cadrul tuturor departamentelor S.S.I.F. Vienna Investment Trust S.A., în exercitarea atribuţiunilor, sarcinilor și competențelor cu care au fost învestite.

3. DEFINIŢII. ABREVIERI

3.1 Definiţii

Definiţiile termenilor utilizaţi sunt preluate din actele normative aplicabile.

Date cu caracter personal - orice informații privind o persoană fizică identificată sau identificabilă („persoana vizată"); o persoană fizică identificabilă este o persoană care poate fi identificată, direct sau indirect, în special prin referire la un element de identificare, cum ar fi un nume, un număr de identificare, date de localizare, un identificator online, sau la unul sau mai multe elemente specifice, proprii identității sale fizice, fiziologice, genetice, psihice, economice, culturale sau sociale;

Arhivare electronică - stocarea documentelor în format digital;

Analiză de risc - analiza scenariilor de amenințări semnificative, pentru a evalua probabilitatea materializării acestora și impactul potențial pe care un astfel de eveniment l-ar avea asupra entităţii şi operaţiunilor acesteia;

Atac etic/test de penetrare - test al sistemelor informatice realizat printr-o simulare a unui atac real asupra rețelelor, sistemelor și programelor informatice utilizate de entitatea testată sau auditată, după caz;

Audit IT - activitatea de colectare și evaluare a unor probe pentru a determina dacă sistemul informatic respectă parametrii de performanțe și de lucru conform cerințelor de proiectare, asigură funcționalitățile necesare cerințelor de afaceri și respectarea legislației în domeniu, este securizat, menține integritatea datelor prelucrate și stocate, permite atingerea obiectivelor strategice ale entității și utilizarea eficientă a resurselor informaționale;

Bază de date – structură de organizare a informației într-unul sau mai multe domenii de aplicare, cu scopul de a o face accesibilă în permanență către utilizatori prin ansamblul de programe informatice;

Centru de date - spațiu securizat, dotat cu tehnică de calcul și echipamente de comunicații prin intermediul cărora se primesc, se stochează și se transmit date în formă electronică, care se implementează respectând standardele specifice, utilizând conceptul de nivel sau un echivalent al acestuia, precum, dar fără a se limita la, standardele SR EN 50600 (European Standard - Data Centers Facilities and Infrastructures) sau TIA-942 (Telecommunications Industry Association);

Incident de securitate – eveniment înregistrat și declarat la nivelul entității privind securitatea informației sau a sistemelor informatice cu o probabilitate semnificativă de compromitere a operațiunilor și de amenințare a securității IT a cărei consecință a determinat sau este de natură să determine compromiterea informațiilor sau a sistemelor informatice;

Indicatori cheie de risc (KRI) – parametrii care măsoară efectiv riscurile aferente procedurilor și activităților entității, furnizând în timp semnalări corespunzătoare ale consecințelor cu efect negativ, care pot genera potențiale pierderi directe sau indirecte;

Infrastructură informatică - elemente ale bazei tehnico- materiale, pe componente sau ca sistem, care susţin culegerea, stocarea şi managementul datelor, precum şi integrarea, căutarea şi vizualizarea datelor şi alte calcule şi servicii de procesare a informaţiei utilizând tehnologii informatice, deţinute sau contractate extern de către entitate şi necesare bunei funcţionări a acesteia;

Risc de securitate - orice circumstanţă sau eveniment care are un efect negativ potenţial asupra securităţii sistemelor informatice;
Risc sistemic - riscul de afectare a unei zone importante a sistemului financiar sau a unei pieţe financiare, cu potenţial de consecinţe negative serioase pentru piaţa internă şi economia reală, instabilitate a sistemului financiar, posibil catastrofică, cauzată sau accentuată de evenimente idiosincratice sau de condiţii ale entităţilor;
Riscuri semnificative - riscuri cu impact însemnat asupra situaţiei financiare, patrimoniale şi/sau reputaţionale a entităţilor;
Raport de testare IT - instrumentul prin care se comunică scopul testării, obiectivele urmărite, normele/standardele aplicate, perioada acoperită, natura, întinderea, procedurile, constatările și concluziile testării, precum și orice rezervă pe care echipa de testare o are asupra sistemului informatic testat;
Sistem informatic - ansamblu de elemente intercorelate funcţional în scopul automatizării obţinerii informaţiilor necesare activităţilor operaţionale şi manageriale într-o entitate, prin intermediul serviciilor IT, al echipamentelor hardware şi produselor software, proceduri manuale, baze de date şi modele matematice pentru analiză, planificare, control şi luarea deciziilor, utilizând componente de introducere şi prelucrare date, componente de procesare precum servere, calculatoare, sisteme software de operare de bază, programe informatice, reţele de calculatoare şi telecomunicaţii, componente de stocare şi utilizatori, fără ca enumerarea să fie limitativă;
Vulnerabilități - stări de fapt, procese și/sau fenomene care diminuează capacitatea de reacție a sistemelor informatice la riscurile existente ori potențiale sau care favorizează apariția și dezvoltarea lor, cu consecințe în planul funcționalității și utilității.
Semnătură electronică – atribut indispensabil al documentului electronic, obţinut în urma transformării criptografice a acestuia, cu utilizarea cheii private, conform prevederilor Legii nr. 455/2001 privind semnătura electronică, republicată.

3.2 Abrevieri

A.S.F.	- Autoritatea de Supraveghere Financiară
S.S.I.F.	- Societate de Servicii de Investiții Financiare
C.N.V.M.	- Comisia Națională a Valorilor Mobiliare
B.V.B.	- Bursa de Valori Bucureşti
A.N.S.P.D.C.P.	- Autoritatea Naţională de Supraveghere a Prelucrării Datelor cu Caracter Personal

4. DOCUMENTE DE REFERINŢĂ

Legea nr. 126/2018 privind pieţele de instrumente financiare, denumită în continuare Legea nr.126/2018 (publicată în Monitorul Oficial al României, Partea I, nr. 521 din 26.06.2018, în vigoare din 06.07.2018).
Norma nr.4/2018 privind gestionarea riscurilor operaționale generate de sistemele informatice utilizate de entitățile autorizate/avizate/înregistrate, reglementate și/sau supravegheate de către Autoritatea de Supraveghere Financiară
Regulamentul nr. 679/2016 privind protecţia persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal şi privind libera circulaţie a acestor date şi de abrogare a Directivei 95/46/CE (Regulamentul general privind protecţia datelor)
Codul Depozitarului Central S.A., cu modificările şi completările ulterioare (Codul D.C.)
Regulamentul nr. 2/2016 privind aplicarea principiilor de guvernanţă corporativă de către entităţile autorizate, reglementate şi supravegheate de ASF.
Acte normative aplicabile, în vigoare.

5. MANAGEMENTUL SOCIETĂȚII ȘI SECURITATEA INFORMAȚIEI

Conducerea societăţii S.S.I.F. Vienna Investment Trust S.A. este conştientă de pericolele potenţiale pe care le prezintă sistemele informatice. Astfel, adoptă “Reguli și proceduri pentru securitatea si controlul sistemelor informatice”, pentru asigurarea unui înalt nivel de protecţie, într-un mod corect şi eficient. Politicile sunt accesibile tuturor angajaţilor, partenerilor şi clienților.

Securitatea informației face parte din responsabilitățile angajatului și, în același timp, este o obligație legală.

Managerii de departamente sunt responsabili atât pentru comunicarea în cadrul departamentelor lor a cerințelor definite de conducerea societății împreună cu departamentul de IT și Managerul de riscuri în ceea ce privește protecția informației și a datelor cu caracter personal, cât și pentru respectarea/implementarea acestor cerințe.

Angajații vor fi instruiți periodic și adecvat cu privire la protecția informațiilor și a datelor.

Managementul va fi un exemplu de comportament adecvat privind securitatea informației.

Obiectivul securității informaţiei este de a proteja bunurile informaționale ale S.S.I.F. Vienna Investment Trust S.A., ale clienților și partenerilor, de a sigura continuitatea serviciilor și de a reduce potenţialele daune aduse societății prin prevenirea și minimizarea impactului incidentelor de securitate.

Politica pentru securitatea informațiilor este aprobată de management și reflectă angajarea conducerii S.S.I.F. Vienna Investment Trust S.A. în implemetarea și menţinerea unui Sistem de Management al Securității Informației, prin intermediul căruia să putem proteja bunurile informaționale ale societății de toate amenințările, fie ele interne sau externe, deliberate sau accidentale.

Prin conformitatea cu standardul ISO 27001 ne asiguram că:

- Informațiile vor fi protejate împotriva accesului neautorizat;
- Confidențialitatea informațiilor va fi păstrată;
- Integritatea informațiilor va fi păstrată;
- Disponibilitatea informațiilor va fi asigurată;
- Cerințele legislative aplicabile sunt îndeplinite;
- Planurile de Continuitate sunt menținute/actualizate și testate;
- Întregul personal va fi instruit cu privire la securitatea informațiilor;
- Toate incidentele de securitate, reale sau suspecte, vor fi raportate către administratorul de sistem, iar în lipsa acestuia Directorului General.

Este responsabilitatea fiecărui angajat al societății să adere la aceste Reguli şi Proceduri, să cunoască și să aplice prevederile prezentei.

6. PROCEDURA

Secţiunea 1 - Date cu caracter personal

Art.1. Prin prelucrarea datelor cu caracter personal se înţelege orice operaţiune sau set de operaţiuni care se efectuează asupra datelor cu caracter personal (informaţii referitoare la o persoană fizică identificată sau identificabilă – numele şi prenumele, data şi locul naşterii, cetăţenia, naționalitatea, țara de origine, calitatea de rezident/nerezident, semnătura, telefon, fax, domiciliul stabil/reședința, e-mail, profesie, loc de muncă, situaţie familială, situaţie economică şi financiară, date bancare, date privind bunurile deţinute, cod numeric personal sau echivalentul acestuia pentru persoanele străine, seria şi numărul documentului de identitate, data eliberării documentului și entitatea care l-a emis etc.), prin mijloace automate sau neautomate, cum ar fi colectarea, înregistrarea, organizarea, stocarea, adaptarea ori modificarea, extragerea, consultarea, utilizarea, dezvăluirea către terţi prin transmitere, diseminare sau în orice alt mod, alăturarea sau combinarea, blocarea, ştergerea sau distrugerea.-

Art.2. (1) Datele cu caracter personal sunt:

(a) prelucrate în mod legal, echitabil și transparent față de persoana vizată („legalitate, echitate și transparență”);

(b) colectate în scopuri determinate, explicite și legitime și nu sunt prelucrate ulterior într-un mod incompatibil cu aceste scopuri; prelucrarea ulterioară în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice nu este considerată incompatibilă cu scopurile inițiale;
(c) adecvate, relevante și limitate la ceea ce este necesar în raport cu scopurile în care sunt prelucrate („reducerea la minimum a datelor”);
(d) exacte și, în cazul în care este necesar, actualizate; se vor adopta toate măsurile necesare pentru a se asigura că datele cu caracter personal care sunt inexacte, având în vedere scopurile pentru care sunt prelucrate, sunt șterse sau rectificate fără întârziere („exactitate”);
(e) păstrate într-o formă care permite identificarea persoanelor vizate pe o perioadă care nu depășește perioada necesară îndeplinirii scopurilor în care sunt prelucrate datele; datele cu caracter personal pot fi stocate pe perioade mai lungi în măsura în care acestea vor fi prelucrate exclusiv în scopuri de arhivare în interes public, în scopuri de cercetare științifică sau istorică ori în scopuri statistice, sub rezerva punerii în aplicare a măsurilor de ordin tehnic și organizatoric adecvate prevăzute în Regulamentul general privind protecţia datelor în vederea garantării drepturilor și libertăților persoanei vizate („limitări legate de stocare”);
(f) prelucrate într-un mod care asigură securitatea adecvată a datelor cu caracter personal, inclusiv protecția împotriva prelucrării neautorizate sau ilegale și împotriva pierderii, a distrugerii sau a deteriorării accidentale, prin luarea de măsuri tehnice sau organizatorice corespunzătoare („integritate și confidențialitate”).
(2) Societatea este responsabilă de respectarea alineatului (1) și poate demonstra această respectare („responsabilitate”).
(3) Prelucrarea este considerată legală numai dacă și în măsura în care se aplică cel puțin una dintre următoarele condiții:
(a) persoana vizată și-a dat consimțământul pentru prelucrarea datelor sale cu caracter personal pentru unul sau mai multe scopuri specifice;
(b) prelucrarea este necesară pentru executarea unui contract la care persoana vizată este parte sau pentru a face demersuri la cererea persoanei vizate înainte de încheierea unui contract;
(c) prelucrarea este necesară în vederea îndeplinirii unei obligații legale care îi revine societăţii;
(d) prelucrarea este necesară pentru a proteja interesele vitale ale persoanei vizate sau ale altei persoane fizice;
(e) prelucrarea este necesară pentru îndeplinirea unei sarcini care servește unui interes public sau care rezultă din exercitarea autorității publice cu care este învestită societatea;
(f) prelucrarea este necesară în scopul intereselor legitime urmărite de societate sau de o parte terță, cu excepția cazului în care prevalează interesele sau drepturile și libertățile fundamentale ale persoanei vizate, care necesită protejarea datelor cu caracter personal, în special atunci când persoana vizată este un copil.
Litera (f) nu se aplică în cazul prelucrării efectuate de autorități publice în îndeplinirea atribuțiilor lor.
(4) În cazul în care prelucrarea în alt scop decât cel pentru care datele cu caracter personal au fost colectate nu se bazează pe consimțământul persoanei vizate sau pe dreptul Uniunii sau dreptul intern, societatea, pentru a stabili dacă prelucrarea în alt scop este compatibilă cu scopul pentru care datele cu caracter personal au fost colectate inițial, ia în considerare, printre altele:
(a) orice legătură dintre scopurile în care datele cu caracter personal au fost colectate și scopurile prelucrării ulterioare preconizate;
(b) contextul în care datele cu caracter personal au fost colectate, în special în ceea ce privește relația dintre persoanele vizate și societate;
(c) natura datelor cu caracter personal, în special în cazul prelucrării unor categorii speciale de date cu caracter personal, sau în cazul în care sunt prelucrate date cu caracter personal referitoare la condamnări penale și infracțiuni;
(d) posibilele consecințe asupra persoanelor vizate ale prelucrării ulterioare preconizate;
(e) existența unor garanții adecvate, care pot include criptarea sau pseudonimizarea.

Art.3. S.S.I.F. Vienna Investment Trust desemnează un responsabil cu protecția datelor.
(2) Responsabilul cu protecția datelor are cel puțin următoarele sarcini:
(a) informarea și consilierea societăţii, precum și a angajaților care se ocupă de prelucrare, cu privire la obligațiile care le revin în temeiul Regulamentului general privind protecţia datelor și al altor dispoziții de drept al Uniunii sau drept intern referitoare la protecția datelor;
(b) monitorizarea respectării Regulamentului general privind protecţia datelor, a altor dispoziții de drept al Uniunii sau de drept intern referitoare la protecția datelor și a politicilor societăţii sau ale persoanei împuternicite în ceea ce privește protecția datelor cu caracter personal, inclusiv alocarea responsabilităților și acțiunile de sensibilizare și de formare a personalului implicat în operațiunile de prelucrare, precum și auditurile aferente;
(c) furnizarea de consiliere la cerere în ceea ce privește evaluarea impactului asupra protecției datelor și monitorizarea funcționării acesteia;
(d) cooperarea cu autoritatea de supraveghere;
(e) asumarea rolului de punct de contact pentru autoritatea de supraveghere privind aspectele legate de prelucrare precum și, dacă este cazul, consultarea cu privire la orice altă chestiune.

Art.4.(1) În cazul în care datele cu caracter personal referitoare la o persoană vizată sunt colectate de la aceasta, societatea, în momentul obţinerii acestor date cu caracter personal, furnizează persoanei vizate toate informaţiile următoare:

a. identitatea şi datele de contact ale societăţii şi, după caz, ale reprezentantului acestuia;
b. datele de contact ale responsabilului cu protecţia datelor, după caz;
c. scopurile în care sunt prelucrate datele cu caracter personal, precum şi temeiul juridic al prelucrării;
d. în cazul în care prelucrarea se face în temeiul articolului 6 alineatul (1) litera (f) din Regulamentul general privind protecţia datelor, interesele legitime urmărite de operator sau de o parte terţă;
e. destinatarii sau categoriile de destinatari ai datelor cu caracter personal;
f. dacă este cazul, intenţia societăţii de a transfera date cu caracter personal către o ţară terţă sau o organizaţie internaţională şi existenţa sau absenţa unei decizii a Comisiei privind caracterul adecvat sau, în cazul transferurilor menţionate la articolul 46 sau 47 sau la articolul 49 alineatul (1) al doilea paragraf din Regulamentul general privind protecţia datelor, o trimitere la garanţiile adecvate sau corespunzătoare şi la mijloacele de a obţine o copie a acestora, în cazul în care acestea au fost puse la dispoziţie.

(2) În plus faţă de informaţiile menţionate la alineatul (1), în momentul în care datele cu caracter personal sunt obţinute, societatea furnizează persoanei vizate următoarele informaţii suplimentare necesare pentru a asigura o prelucrare echitabilă şi transparentă:

a. perioada pentru care vor fi stocate datele cu caracter personal sau, dacă acest lucru nu este posibil, criteriile utilizate pentru a stabili această perioadă;
b. existenţa dreptului de a solicita societăţii, în ceea ce priveşte datele cu caracter personal referitoare la persoana vizată, accesul la acestea, rectificarea sau ştergerea acestora sau restricţionarea prelucrării sau a dreptului de a se opune prelucrării, precum şi a dreptului la portabilitatea datelor;
c. atunci când prelucrarea se bazează pe articolul 6 alineatul (1) litera (a) sau pe articolul 9 alineatul (2) litera (a) din Regulamentul general privind protecţia datelor, existenţa dreptului de a retrage consimţământul în orice moment, fără a afecta legalitatea prelucrării efectuate pe baza consimţământului înainte de retragerea acestuia;
d. dreptul de a depune o plângere în faţa unei autorităţi de supraveghere;
e. dacă furnizarea de date cu caracter personal reprezintă o obligaţie legală sau contractuală sau o obligaţie necesară pentru încheierea unui contract, precum şi dacă persoana vizată este obligată să furnizeze aceste date cu caracter personal şi care sunt eventualele consecinţe ale nerespectării acestei obligaţii;

f. existenţa unui proces decizional automatizat incluzând crearea de profiluri, precum şi, cel puţin în cazurile respective, informaţii pertinente privind logica utilizată şi privind importanţa şi consecinţele preconizate ale unei astfel de prelucrări pentru persoana vizată.

(3) În cazul în care societatea intenţionează să prelucreze ulterior datele cu caracter personal într-un alt scop decât cel pentru care acestea au fost colectate, societatea furnizează persoanei vizate, înainte de această prelucrare ulterioară, informaţii privind scopul secundar respectiv şi orice informaţii suplimentare relevante, în conformitate cu alineatul (2).

(4) Alineatele (1), (2) şi (3) nu se aplică dacă şi în măsura în care persoana vizată deţine deja informaţiile respective.

Art.5.(1) Datele şi informaţiile solicitate de la clienţi şi furnizate de aceştia în vederea completării contractelor şi a cererilor de deschidere de cont sunt date cu caracter personal, care servesc exclusiv la cunoaşterea clientului în vederea creării profilului investiţional, estimării duratei investirii şi a riscului aferent investiţiei în instrumente financiare.

(2) Colectarea datelor personale se face cu acceptul clientului care furnizează informaţiile respective. În cazul refuzului furnizării de informaţii relevante de către client, agentul de servicii de investiţii financiare îl va avertiza despre imposibilitatea creării profilului investiţional şi că nu i se vor putea face recomandări cu privire la vânzarea/cumpărarea de instrumente financiare.

(3) Obligaţia păstrării confidenţialităţii tuturor datelor furnizate de clienţi revine fiecărui angajat care are acces, fie şi accidental, la acestea.-

Art.6.(1) Transmiterea datelor şi a informaţiilor, precum şi punerea la dispoziţie a documentelor referitoare la clienţi şi la operaţiunile acestora pe piaţa de capital se vor putea face doar la cererea expresă din partea Autorității de Supraveghere Financiară sau a altor autorităţi abilitate de lege.

(2) În cazul în care dezvăluirea datelor este impusă de lege, societatea, prin reprezentantul legal şi/sau prin persoana care îndeoplineşte funcţia de conformitate, se va asigura că terţul care solicită dezvăluirea acţionează în conformitate cu dispoziţiile legale incidente, iar persoana vizată va fi informată în legătură cu dezvăluirea numai dacă legea permite.-

Secţiunea 2 - Sistemul informatic

Condiţii de acces în sistemele de tranzacţionare

Art.7. Accesul Societăţii la sistemul de tranzacţionare este condiţionat de existenţa personalului calificat şi autorizat să desfăşoare activitatea de tranzacţionare, relaţii cu clienţii şi evidenţa tehnico-operativă şi contabilă, precum şi de implementarea mecanismelor de supraveghere adecvate care să asigure desfăşurarea în condiţii optime a activităţii Societăţii.-

Art.8.(1) S.S.I.F. trebuie să dispună permanent de personal tehnic specializat, testat şi avizat în prealabil, în vederea utilizării în condiţii de securitate a sistemului de tranzacţionare.

(2) Condiţiile necesare cu privire la pregătirea şi testarea corespunzătoare a agenţilor de bursă sunt stabilite prin reglementările operatorului de piaţă.-

Art.9. În vederea desfăşurării activităţii curente de tranzacţionare, S.S.I.F. respectă următoarele condiţii:

a) deschide conturi de instrumente financiare prin înregistrarea corectă şi completă a tuturor elementelor de identificare a deţinătorilor de cont;

b) încadrează corect tipul de cont, în funcţie de identitatea deţinătorului, în conformitate cu prevederile legislative aplicabile, iar în cazul în care tipul de cont al deţinătorului se încadrează în mai mult de un tip de cont, se va alege tipul cu prioritatea cea mai scăzută;

c) verifică permanent corectitudinea datelor de identificare şi efectuează orice modificări necesare;

d) introduce şi execută ordinele de bursă în conformitate cu prevederile legale în vigoare.-

Art.10. Regulile referitoare la comportamentul S.S.I.F. şi agenţilor de bursă în timpul şedinţei de tranzacţionare sunt stabilite prin reglementările operatorilor de piaţă.-

Art.11. Este interzisă utilizarea sistemului de tranzacţionare al B.V.B. în mod abuziv sau într-o manieră care ar putea conduce la diminuarea artificială a performanţelor sistemului sau ar putea afecta securitatea şi siguranţa sistemului şi/sau a Participanţilor la piaţă.-

Art.12. S.S.I.F. este răspunzătoare pentru încălcarea unei reguli, indiferent dacă aceasta a fost încalcată urmărindu-se propriul interes sau interesul unui client, dacă a fost încalcată de către un angajat al Societăţii sau dacă este rezultatul direct sau indirect, cauzat cu intenţie, din greşeală, neglijenţă sau omisiune, prin acţiune sau inacţiune de către S.S.I.F. sau de către o persoană aflată în legătură cu acesta.-

Art.13.(1) Accesul S.S.I.F. sau a unui agent de bursă la sistemul de tranzacţionare poate fi retras în cazuri precum, fără a se limita:
a) aplicarea de sancţiuni bursiere sau măsuri preventive Societăţii sau agentului de bursă;
b) solicitarea Societăţii;
c) suspendarea Societăţii, în numele căreia tranzacţionează agentul de bursă.
(2) Reluarea accesului Societăţii sau agentului de bursă la sistemul de tranzacţionare se efectuează după încetarea cauzelor care au determinat retragerea, pe baza instrucţiunii Departamentelor de specialitate.-

Modul de utilizare a sistemelor de tranzacţionare

Art.14.(1) Operatorul de piaţă stabileşte un sistem de codificare a numelor de utilizator şi a Societăţii, reguli de formare şi schimbare a parolelor de acces, precum şi niveluri de acces la sistem pentru fiecare tip de utilizator din cadrul S.S.I.F.
(2) Accesul la sistemul de tranzacţionare se realizează prin staţiile de lucru conectate la sistem, situate la sediul principalsau la sediile secundare ale Societăţii.
(3) Staţiile de lucru pot fi conectate la sistemul de tranzacţionare numai cu acordul prealabil al operatorului de piaţă.
(4) S.S.I.F. are obligaţia să asigure agenţilor de bursă proprii condiţiile tehnice necesare cerute, în vederea tranzacţionării în condiţii optime.-

Art.15.(1) Societatea are asigurate soluţii de back-up pentru serviciile de comunicaţii de date cu B.V.B., pe baza unor cerințe aprobate de Consiliul Bursei.
(2) Soluţiile de back-up menţionate la alin.1 sunt realizate printr-un mediu de comunicaţie diferit fizic de cel utilizat pentru legătura principală.
(3) Accesul Societăţii la sistemul de tranzacţionare al B.V.B. este condiţionat de îndeplinirea cerinţelor prevăzute la alin.1 şi 2.-

Art.16.(1) Accesul la sistemele de tranzacţionare este permis agenţilor de bursă numai pe baza unui cod de utilizator propriu şi a unei parole confidenţiale, cunoscută numai de către acesta, care permite asigurarea protecţiei informaţiei.
(2) Fiecare agent de bursă are obligaţia să-şi modifice periodic parola de acces în sistemele de tranzacţionare în vederea creşterii gradului de siguranţă în operare. Orice altă modificare de parolă va fi solicitată expres operatorului de piaţă, în scris.-

Defecţiuni tehnice ale sistemelor de tranzacţionare

Art.17. Societatea trebuie să asigure şi să menţină, prin intermediul unei persoane desemnate în acest scop, o legătură permanentă cu Departamentul de specialitate al operatorului de piaţă, în vederea soluţionării operative a eventualelor probleme tehnice intervenite.-

Art.18. În timpul şedinţelor de tranzacţionare, asistenţa acordată de către operatorul de piaţă agenţilor de bursă include, dar nu se limitează la:
a) monitorizarea continuă a integrităţii şi performanţelor tehnice ale sistemului de tranzacţionare, detectarea erorilor potenţiale şi participarea la eliminarea erorilor detectate;
b) participarea la eliminarea erorilor raportate de către agenţii de bursă;
c) iniţierea remedierii defecţiunilor tehnice apărute în sistemul de tranzacţionare al operatorului de piaţă sau în aplicaţia-client care funcţionează pe staţia de lucru a agenţilor de bursă şi depunerea tuturor eforturilor pentru eliminarea unor astfel de defecţiuni tehnice în cel mai scurt timp posibil.-

Răspunderea referitoare la activitatea de tranzacţionare

Art.19. Societatea va fi răspunzătoare pentru repararea în întregime a oricăror prejudicii produse, în următoarele situaţii:
a) nerespectarea caracteristicilor specificate de operatorul de piaţă privind configuraţia la nivel hardware şi software a calculatoarelor S.S.I.F. care fac parte din staţiile de lucru conectate la sistemele de tranzacţionare;
b) nerespectarea instrucţiunilor de instalare, configurare şi utilizare specificate;
c) instalarea pe staţiile de lucru proprii a altor produse software care pot afecta funcţionarea sistemelor de tranzacţionare;
d) conectarea unei staţii de lucru simultan şi la alte reţele electronice.-

Art.20.(1) Nu pot fi pretinse daune-interese sau despăgubiri pentru pierderi cauzate de:
a) defecţiuni apărute în sistemele de tranzacţionare sau în sistemele de compensare-decontare;
b) întreruperea alimentării cu energie electrică, nefuncţionarea legăturii de comunicaţii cu operatorul de piaţă, datorată furnizorului de comunicaţii sau a altor defecţiuni de această natură, situaţie în care răspunderea revine furnizorului de servicii de comunicaţii;
c) orice daune directe şi/sau indirecte cauzate de sau rezultate din oprirea sistemului de tranzacţionare sau sistemului de compensare-decontare, din motive în afara controlului Societăţii;
d) situaţii de forţă majoră.
(2) În cazul opririi unuia sau mai multor simboluri de la tranzacţionare din motive datorate unor defecţiuni tehnice ale sistemului de tranzacţionare sau al sistemului de comunicaţii, nu se pot pretinde daune – interese sau despăgubiri Societăţii.-

Art.21. Accesul la informaţiile confidenţiale va fi restrâns doar la acele persoane care folosesc aceste informaţii în activitatea lor curentă, respectiv:

a. agenţii pentru servicii de investiţii financiare – vor putea accesa numai informaţiile referitoare la clienţii lor;
b. tranzacţionare – vor putea accesa numai informaţiile referitoare la Raportul de tranzacţionare şi Raportul Compensare-Decontare pentru a urmări concordanţa existentă între datele conţinute de cele 2 rapoarte (sau orice alte rapoarte de acest fel) şi ordinele de
c. bursă iniţiale introduce în sistemul de tranzacţionare;
d. contabilii – vor putea accesa doar datele privind evidenţa contabilă specifică şi generală;
e. controlul intern – va avea acces la toate informaţiile conţinute de sistemul informatic, în scopul îndeplinirii atribuţiilor ce îi revin;
f. management – va putea accesa toate informaţiile conţinute de sistemul informatic.-

Art.22. Conducerea societăţii va stabili persoanele care au acces la diferitele categorii de informaţii conţinute de sistemul informatic şi persoanele responsabile cu securitatea sistemului informatic (folosirea parolelor şi schimbarea lor periodică).-

Art.23. Departamentul de Resurse Umane are obligaţia de a proceda la încetarea contractului individual de muncă şi la anularea drepturilor acordate salariaţilor (contul de e-mail; accesul în aplicaţia informatică a Societăţii), după ce cererea de demisie a fost semnată de Preşedintele Societăţii.-

Art.24. Administratorul sistemului informatic va dezvolta soluţii de backup pentru evidenţele societăţii. Datele informatice se vor arhiva periodic, pe cel puţin două suporturi tehnice ce vor fi păstrate în locaţii diferite, pentru a putea fi recuperate în caz de dezastru.-

❖ ***Organizarea pe procese a activităţilor aferente utilizării tehnologiei informaţiei***

1. Managementul disponibilităţii

Art.25.(1) Pentru asigurarea serviciilor contractate de către clienți și a raportărilor către instituţiile abilitate, S.S.I.F. Vienna Investment Trust S.A. urmărește funcționarea sistemelor informatice utilizate și evidenţiază fiecare schimbare în vederea îmbunătățiri aspectelor legate de disponibilitatea serviciilor IT utilizate. S.S.I.F. Vienna Investment Trust S.A. are încheiat un contract cu un furnizor de soluții informatice, contract ce acoperă configurarea şi mentenanţa de echipamente de tip server, de servere, instalarea, întreținerea și punerea în functiune, după caz, a produselor de calcul din dotarea societății, oferirea serviciilor de back-up în vederea păstrării în siguranță a datelor și a informațiilor, precum și a recuperării și restaurării datelor și informațiilor în caz de dezastru.
(2) S.S.I.F. Vienna Investment Trust S.A., desemnează, prin decizie a Consiliului de Administraţie, un administrator de sistem.-

Sisteme informatice importante si sisteme informatice pentru asigurarea raportărilor către A.S.F.

Art.26. (1). S.S.I.F. Vienna Investment Trust S.A. utilizează următoarele sisteme informatice importante pentru asigurarea serviciilor contractate de către clienți

- ✓ *ISSF-Office* – aplicația este proprietatea Capital Software Romania iar S.S.I.F. Vienna Investment Trust S.A. are dreptul de utilizare. Societatea a încheiat un contract de furnizare și îmbunătățire continuă a sistemelor informatice cu furnizorul programelor.
- ✓ ArenaXT - reprezintă platforma de brokeraj dezvoltată de specialiștii B.V.B. pentru intermediari.ArenaXT client este terminalul de tranzacționare care oferă suport operațional și informațional pentru activitatea de tranzacționare. Poate fi folosită atât de către clienții care își administrează propriile investiții, cât și de către traderii care admistrează investițiile clienților lor.

ISSF-Office este sistemul informatic utilizat de majoritatea departamentelor societății, respectiv: Compartimentul Conformitate, Departamentul Front-Office, Tranzacționare, Departamentul Back-Office, Departamentul Administrare Riscuri, Departamentul Finaciar-Contabil. ISSF – Office este un sistem informatic cu arhitectură ”client-server”, componenta de tip „server” a sistemului rulează pe o stație de lucru dedicată, din dotarea Capital Software Romania. Accesul pe stațiile de lucru se face pe bază de identificator unic și parolă personală secretă, fiecare utilizator având alocate drepturi de acces corespunzătoare atribuțiilor.
Bursa de Valori București asigură siguranța, performanța, fiabilitatea sistemului de bază și funcționarea platformei ***ArenaXT,*** precum și îmbunătățirea aspectelor legate de IT. Pentru a rula platforma ArenaXT pe stațiile de lucru, S.S.I.F. VIENNA INVESTMENT TRUST S.A. asigură dotarea tehnică necesară funcționării acesteia. În vederea permiterii accesului, identificatorul unic și parola de acces sunt alocate de către B.V.B.; ulterior, în cadrul primei sesiuni de autentificare, pentru asigurarea confidențialității și protejarea datelor introduse în platformă, societatea modifică parola. Societatea deține acces controlat atât pentru brokeri, cât și pentru clienții autorizați să utilizeze platforma ARENA XT, pe bază de identificator unic și parolă personală secretă și drepturi de acces corespunzătoare.
(2) S.S.I.F. Vienna Investment Trust S.A. utilizează următoarele sisteme informatice pentru asigurarea raportărilor către A.S.F.:

ReSe3 este un sistem informatic cu arhitectură ”client-server”. Componenta de tip „server” a sistemului rulează pe o stație de lucru dedicată, din dotarea A.S.F. Pentru a transmite documentele elaborate în conformitate cu reglementările în vigoare şi în formatele compatibile sistemului, S.S.I.F. Vienna Investment Trust S.A. se conectează la acesta prin intermediul aplicației „Raportări Piața Capital Client”, care este componentă de tip ”client” a sistemului. Societatea are instalată aplicația „Raportări Piața Capital Client” pe stația de lucru și asigură dotarea tehnică necesară funcționării aplicației. Instalarea aplicației se face de pe website-ul A.S.F. Programul este funcțional pe stațiile de lucru doar împreună cu JavaScript. A.S.F. asigură siguranța, performanța, fiabilitatea sistemului de bază și funcționarea programului.
Sistemul de raportare electronică SIR este un sistem informatic cu arhitectură „client-server” și interfață de tip web. Pentru a transmite documentele elaborate în conformitate cu reglementările în vigoare şi în formatele compatibile sistemului, societatea se conectează la acesta prin intermediul internetului, prin accesarea locului dedicat: *http://gw-cnvm.cnvmr.ro:11001/ews/participants/securitate/users/Login.do.*
Identificatorul unic și parola de acces în vederea permiterii accesului în programele SIR și ReSe3 au fost alocate de C.N.V.M./A.S.F.; ulterior, în cadrul primei sesiuni de autentificare, pentru asigurarea confidențialității și protejarea datelor introduse în sistem, societatea a modificat parola. A.S.F. asigură siguranța, performanța, fiabilitatea sistemului de bază și funcționarea programului .

2. Managementul utilizatorilor

Art.27. Utilizatorii sistemelor informatice sunt instruiţi individual cu privire la utilizarea sistemelor. Instruirea se face luând în considerare responsabilităţile specifice fiecărui utilizator.-

Art.28. Persoanele nou angajate vor fi obligatoriu instruite cu privire la utilizarea sistemelor informatice în momentul angajării. Angajații vor semna un document prin care să se confirme faptul că au luat la cunoştinţă politica de securitate a entității.-

Art.29. S.S.I.F. Vienna Investment Trust S.A. va instrui toţi utilizatorii sistemelor nou introduse pentru a garanta faptul că acestea vor fi folosite eficient şi că nu vor compromite securitatea informatică.-

Art.30. Fiecare utilizator are un identificator unic şi o parolă personală secretă pentru accesul la sistemele/programele informatice ale societății.-

Art.31.(1) Privilegiile acordate utilizatorilor sunt revizuite periodic pentru a determina dacă acestea continuă să fie necesare pentru ca utilizatorul să îşi poată îndeplini sarcinile ce îi revin.
(2) În cazul în care, în urma revizuirii menţionate la alin.(1), se constată că privilegiile acordate nu îi mai sunt necesare în îndeplinirea atribuţiilor, aceste privilegii vor fi revocate imediat.
(3) Toate privilegiile de acces la sistemele informatice sunt revocate imediat în momentul în care un angajat îşi încetează activitatea în cadrul companiei.
(4) S.S.I.F. Vienna Investment Trust S.A. dispune de mecanisme adecvate privind gestionarea adecvată a accesului la sistemele/programele informatice importante:

- ✓ Principalele sisteme/programe informatice (ArenaXT,*ISSF-Office)* sunt utilizate numai pe bază de identificator unic, parolă personală secretă și drepturi de acces. Pentru programele informatice ReSe3 și SIR la care au acces mai mulți utilizatori în baza aceluiași identificator unic și parolă secretă, societatea dispune de o politică de control a accesului (lista de control a accesului)
- ✓ Controlul accesului la aplicații este configurat astfel încât să minimalizeze riscurile cu privire la securitatea informației și să permită desfășurarea în bune condiții a activităților din cadrul societății.
- ✓ Utilizatorilor li se permite accesul numai la comenziile și funcțiile din sistem pe care au dreptul să le folosească.

- ✓ Accesul la anumite informații considerate cu caracter personal este permis numai angajaților care au nevoie de aceste informaţii în îndeplinirea sarcinilor ce le revin;
- ✓ Pentru accesarea sistemul de operare se va utiliza o parolă de utilizator (user) cu drepturi suficiente pentru îndeplinirea obligațiilor. ;
- ✓ Interzicerea folosirii de către utilizatori a programelor software care provin din surse externe sau dubioase;
- ✓ Informarea utilizatorilor în privinţa pericolului privind viruşii informatici;
- ✓ Implementarea unor sisteme automate de devirusare şi de securitate a sistemelor informatice;
- ✓ Dezactivarea tastei "Print screen", atunci când este necesar sau doar atunci când sunt afişate pe monitor date cu caracter personal/date confidențiale/informații confidențiale, interzicându-se astfel scoaterea la imprimantă a acestora.-

3. Managementul incidentelor

Art.32. Obiectivul S.S.I.F. Vienna Investment Trust S.A. în managementul incidentelor este acela de a asigura reînceperea furnizării serviciilor/programelor informatice IT către utilizatorii finali în cel mai scurt timp posibil în cazul unei întreruperi a furnizării normale a acestor servicii. Procesul se bazează pe identificarea și monitorizarea incidentelor apărute, astfel încât să se evite apariția acestora sau să se atenueze efectul incidentului.-

Art.33. Pentru a preveni incidentele legate de buna funcționare a activității personalului, a sistemelor informatice și de comunicaţii, a asigurării serviciilor către clienți precum și a raportărilor către A.S.F., S.S.I.F. Vienna Investment Trust S.A. a implementat un proces de management al incidentelor astfel:

- ✓ Blocarea şi filtrarea accesului la resurse în funcţie de necesităţi:
- ✓ Conştientizarea aspectelor legate de securitate de către utilizatori:
- ✓ Detectarea în timp util a incidentelor de securitate pentru atenuarea efectelor lor pentru a reduce riscul şi costul asociat:
- ✓ Protectia accesului la rețea cu aplicații Firewall:
- ✓ Monitorizarea accesului în încăperi, la servere, în reţea, la documente, fișiere și la medii de stocare:
- ✓ Accesul cu mijloace informatice şi de înregistrare audio video numai autorizat, în caz contrar predarea lor:
- ✓ Protecţia accesului pe staţii şi servere pe bază de identificare, parola şi drepturi de acces;
- ✓ Protecţia accesului la fişiere, pe bază de identificare, parolă şi drepturi de acces, unde este cazul:
- ✓ Protecţia accesului la sistemele informatice utilizate, pe bază de identificare, parolă şi drepturi de acces:
- ✓ Acces controlat la reţea şi utilizarea exclusivă în scopuri profesionale a serviciilor email şi internet;
- ✓ Acces controlat pentru clienţii autorizaţi să utilizeze platforma ArenaXT.
- ✓ Acces controlat pentru lucrul la distanţă.
- ✓ Dezactivarea unităţile de floppy-disc, USB, CD-writer sau alt dispozitiv de ieşire pentru a împiedica copierea datelor, acolo unde este necesar;
- ✓ Monitorizarea accesărilor.-

Art.34. Activităţile din cadrul acestui proces includ identificarea problemelor, găsirea soluţiilor pentru rezolvarea problemelor, implementarea controlată a schimbărilor necesare în cadrul infrastructurii şi apoi verificarea rezolvării problemei.

S.S.I.F. VIENNA INVESTMENT TRUST S.A. nu permite:

- ✓ acces neautorizat şi transfer de date, indiferent de gradul de confidenţialitate;
- ✓ modificarea, ştergerea sau deteriorarea datelor;
- ✓ perturbarea sistemelor informatice;
- ✓ producerea, vânzarea, procurarea pentru utilizare şi distribuţie fără drept a dispozitivelor care pot perturba grav sistemele informatice;
- ✓ interceptarea parolelor şi a codurilor de acces în scopul sabotării sistemelor şi reţelelor de calculatoare;
- ✓ falsificarea datelor cu intenţia de a fi folosite ulterior ca date autentice;
- ✓ înşelătorii sau fraude comise prin intermediul computerelor;
- ✓ utilizarea neautorizată a programelor.-

4. Managementul schimbării

Art.35. Managementul schimbării este procesul responsabil cu controlul ciclului de viață al tuturor schimbărilor pentru a permite implementarea schimbărilor benefice cu minimum de întrerupere a serviciilor IT.-

Art.36.(1) Pentru asigurarea trasabilității, transparenței, documentării și evidenței, a reducerii erorilor și fraudelor, S.S.I.F. Vienna Investment Trust S.A. va urmări şi evidenţia fiecare schimbare în vederea asigurării controlului asupra implementării modificărilor/schimbărilor solicitate de planurile de afaceri și operaționale, la nivelul companiei, al personalului, al proceselor, al sistemelor, al serviciilor IT și al operării cu furnizorii externi.
(2) Structura de conducere din cadrul S.S.I.F. Vienna Investment Trust S.A. este responsabilă cu managementul schimbării în vederea asigurării controlului asupra implementării modificărilor/schimbărilor solicitate de planurile de afaceri și operaționale, la nivelul companiei, al personalului, al proceselor, al sistemelor, al serviciilor IT și al operării cu furnizorii externi.-

a. Ciclul de viaţă al programelor informatice

Art.37.(1) Societatea nu dezvoltă programe informatice proprii, astfel încât nu se impune implementarea unui proces documentat de dezvoltare software a programului informatic, de promovare, suport după implementare și primire de noi cerințe pentru modificarea celor inițiale după ce acestea vor fi puse în funcțiune.
(2) Societatea va colecta, doar atunci când va fi cazul, cerințele de afaceri, de analiză a acestora, de redactare a specificațiilor de afaceri și tehnice, de alocare a resurselor și de primire de noi cerințe pentru modificarea celor inițiale.
(3) Societatea va menține un nivel cât mai dezvoltat al sistemelor informatice utilizate în relația cu clienții. În cazul în care se constată că sistemele informatice existente nu mai corespund cerințelor societății, se va proceda la înlocuirea acestora.-

b. Managementul versiunilor

Art.38.(1) S.S.I.F. Vienna Investment Trust S.A. păstrează un istoric cu privire la procesul de versionare a aplicaţiilor/sistemelor importante pe care le utilizează, în scopul gestionării riscurilor operaţionale generate de sistemele informatice utilizate, pe toată perioada de utilizare a aplicației/sistemului.
În acest sens:

- o fiecare versiune a unui program informatic va primi un cod unic;
- o testele de acceptanță sunt finalizate şi semnate de utilizatorii de test și de utilizatorii finali, acolo unde va fi cazul;
- o toate versiunile se vor aduce la cunoștiința managementului înaintea implementării.

(2) Sistemele informatice utilizate de societate sunt achizitionate pe baza de licență, societatea având dreptul de a utiliza sistemele informatice. Dezvoltatorii progamelor informatice asigură siguranța, performanța, fiabilitatea sistemelor de bază și funcționarea acestora, precum și îmbunătățirea aspectelor legate de IT.
(3) Departamentul de IT împreună cu angajații S.S.I.F. testează programele utilizate înainte de implementare. După finalizarea testelor, se va întocmi un raport ce va fi adus la cunoştinţa Structurii de conducere a societații. Dacă programele informatice corespund cerințelor societății, se va proceda laaprobarea implementări programelor informatice testate.-

c. Managementul testării şi asigurării calităţii programelor informatice

Art.39.(1) Societatea va testa sistemele/programele informatice importante înainte de prima utilizare și la orice modificare în cadrul cicului de viata al acestora, utilizând resurse umane și tehnice interne sau externe entităţii.
(2) Testarea se efectuează în baza prezentei proceduri,a instruiri efectuate angajaților precum și în baza unui scenariu formalizat de testare, prin care să se asigure că testarea răspunde cerinţelor impuse de managementul securităţii.
(3) Rezultatul testărilor prevăzute la alin.(1) se consemnează într-un raport de testare IT care va cuprinde cel puțin următoarele elemente:

- Scopul testării.
- Perioda testării.
- Descrierea programului testat.
- Identificarea aplicațiilor utilizate și a persoanelor implicate.
- Analiza riscurilor implicate de achizţtia sau modificarea programului informatic important, a posibilelor vulnerabilități și a măsurilor de reducere a riscurilor asociate prin controale de sistem sau de program informatic.
- Descrierea modului prin care s-au efectuat testele, scenariile de test, eventualele norme sau standarde aplicate și rezultatul testării.
- Concluzia echipei de testare.
- Semnătura membrilor echipei de testare.

(4) Rapoartele de testare IT se păstrează în cadrul societății cel puţin până la următoarea auditare IT și vor fi puse la dispoziția auditorului IT și A.S.F. la cerere. -

5. Managementul capacităţii

Art.40.(1) Managementul capacității ține cont de toate resursele necesare livrării unui serviciu IT și urmărește îndeplinirea nevoilor curente și viitoare legate de capacitatea și performanța societății.
(2) În vederea asigurării performanței, scalabilității și a capacității serviciilor IT asigurate de infrastructura informatică pentru prevenirea afectării parțiale sau totale a capacității de procesare, stocare sau furnizare a serviciilor către clienții si către A.S.F., managementul capacității implementat la nivel de societate include două subprocese:

a) *Managementul capacităţii serviciilor* – Societatea se asigură că programele informatice sunt licențiate și corespund cerințelor. Departamentul IT se asigură că sistemele informatice utilizate sunt updatate la zi, astfel încât să prevină afectarea parțială sau totală a capacității de procesare, stocare sau furnizare a serviciilor către clienții şi către A.S.F.

b*) Managementul capacității componentelor* - Societatea se asigură că stațiile de lucru (hardware şi software) și serverele îndeplinesc cerințele minime de sistem și configurația de bază astfel încât serviciile furnizate să nu fie întrerupte.

(3) Societatea monitorizează permanent componentele infrastructurii, inclusiv aplicaţii, servicii, sisteme de operare, protocoale de reţea, valori, sisteme și infrastructură de rețea, spațiu disc utilizat, lărgime bandă, pentru a preveni afectarea parțială sau totală a capacității de procesare, stocare sau furnizare a serviciilor către clienți sau a raportărilor către ASF.

(4) Toţi acești parametri sunt înregistrați și stocati astfel încât să furnizeze o imagine completă asupra tuturor proceselor. Programul utilizat transmite alerte, furnizând informațiile necesare pentru a se proceda imediat la rezolvarea problemelor. Acesta furnizează grafice automate pentru planificare și tendințe care permit societății să planifice înlocuirea componentelor din infrastuctură, înainte ca acestea să devină prea vechi, pentru a fi folositoare.-

6. Managementul configuraţiilor

Art.41 (1) Managementul configuraţiilor ţine evidenţa tuturor elementelor de configuraţie necesare în vederea furnizării Serviciilor IT. Elementele de configuraţie includ software, hardware, acorduri de furnizare a serviciilor (SLA), planuri de disaster recovery, politici etc.
(2) Societatea se asigură şi menţine configuraţii corespunzătoare ale staţiilor de lucru, astfel încât sistemele/ programele informatice importante să ruleze fără probleme.
(3) S.S.I.F. Vienna Investment Trust S.A. utilizează software-uri sub licență, acestea reînnoindu-se anual. În momentul în care societatea va constata deficiențe repetate în rularea unui soft, acesta va fi înlocuit, astfel încât să se prevină afectarea parțială sau totală a capacității de furnizare a serviciilor către clienți sau a raportărilor către ASF.
(4) Elementele de configurație (configurația hardware) sunt înlocuite atunci când specialiști departamentului IT decid acest lucru.
(5) S.S.I.F Vienna Inveatment Trust S.A. deține o procedură distinctă privind planurile de recuperare în caz de dezastru.-

7. Managementul nivelurilor de servicii

Art.42.(1) Societatea identifică și aplică măsuri de securitate cu privire la gestionarea accesului furnizorilor la mijloacele de procesare a datelor şi a informaţiilor pentru fiecare caz în parte.
(2) Societatea va agrea nivelurile de servicii aferente furnizorilor de servicii externalizate cu fiecare furnizor în parte, în funcţie de specificul şi obiectul acordului de servicii.
(3) S.S.I.F. Vienna Investment Trust S.A. încheie contracte cu furnizorii de servicii externalizate, contracte ce vor conţine cel puțin următoarele:

- ✓ Responsabilități si obligații legale;
- ✓ Cerințe de securitate și/sau măsuri interne de securitate;
- ✓ Responsabilității și obligații aferente accesării, procesării sau gestionării infomațiilor entității și a facilităților sale de procesare a datelor;
- ✓ Responsabilității și obligații de planificare a perioadei de tranziție și rezolvarea problemelor potențiale ale întreruperii operațiunilor pe parcursul acestei perioade;
- ✓ Planificări pentru situații neprevăzute;
- ✓ informații și monitorizare a incidentelor de securitate și managementul acestora;
- ✓ Planificarea și gestionarea tranziției spre un acord de servicii IT externalizate și aplică procese adecvate pentru managementul schimbării și renegocierea/rezilierea acordurilor.

(4) S.S.I.F. Vienna Investment Trust S.A. a încheiat contracte de furnizare servicii cu furnizori externi cu bună reputaţie, clauzele contractuale şi durata contractelor nepermiţând întreruperi fără preaviz. În cazuri excepţionale, compania este în permanent contact cu piaţa şi poate contracta serviciile unui alt furnizor existent.
(5) Departamentul de IT (serviciu externalizat) asigură backup-ul societății prin fiabilitate și performanță garantată de SLA (Service Level Agreement) 99,9%.-

8. Managementul securităţii

a. Cerinţe generale

Art.43. Raportat la activitatea desfășurată, S.S.I.F. Vienna Investment Trust S.A. se asigură că sistemele informatice utilizate îndeplinesc cel puțin următoarele cerințe:

- ✓ asigură integritatea, confidențialitatea, autenticitatea, disponibilitatea datelor în concordanță cu categoria de risc a sistemului informatic definită intern de către entitate, precum și prelucrarea acestora în conformitate cu reglementările A.S.F., luând în considerare posibilitatea actualizării acestora, în funcție de modificările intervenite în legislația incidentă;
- ✓ asigură respectarea conținutului de informații prevăzut în formularele de raportare corespunzătoare entităților, așa cum sunt prevăzute în legislația specifică, precum și alte raportări solicitate prin reglementările A.S.F.;
- ✓ asigură reconstituirea rapoartelor și informațiilor supuse verificării;
- ✓ asigură stocarea și păstrarea datelor înregistrate și jurnalizate de către sistemele de tranzacționare și back-office pentru o perioadă de timp în conformitate cu legislația aplicabilă în vigoare. Sistemul de păstrare a datelor trebuie să asigure posibilitatea ca aceste date să poată fi transmise sau puse la dispoziția A.S.F. la cerere;
- ✓ asigură posibilitatea de restaurare a datelor arhivate pe suport digital extern, precum, dar fără a se limita la, informații, date introduse, situații financiare sau alte documente;
- ✓ asigură elemente de identificare a datelor supuse prelucrării sau verificării. Sistemele informatice asigură identificarea exactă a timpului la care au fost efectuate înregistrările și identificarea utilizatorilor sistemului la acel moment;
- ✓ asigură confidențialitatea și protecția informațiilor și a programelor prin parole, coduri de identificare pentru accesul la informații, precum și realizarea de copii de siguranță pentru programele și informațiile deținute;
- ✓ asigură mecanisme de securitate și control al sistemelor informatice, pentru păstrarea în siguranță a datelor și informațiilor stocate, a fișierelor și bazelor de date, inclusiv în situația unor evenimente de risc.-

Art.44. Sistemele informatice care oferă accesul la platforme electronice de tranzacționare, precum și cele care evidențiază operațiuni de compensare, decontare și registru pentru instrumente financiare și operațiuni cu aceste instrumente, asigură cel puțin, fără a se limita la:

- ✓ securitatea și integritatea datelor procesate prin folosirea unei modalități de securizare, atât asupra datelor trimise către platformele electronice de tranzacționare și către cele de compensare, decontare și registru, cât și asupra datelor recepționate de la aceste sisteme;
- ✓ mecanisme care să garanteze nerepudierea datelor transmise și recepționate;
- ✓ jurnalizarea în timp real a informației despre ordinele transmise spre executare, a stării acestor ordine, respectiv a modificărilor care se aduc acestor ordine în decursul existenței lor de către clienții și intermediarii care utilizează aceste sisteme informatice;
- ✓ mecanisme de nerepudiere a integrității înregistrării operațiunilor de sistem informatic.-

Art.45. S.S.I.F. Vienna Investment Trust S.A. urmăreşte:

- ✓ păstrarea la sediul propriu a documentaţiei complete și actualizate, pe fiecare nivel de acces, a programelor informatice utilizate;
- ✓ respectarea oricăror altor cerinţe care rezultă din dispoziţiile legale în vigoare, aplicabile în funcţie de obiectul de activitate al entităţii.-

b. Teste de penetrare

Art.46.(1) S.S.I.F. Vienna Investment Trust S.A. adoptă în permanenţă măsuri pentru implementarea proceselor de testare a posibilității de penetrare a sistemelor, cel puțin din exteriorul entității, la nivel de program informatic, sisteme de operare, baze de date, rețea.

(2) Procesul implică o evaluare activă a sistemului pentru a descoperi punctele slabe care l-ar putea afecta. Nu numai că vor fi identificate punctele slabe, ci, de asemenea, le vom exploata pentru a determina riscul real ce l-ar putea ridica o ameninţare pentru societate.

(3) La încheierea testării, se va genera un raport cuprinzător ce va descrie în detaliu problemele de securitate găsite în timpul testării, inclusiv impactul acestora și riscul pentru societate. Pentru fiecare neconformitate de securitate cuprinsă în raport, se va da o explicație detaliată a acțiunilor de atenuare și recomandări sunt sugerate, iar, acolo unde este posibil, va fiidentificată cauza principală a neconformității și se vor face recomandări la nivel operaţional şi de politică.-

9. Managementul continuităţii

Art.47.(1) S.S.I.F. Vienna Investment Trust S.A. asigură replicarea datelor și a sistemelor informatice importante. Pentru sistemele informatice importante, societatea urmăreşte să asigure:

- o disponibilitate ridicată, corelată cu natura, dimensiunea și complexitatea activității, la sediul principal de procesare a entităţii (propriu sau externalizat);
- un sistem de recuperare în caz de dezastru situat fie într-o altă locaţie a entităţii, fie prin intermediul unui furnizor extern de servicii, care să minimizeze riscul de dezastru natural;
- furnizorii externi de servicii respectă cerințele Normei A.S.F. nr. 6/2015.

(2) S.S.I.F. Vienna Investment Trust S.A. a încheiat contracte de furnizare servicii informatice, clauzele contractuale şi durata contractelor nu permit întreruperi fără preaviz. În cazuri excepţionale, compania este în permanent contact cu piaţa şi poate contracta serviciile unui alt furnizor existent.-

Art.48. Funcţionarea planurilor alternative de recuperare și continuitate a afacerii se testează periodic pe baza unor scenarii practice și reale, cu asigurarea posibilității continuării operaţiunilor pe sistemele de rezervă.-

Art.49. S.S.I.F. Vienna Investment Trust S.A. își continuă activitatea în caz de avarie sau dezastru, prin intermediul unui centru de recuperare cu reluarea activității într-un interval de timp optim.

Art.50. Societatea urmărește următoarele caracteristici ale centrului de date și ale planului de recuperare:

- este permanent operațional, pe perioada de definire a serviciilor (număr zile pe săptămână, număr ore pe zi) și asigură serviciile IT susținute de sistemele informatice importante și definite în planul de recuperare, în intervalul de timp optim, respectiv două zile;
- este sincronizat cu sistemul principal pentru a se asigura același nivel sau un nivel de servicii cu o scădere acceptabilă de servicii pentru serviciile replicate;
- asigură comutarea și continuarea activității, în intervalul de timp optim.-

Art.51. S.S.I.F. Vienna Investment Trust se încadrează în categoria “risc important”, intervalul de timp optim pentru reluarea activității fiind de două zile.-

❖ **Crearea şi Utilizarea Copiilor de Siguranţă (Back-up)**

Art.52.(1). În vederea păstrării în siguranță a datelor și a informațiilor, SSIF asigură două sisteme de back-up, în două locații diferite. În acest sens, SSIF dispune de server de back-up dedicat care asigură salvarea în timp real a datelor și a informațiilor.

(2) Un server de back-up este situat la sediul autorizat al Societății, locație unde este situat rack-ul cu echipamente de rețea. Serverul local al societății este dotat cu două hardiskuri configurate în mirroring pentru protecția datelor și surse rendundante de alimentare, astfel se previne pierderea datelor în cazul în care unul dintre cele două hardiskuri se defectează.

(3) Un alt server de back-up este situat într- un DATA CENTER, locație specializată în stocarea informațiilor.

(4) Informațiile și datele se salvează în timp real pe serverul local, iar la intervale regulate acestea sunt replicate în Data Center.

(5) În cazul în care baza de date a sistemelor informatice importante se alterează acestea pot fi restabilitate la o dată anterioară. Societatea păstrează toate datele si informațiile stocate.

(6) S.S.I.F. Vienna Investment Trust S.A. asigură replicarea următoarelor date fară a se limita la acestea:
- baza de date a sistemul de back-office.
- documentele și fișiere după stațiile de lucru;
- e-mail;
- site.

(7) În cadrul Societății, există o persoană responsabilă cu efectuarea back-up-ului care va efectua și testarea restaurării acestuia, respectiv Fulea Lucian Ioan asistat de un angajat din cadrul departamentului IT.-

Puncte de control şi măsurare

Art.53. S.S.I.F. Vienna Investment Trust S.A. efectuează, ca urmare a evaluărilor proprii și ori de câte ori este cazul, controale preventive, controale corective şi controale de avertizare.-

Art.54.(1) Societatea controlează riscurile generate de utilizarea sistemelor informatice prin:

a) Stabilirea de obiective de control astfel:

- *Controale preventive* - Depistează problemele înainte ca acestea să apară • Monitorizează atât operaţiunile cât şi resursele • Încearcă să prezică problemele potenţiale, înainte ca acestea să apară şi să facă ajustări • Previn apariţia unei erori, omisiuni sau vreunui act maliţios • Blochează încercările de violare a politici de securitate.
- *Controale corective* - Minimizează impactul unei ameninţări • Rezolvă problemele descoperite de controalele detective • Este identificată cauza problemei • Corectează erorile apărute • Modifică sistemele de procesare pentru a minimaliza apariţia problemei pe viitor.
- *Controale de avertizare (detective):* - Utilizează controale care depistează şi raportează apariţia unei erori, omisiuni sau vreunui act maliţios • Avertizează asupra violărilor sau încercărilor de violare a politicii de securitate şi includ controale cum ar fi audit, metode pentru detectarea intruziunilor, etc .

b) Implementarea de puncte de control

După evaluarea si verificarea sistemelor informatice în baza estimărilor riscurilor inerente şi de control, inclusiv a obiectivelor de control, Departamentul IT înregistrează în mod detaliat toate informațiile pentru a servi drept indicatoare puncte de control.

c) Monitorizarea punctelor de control și a indicatorilor cheie de risc

(2) În scopul prevederilor alin. (1), se efectuează atât controale generale la nivelul sistemului informatic, cât şi controale specifice la nivelul fiecărei componente a acestuia, după caz. Informaţiile din punctele de control sunt colectate periodic la alegerea societăţii sau când este cazul și vor fi păstrate la dispoziţia S.S.I.F. Vienna Investment Trust S.A. și raportate către A.S.F. pe baza cerințelor de raportare.-

Art.55. S.S.I.F. Vienna Investment Trust S.A. aplică proceduri operaționale în domeniul combaterii spălării banilor și finanțării terorismului, precum și regimului de sancțiuni internaționale ca parte integrată a reglementărilor emise de A.S.F.-

1. Controale generale

Art.56. Controalele generale la nivelul societăţii sau al furnizorilor externi de servicii sunt proiectate astfel încât informaţiile financiare generate de sistemele informatice ale entității să fie de încredere, reale și corecte.

Controalele generale includ:

a) *Controale referitoare la sincronizarea de timp la o referință recunoscută naţional sau internaţional*;
b) *Controale asupra operării centrului de date* - Centrul de date este serviciu externalizat, acesta va fi monitorizat îndeaproape de Departamentul IT. Departamentul IT va controla operativitatea centrului de date ocazional sau ori de câte ori se impune acest lucru, astfel încât să se asigure de continuitatea procesării datelor.
c) *Controale asupra sistemelor de aplicaţii* - Departamentul IT verifică sistemele de aplicații frecvent.

d) *Controale asupra securității accesului* – Departamentul IT verifică dacă accesul la sistemele informatice se face prin acele niveluri de securitate descrise mai sus în cadrul Managementului utilizatorilor.
e) Societatea menține controale asupra *administrării și întreținerii programelor informatice* existente pe **stațiile de lucru**, astfel încât acestea să corespundă cerințelor dezvoltatorului de software, programele informatice să funcționeze corespunzător și activitatea zilnică să nu fie întreruptă.-

2. Controale programe informatice

Art.57.(1) S.S.I.F Vienna Investment Trust S.A. are implementat un proces de verificare manuală a modului de procesare a tranzacţiilor şi a operaţiunilor efectuate prin intermediul platformei ArenaXT, precum și a sistemului informatic I.S.S.F. Office şi I.S.S.F. Derivate.
(2) Societatea reconciliază zilnic soldurile și instrumentele financiare ale clienților evidențiate în sistemele proprii.-

Art.58. Ținând cont de exigenţa limitării riscurilor şi a fraudei, S.S.I.F Vienna Investment Trust S.A. a limitat accesul la diverse medii, efectuează controale cu privire la *operarea sistemelor informatice,* limitând accesul persoanelor neautorizate la informații.-

Art.59. S.S.I.F. Vienna Investment Trust S.A. asigură siguranţa fizică a sistemelor hardware, software şi a bazelor de date, pentru prevenirea utilizării necorespunzătoare a informaţiei de către personalul entității în vederea obţinerii unor beneficii personale sau prejudicierea reputaţiei societăţii.-

3. Controale de flux financiar

Art.60.(1) Societatea evidenţiază distinct, în contabilitate, sumele primite de la clienţi şi utilizează în banca de decontare un cont în nume propriu şi un cont în numele clienţilor. De asemenea, instrumentele financiare ale clienţilor sunt evidenţiate în conturi separate de cele ale S.S.I.F.
(2) Societate nu va acţiona astfel încât să pericliteze, să poată fi considerat că periclitează sau să inducă o situaţie care poate să prejudicieze fondurile şi/sau instrumentele financiare ale clienţilor ori piaţa reglementată pe care tranzacţionează şi se va asigura că agenţii pentru servicii de investiţii financiare şi ceilalţi angajaţi ai săi nu se vor comporta în acest mod.
(3) Societatea respectă, în toate situaţiile, următoarele:
a) asigură păstrarea în siguranţă a instrumentelor financiare pe care le ţine în custodie;
b) nu face uz de nici unul din instrumentele financiare pe care le ţine în custodie sau de drepturile ce decurg din acestea şi nu transferă aceste instrumente financiare fără acordul expres al deţinătorilor;
c) returnează clienţilor, la solicitarea acestora, instrumentele financiare şi fondurile băneşti încredinţate.
(4) Societatea transferă la sfârşitul fiecărei zile de decontare din contul/conturile în care se află fondurile băneşti aparţinând clienţilor în contul propriu, sumele aferente comisioanelor ce i se cuvin.
(5) Societatea utilizează pentru sistemul de back-office o aplicaţie software care evidenţiază zilnic în subconturile individuale ale clienţilor atât identitatea fiecărui client, cât şi deţinerile acestuia (sold și/sau instrumente financiare).
(6) Niciun transfer între contul House și contul global de clienți sau între subconturile individuale ale clienților din cadrul contului global evidențiat în sistemul propriu de back-office al Societății – participantă la sistemul Depozitarului Central, nu poate avea loc în lipsa unei tranzacții, cu excepția operațiunilor de împrumut de valori mobiliare, a operațiunilor de constituire a garanțiilor financiare cu transfer de proprietate formate din valori mobiliare, a operațiunilor de însușire a garanțiilor fără transfer de proprietate constituite din valori mobiliare.-

Art.61.(1) S.S.I.F. menţine evidenţe ale înregistrărilor şi conturilor astfel încât să asigure acurateţea acestora şi, în mod distinct, corespondenţa acestora cu instrumentele financiare şi fondurile deţinute în numele clienţilor.

(2) Societatea verifică în mod regulat concordanţa dintre evidenţele, înregistrările şi registrele proprii şi cele ale oricărei terţe părţi în numele căreia sunt deţinute acele active.
(3) Societatea utilizează principiul dublei validării, potrivit căruia, pentru fiecare operaţiune de creditare/debitare a contului beneficiarului, există o operaţiune corespondentă de debitare/creditare în contul contrapărţii care furnizează/primeşte valori mobiliare, principiu prin care se identifică în orice moment şi fără întârziere deţinerile mobiliare ale unui client propriu.
(4) Societatea realizarea zilnic o verificare internă a evidențelor proprii, care să certifice faptul că deținerile financiare ale clienților proprii corespund realității.
(5) Societatea efectuează zilnic o reconciliere a tuturor conturilor individuale ale clienților și a contului House, respectiv a deținerilor de valori mobiliare și a sarcinilor asupra acestora, evidențiate în sistemul propriu de back-office, cu conturile globale deschise în sistemele depozitarilor centrali.-

Art.62. Societatea ține o evidență strictă, distinctă întocmită şi ţinută la zi asupra:

- apelurilor în marjă;
- notelor privind alte debite/credite ale clientilor;
- fişelor conturilor clienţilor, conturilor persoanelor relevante şi contului propriu;
- operaţiunilor referitoare la tranzacţiile cu instrumente financiare, ale intrărilor/ieşirilor de numerar şi ale altor avansuri sau debite ale clienţilor, precum şi documentele primare care au stat la baza lor. Evidenţele reflecta contul în care tranzacţia a fost efectuată, denumirea contului, instrumentul financiar tranzacţionat, cantitatea, preţul unitar şi preţul total de vânzare sau cumpărare şi data tranzacţiei;
- deţinerilor clienţilor, evidență care reflectă, în contul de numerar al fiecărui client, toate vânzările/cumpărările, primirile/livrările de instrumente financiare;
- activelor şi pasivelor, conturilor de venituri, de cheltuieli şi de capital (actualizate cel puţin lunar);
- documentelor ce reflectă, separat, fiecare instrument financiar, la data compensării, toate poziţiile pe care S.S.I.F. le deţine în conturile personale şi ale clienţilor săi, precum şi localizarea lor;
- instrumentelor financiare în curs de transfer, dividende şi dobânzi primite, împrumuturi acordate sau primite, precum şi ale instrumentelor financiare ce nu au fost primite sau nu au fost livrate, actualizate cel puţin zilnic.-

❖ ***<u>Indicatori cheie de risc – Key Risk Indicator (KRI) - aferenţi punctelor de control</u>***

Art.63. S.S.I.F. Vienna Investment Trust S.A. își defineşte apetitului la risc prin definirea unor limite la care indicatorii de risc sunt folosiți ca suport. Societatea asigură procesul de monitorizare și măsură prin indicatorii cheie de risc (KRI), identificând pierderile operaționale potențiale cauzate de deficiențele legate de IT și comunicații.-

Art.64 Societatea a stabilit un set de indicatori cheie de risc aferenți naturii, dimensiuni și complexității acesteia, respectiv:

- **Control General - Managementul Riscului de Furnizor extern.** *Obiectiv de control:* Identificarea și diminuarea riscurilor legate de capacitatea furnizorilor de a continua eficient furnizarea de servicii într-un mod sigur și eficace, în mod continuu. Contractele sunt conforme cu standardele societăţii şi cu cerințele legale. Contractele vor lua în considerare: acordurile de nedivulgare (NDAs), viabilitate, SLA, conformitate continuă a furnizorului cu cerințele de securitate, furnizorii alternativi, etc. *Puncte de Control:* 1. Identificarea și monitorizarea riscurilor de furnizor extern, în conformitate cu procesul de management al riscului stabilit de organizație. 2. Identificarea și documentarea riscurilor contractuale (și remediile) asociate cu incapacitatea tertului de a-și îndeplini obligaţiile contractuale. 3. Toate contractele sunt verificate pentru evaluarea respectării cerințelor legale.

KRI	Valoare maximală
Număr contracte servicii externe fără SLA	0
Număr de încălcări ale SLA	2
Număr de încălcări ale NDA	0
Număr contracte servicii externe IT software fără considerarea furnizorilor alternativi	2

- **Control General. Continuitatea Afacerii.** *Obiectiv de control:* Planul de continuitate a afacerii (inclusiv a planului de recuperare în caz de dezastru) trebuie testat pentru a asigura viabilitatea acestuia în cazul unor evenimente ce împiedică funcţionarea proceselor de business. *Puncte de Control:* Tratarea Planului de Continuitate se va face cel puţin anual.

KRI	Valoare minimală
Număr de Testări anuale	1

- **Control de Aplicaţie – Dubla validare.** *Obiectiv de control:* Invalidările operaţiunilor ce presupun dublă validare trebuiesc monitorizate şi analizate pentru a stabili cauza erorilor. *Puncte de Control:* Monitorizarea operaţiunilor cu dublă validare invalidate se efectuează lunar.

KRI	Valoare maximală
Număr de operaţiuni cu dublă validare ce se efectuează lunar, în care operaţiunile sunt invalidate.	10

- **Control de Flux Financiar – RoClear – ISSF.** *Obiectiv de control:* Eventualele neconcordanţe între informaţiile transmise şi cele înregistrate la nivelul sistemului Depozitarului Central vor fi analizate şi reconciliate. *Puncte de Control:* Reconcilirea zilnică a raportului din ISSF-Office cu RoClear, prin încărcarea raportului din ISSF-Office la Depozitarul Central.

KRI	Valoare maximală
Număr de reconcilieri zilnice ce au diferenţe ce necesită corectare, pe an.	10

- **Control de Flux Financiar – Arena - ISSF.** *Obiectiv de control:* Eventualele neconcordanţe între cererile de transfer de instrumente financiare transmise către societate şi cele înregistrate la nivelul sistemului Depozitarului Central şi Arena vor fi analizate şi reconciliate. *Puncte de Control:* Reconcilirea zilnică, a doua zi, a transferurilor de instrumente financiare în ISSF-Office, dacă acestea coincid cu informaţiile din Arena şi Depozitarul Central.

KRI	Valoare maximală
Număr de reconcilieri zilnice ce au diferenţe, pe an.	10

- **Control de Flux Financiar – Banca – ISSF-Office Contabilitate.** *Obiectiv de control:* Eventualele neconcordanţe între transferurile financiare înregistrate la instituţia de credit (bancă) şi cele înregistrate în ISSF-Office Contabilitate vor fi analizate şi reconciliate. *Puncte de Control:* Reconcilirea zilnică a operaţiunilor zilnice din conturile bancare cu sumele înregistrate în contabilitate.

KRI	Valoare maximală
Număr de reconcilieri zilnice ce au diferenţe, exceptând tranferurile bancare ce se decontează a doua zi, pe an.	6

❖ ***Managementul Securităţii Sistemelor Informatice şi de Comunicaţii***

Art.65. S.S.I.F Vienna Investment Trust S.A. este înregistrată, conform legii, ca operator de date cu caracter personal sub nr. 6533/2007.-

Art.66. Societatea respectă prevederile Legii nr.677/2001 pentru protecţia persoanelor cu privire la prelucrarea datelor cu caracter personal şi libera circulaţie a acestor date, cu modificările şi completările ulterioare.-

Secțiunea 5

Plan de cooperare în domeniul securității rețelelor și a informației

Art.67.(1) Planul de cooperare stabileşte rolurile organizaționale, obligațiile și răspunderile în cadrul cooperării, precum și procedurile de menținere sau de restabilire a funcționalității rețelelor și a sistemelor infomatice în cazul în care acestea sunt afectate de un risc sau de un incident cibernetic cu impact semnificativ.

(2) Punerea în aplicare a prezentei proceduri implică constituirea unei **Echipe de Răspuns la incidente de urgență aferente securității informatice,** denumită pe scurt **CERT**. Lista cu persoanele implicate în CERT este detaliată în Anexa nr.2.

(3) Dacă un incident aferent securității informatice se produce, CERT va fi convocată de urgenţă, se va întruni, va colecta, analiza şi identifica circumstanţele şi starea de fapt a incidentului. Echipa CERT va proceda la restabilirea funcționării rețelelor și sistemelor informatice în cazul în care acestea sunt afectate de un eveniment sau incident cibernetic cu impact semnificativ.-

Responsabilitățile echipei CERT

Art.68.(1) Membrii Echipei CERT au funcţii şi responsabilităţi pre-definite care pot fi prioritare îndatoririlor obişnuite.

(2) Ori de câte ori un incident de securitate este suspectat sau confirmat, precum un virus, vierme, descoperirea unor activităţi suspecte, informaţii modificate etc., trebuie urmată *procedura standard pentru minimizarea riscurilor.*

(3) Administratorul de sistem este responsabil cu înştiinţarea şi coordonarea echipei CERT în vederea tratării incidentelor.

(4) Echipa CERT este responsabilă cu strângerea dovezilor fizice şi electronice ce vor face parte din documentaţia pentru tratarea incidentelor. Folosind resurse tehnice speciale, aceștia vor monitoriza nivelul daunelor şi gradul de eliminare sau atenuare a vulnerabilităţilor, acolo unde este cazul.

(5) Echipa CERT este responsabilă cu documentarea anchetei privind incidentele. Echipa CERT este responsabilă de coordonarea activităţilor de comunicare cu terţii pentru remedierea incidentelor.

(6) Echipa CERT poate contacta autoritățile competente atunci când apreciază că este vorba de o activitate ilicită de criminalitate informatică.

Conform legislației române, reprezintă fapte penale următoarele:

- Introducerea, modificarea sau ștergerea neautorizată de date informatice.
- Restricționarea accesului la aceste date ori împiedicarea în orice mod a funcționării unui sistem informatic. Efectuarea unei operațiuni de retragere de numerar, încărcare sau descărcare a unui instrument de monedă electronică ori de transfer de fonduri, prin utlizarea, fără consimțământul titularului, a unui instrument de plată electronică sau a datelor de identificare care permit utilizarea acestuia;
- Falsul informatic –introducerea, modificarea sau ștergerea, fără autorizaţie prealabilă, de date informatice ori restricționarea, fără drept, a accesului la aceste date, rezultând date necorespunzătoare adevărului;
- Accesul neautorizat la un sistem informatic;

- Interceptarea, fără mandat, a unei transmisii de date informatice ce nu este publică și care este destinată unui sistem informatic, provine dintr-un asemenea sistem sau se efectuează în cadrul unui sistem informatic;
- Interceptarea, fără drept, a unei emisii electromagnetice provenite dintr-un sistem informatic, ce conține date informatice care nu sunt publice;
- Modificarea, ștergerea sau deteriorarea de date informatice ori restricționarea accesului la aceste date, fără drept;
- Fapta de a perturba grav, fără drept, funcționarea unui sistem informatic, prin introducerea, transmiterea, modificarea, ștergerea sau deteriorarea datelor informatice sau prin restricționarea accesului la date informatice;
- Transferul neautorizat de date dintr-un sistem informatic sau mijloc de stocare a datelor informatice;
- Fapta persoanei care, fără drept, produce, importă, distribuie sau pune la dispoziție sub orice formă: (i) dispozitive sau programe informatice concepute sau adaptate în scopul comiterii uneia dintre faptele de mai sus; (ii) parole, coduri de acces sau alte asemenea date informatice care permit accesul total sau parțial la un sistem informatic, în scopul săvârșirii uneia dintre faptele de mai sus;
- Deținerea, fără drept, a unui dispozitiv, a unui program informatic, a unei parole, a unui cod de acces sau a altor date informatice similare, în scopul săvârșirii uneia dintre faptele de mai sus;
- Inclusiv tentativa la infracțiunile enumerate se pedepsește.-

Art.69.(1) Prezentul plan de cooperarea acoperă un număr limitat de scenarii în care **securitatea rețelelor și a informației pot fi compromise sau indisponibile,** astfel:

Scenariu:	**Atac Cibernetic Ramsomware server local**
Risc:	1 - Major
Probabilitate:	Scăzută
Impact:	Criptarea fișierelor/Bază de date inaccesibilă/Intreruperea activității
Incident:	Atac Ramsomware
Servicii afectate:	Server local/Stații de lucru/website/e-mail, back-up.
Echipa CERT	
Administrator de sistem: Lucian Fulea	Contactează telefonic și convoacă Echipa CERT prezentată în **Anexa 2**;
	Echipa CERT aplică procedura standard de minimizare a riscurilor.
Responsabil: Lucian Fulea West Network RCS&RDS Capital Software	WEST NETWORK: Gabriel Stanica 0751-013-799 George Dimitruc 0754-352.222 RDS&RCS: 031-400.65.00 Capital Software: 021-318.40.62 / 0747.523.513

Scenariu:	**Atac Cibernetic website**
Risc:	2 - Mediu
Probabilitate:	Scăzută
Impact:	Nefuncționare site/Compromitere date
Incident:	Atac cibernetic website
Servicii afectate:	Website
Echipa CERT	
Administrator de sistem Lucian Fulea	Contactează telefonic și convoacă Echipa CERT prezentată în **Anexa 2**;
	Echipa CERT aplică procedura standard de minimizare a riscurilor
Responsabil: Lucian Fulea West Network RCS&RDS Capital Software	WEST NETWORK: Gabriel Stanica 0751-013-799 George Dimitruc 0754-352.222 RDS&RCS: 031-400.65.00 Capital Software: 021-318.40.62 / 0747.523.513

Scenariu:	**Alterarea sau distrugerea datelor (intenționat/neintenționat)**
Risc:	3 - Minim
Probabilitate:	Medie
Impact:	Bază de date inaccesibilă /inexistentă
Incident:	Alterarea sau distrugerea datelor (intentionat/neintentionat)
Servicii afectate:	Nefuncționalitatea temporară a bazelor de date

Echipa CERT	
Administrator de sistem Lucian Fulea	Contactează telefonic și convoacă Echipa CERT prezentată în **Anexa 2**;
	Echipa CERT aplică procedura standard de minimizare a riscurilor.
Responsabil: Lucian Fulea West Network RCS&RDS Capital Software	WEST NETWORK: Gabriel Stanica 0751-013-799 George Dimitruc 0754-352.222 RDS&RCS: 031-400.65.00 Capital Software: 021-318.40.62 / 0747.523.513
Scenariu:	Nefuncționare rețea/internet
Risc:	3 - Minim
Probabilitate:	Medie
Impact:	Întreruperea temporară a activității/societatea nu poate executa ordinele clientilor
Incident:	Intrerupere in furnizarea serviciilor de date
Servicii afectate:	Arena XT/E-mail
Echipa CERT	
Administrator de sistem: Lucian Fulea	Contactează telefonic și convoacă Echipa CERT prezentată în **Anexa 2**;
	Echipa CERT aplică procedura standard de minimizare a riscurilor.
Responsabil: Lucian Fulea West Network RCS&RDS Capital Software	WEST NETWORK: Gabriel Stanica 0751-013-799 George Dimitruc 0754-352.222 RDS&RCS: 031-400.65.00 Capital Software: 021-318.40.62 / 0747.523.513

Procedură standard pentru minimizarea riscurilor

- Scoaterea cât mai rapid din funcțiune și/sau deconectarea echipamentului infectat ori compromis pentru a preveni escaladarea incidentului;
- În cazul în care, prin intermediul echipamentului infectat sau compromis, ați comunicat cu parteneri de afaceri și/sau clienți, consultați-vă întotdeauna cu managerul dvs. înainte de a-i contacta pe aceștia;
- Oprirea conexiunii cu Centrul de Date astfel încât să se prevină alterarea back-up-ului;
- Colectarea datelor despre incident;
- Analizarea datelor colectate;
- Identificarea/Diagnosticarea incidentului;
- Rezolvarea problemei și refacerea funcționării echipamentului și a datelor de pe acesta în cel mai scurt timp posibil;
- Mentinerea legăturii cu terții implicați (RDS-RCS ș.a);
- Întocmirea unei evaluări a situației post-factum: încercați să determinați comportamentul neglijent sau riscant ce a permis incidentul și luați măsuri de îmbunătățire pentru viitor a nivelului de securitate.

Art.70.(1) Societatea monitorizează resursele informatice și de comunicații astfel încât să fie posibilă detectarea în timp util a atacurilor informatice şi a situaţiilor de încălcare a regulamentelor de securitate. Societatea utilizează un program informatic de monitorizare ce urmărește şi înregistrează:

- Tipul traficului extern şi conţinutul acestuia în cazurile în care acest lucru se impune sau este ordonat.
- Tipul traficului în reţea, a protocoalelor şi a echipamentelor conectate.
- Parametrii de securitate pentru sistemele individuale (la nivelul sistemelor de operare).

(2) Fişierele jurnal vor fi examinate regulat în vederea detectării eventualelor atacuri informatice şi abateri de la regulamentele de securitate ale S.S.I.F. Vienna Investment Trust S.A.-

(3) Detectarea viruşilor - Toate staţiile de lucru conectate la reţeaua de comunicaţii a SSIF Vienna Investment Trust, utilizează programe antivirus updatate la zi și licențiate. Programele antivirus nu se dezactivează.

Configuraţia programului antivirus trebuie să nu fie modificată într-un mod care să reducă eficacitatea programului. Frecvenţa actualizărilor este automată.

Orice virus care nu a putut fi înlăturat automat de către programul antivirus constituie un incident de securitate şi trebuie raportat imediat echipei CERT.

(4) Societatea previne toate aceste situații prin replicarea bazelor de date a sistemelor informatice importante și a tuturor informațiilor existente pe stațiile de lucru. Toate informațiile pot fi restabilite în termenul prevăzut de legislația în vigoare.

Societatea instruiește angajații proprii cu privire la:

- utilizarea în siguranță a sistemelor informatice importante;
- utilizarea în siguranță a poștei electronice;
- utilizarea în siguranță a datelor si informațiilor stocate pe stațiile de lucru;
- utilizarea în siguranță a internetului precum și regimul descărcărilor;
- recunoașterea semnelor de infectare cu diverși viruşi/malware.-

Secțiunea 6
Dispoziții finale

Art.71. S.S.I.F. are obligaţia păstrării, pe o perioadă de cel puţin 5 ani, a tuturor evidenţelor şi înregistrărilor, inclusiv a fișierelor electronice, create, trimise, primite sau stocate, referitoare la serviciile și activitățile de investiţii prestate şi tranzacţiile efectuate de societate, astfel încât să se poată supraveghea respectarea prevederilor Legii nr.297/2004 privind piaţa de capital, cu modificările completările ulterioare şi ale reglementărilor adoptate în aplicarea acesteia şi, în special, verificarea respectării de către societate a obligaţiilor faţă de clienţi sau potenţialii clienţi.-

Art.72. Înregistrările şi evidenţele care specifică drepturile şi obligaţiile S.S.I.F. şi ale clientului în baza unui contract de prestare servicii sau termenii în care S.S.I.F. furnizează serviciile clientului trebuie păstrate cel puţin pe durata relaţiei cu clientul respectiv.-

Art.73 Înregistrările şi evidenţele societăţii, inclusiv a fișierelor electronice, create, trimise, primite sau stocate, trebuie păstrate într-un mod accesibil şi într-o formă şi de o manieră în care să asigure respectarea următoarelor condiţii:

- accesul rapid şi reconstituirea fiecărui element al tranzacţiei;
- efectuarea oricărei modificări sau a altui amendament, precum şi conţinutul înregistrărilor şi evidențelor înainte de astfel de modificări sau amendamente să fie ușor constatate;
- manipularea sau alterarea înregistrărilor şi evidenţelor în alt mod nu trebuie să fie posibilă.-

Art.74. (1) Folosirea incorectă a informaţiilor confidenţiale poate conduce la sancţiuni sau penalizări atât împotriva societăţii, cât şi împotriva persoanei responsabile de folosirea incorectă a unor astfel de informaţii.

(2) În cazul în care, din neglijenţă sau intenţionat, angajatul dezvăluie informaţii confidenţiale unei terţe, persoană fizică sau juridică, acest lucru conducând la pierderea de bani sau sancţiuni aplicate Societăţii, aceasta este îndreptăţită să recupereze contravaloarea daunelor de la angajat, pe baza normelor şi principiilor răspunderii civile contractuale.-

Art.75. Societatea va respecta proceduri administrative şi contabile corespunzătoare, de control şi siguranţă pentru procesarea electronică a datelor, precum şi mecanisme adecvate de control intern.-

Art.76. Persoana care îndeplineşte funcţia-cheie de conformitate va urmări aplicarea prezentei proceduri și, în caz de încălcare sau abatere, va raporta consiliului de administrație informând imediat conducătorii și auditul intern.-

Art.77. Prezenta procedură se completează cu prevederile procedurii privind asigurarea continuității operaționale și de recuperare a datelor și a informațiilor în caz de dezastru precum și cu procedura privind abuzul de piață.-

Anexa nr.1

Activitate		***Categoria de risc a entității***			
		Majoră	***Importantă***	***Medie***	***Scăzută***
A) Evaluare internă a riscului operațional şi registrul riscurilor		*x*	*x*	*x*	*x*
B) Organizare pe procese					
1	***Managementul disponibilităţii***	*x*	*x*	*x*	
2	***Managementul utilizatorilor***	*x*	*x*	*x*	*x*
3	***Managementul incidentelor***	*x*	*x*	*x*	
4	***Managementul schimbării***				
a)	***Managementul ciclului viață a programelor informatice***	*x*	*x*	*x*	*x*
b)	***Managementul versiunilor***	*x*	*x*	*x*	*x*
c)	***Managementul testării***	*x*	*x*	*x*	*x*
5	***Managementul capacităţii***	*x*	*x*	*x*	
6	***Managementul configuraţiilor***	*x*	*x*		
7	***Managementul nivelurilor de servicii (SLA)***	*x*	*x*	*x*	
8	***Managementul securităţii***				
a)	***Cerințe generale***	*x*	*x*	*x*	*x*
b)	***Teste de penetrare***	x	x		
9	***Managementul continuităţii***	*x*	*x*	*x*	
C) Punctele de control şi măsurare					
a)	***Controale generale***	*x*	*x*	*x*	

b)	***Controale la nivelul programelor informaticice***	*x*	*x*		
c)	***Controale de flux financiar***	*x*	*x*	*x*	*x*
D) Implementare indicatori cheie de performanță (KPI) pe procese		*x*			
E) Implementare indicatori cheie de risc (KRI)		*x*	*x*		
F) Managementul securității stemelor informatice şi de comunicaţii					
a)	***Măsuri organizatorice***	*x*	*x*		
b)	***Proceduri de securitate***	*x*	*x*	*x*	*x*
c)	***Evaluarea internă de securitate***	*x*			
d)	***Plan de cooperare în domeniul securităţii sistemelor şi a informaţiei***	*x*	*x*	*x*	*x*

ANEXA NR.2

Echipa CERT

Următoarea persoană este prima responsabilă cu privire la incidentele de securitate:

Departament Trading & Suport Tehnic: LUCIAN FULEA
Număr Telefon: 021.207.48.80
E-mail (office email): lucian.fulea@viennainvestment.ro

Dacă persoana de mai sus nu poate administra incidentul, următoarea persoană va prelua responsabilitatea:

Compartiment Conformitate: BRĂDICEANU ANDI
Număr Telefon: 021.207.48.80
E-mail (office email): andi.bradiceanu@viennainvestment.ro

Alte persoane de contact din Echipa CERT:

WEST NETWORK - STANICA GABRIEL
Număr Telefon: -
E-mail (office email): gabriel.stanica@westnetwork.ro

WEST NETWORK - DIMITRUC GEORGE
Număr Telefon: -
E-mail (office email)l: office@westnetwork.ro