

П Р А В И Л А

ЗА РАБОТА, ЗАЩИТА И КОНТРОЛ НА ИНФОРМАЦИОННИТЕ И КОМПЮТЪРНИ СИСТЕМИ НА ИНВЕСТИЦИОНЕН ПОСРЕДНИК „КАРОЛ” АД

I. ОБЩИ ПОЛОЖЕНИЯ. ПРИНЦИПИ

Чл. 1. (1) Правилата за работа, защита и контрол на информационните и компютърни системи на инвестиционен посредник "КАРОЛ" АД ("Правилата") са приети на основание Закона за пазарите на финансови инструменти, чл. 16, параграф 5 и 7, изр. 2 от Директива 2014/65/ЕС, както и чл. 76 от Делегиран Регламент (ЕС) № 2017/565 .

(2) Настоящите Правила се приемат с цел защита и контрол на компютърните и информационни системи на инвестиционния посредник и осигуряване на максимална защита на данните и информацията за клиентите, съхранявани при инвестиционния посредник.

(3) Настоящите Правила уреждат принципите, правата и задълженията на специализираните отдели и служителите на инвестиционния посредник във връзка със създаването, обработването, съхраняването, архивирането и достъпа до компютърна информация в посредника.

(4) Използвани съкращения в настоящите правила: Закон за пазарите на финансови инструменти – ЗПФИ; Комисия за финансов надзор - КФН.

Чл. 2 (1) Съветът на директорите на инвестиционния посредник приема настоящите правила, които представляват и Стратегия за развитието на информационните технологии (IT стратегия) с цел поддържане на целостта и техническото обезпечение в посредника в краткосрочен и средносрочен аспект („Стратегията“).

(2) Основните цели залегнали в Правилата/ Стратегията следва да бъдат: поддържане на сигурни и съвременни компютърни и информационни системи и мрежи, високо ниво на сигурност, достъп според заеманата функция, постоянен контрол и навременна актуализация на софтуерните продукти, използвани от инвестиционния посредник.

Чл. 3. Работата, защитата и контролът на информационните и компютърни системи в инвестиционния посредник се извършва при спазване на следните основни принципи:

1. разделяне на потребителски от администраторски функции;
2. установяване на нива на достъп до информация;
3. регистриране на достъпа, въвеждането, копирането, промяната и заличаването на данни и информация;
4. осъществяване на текущ и периодичен контрол от специализирани звена и служители за спазване на принципите по т. 1-4.

II. СПЕЦИАЛИЗИРАНО ЗВЕНО ЗА ПОДДЪРЖАНЕ И ЗАЩИТА НА ИНФОРМАЦИОННИТЕ И КОМПЮТЪРНИ СИСТЕМИ

Чл. 4. (1) Инвестиционният посредник има самостоятелен отдел „Информационни технологии“ (ИТ Отдел), чиито функции са следните:

1. Подготвя и инсталира необходимите компютърни системи (хардуер) и софтуер в инвестиционния посредник;
2. Разработва наръчници, методики, правила за оперативна помощ на служители на инвестиционния посредник при работата им с компютърни системи и софтуер;
3. Разработва критерии и правила за одобрение и оценка на софтуер и хардуер за нуждите на инвестиционния посредник, включително и за подбор на доставчици на интернет и информационни услуги;

4. Оценява ефективността на използвания софтуер, хардуер и дейността на доставчиците на интернет, съобразно нуждите на инвестиционния посредник във връзка с извършваната от него дейност. За направена оценка се изготвя доклад с мотивирани предложения, който се изпраща до управителните органи на инвестиционния посредник и ръководителя на отдел „Правен, Нормативно съответствие и Вътрешен одит“.

5. Разработва, внедрява и поддържа системи за препятстване, контрол и предупреждение от нерегламентиран достъп до информация и бази данни;

6. Внедрява и поддържа антивирусен софтуер, софтуер за контрол на интернет трафика, контрол на посещаваните интернет страници и блокиране на достъпа след съгласуване с управителните органи на инвестиционния посредник;

7. Разработва, внедрява и поддържа системи за идентификация за влизане и излизане от компютърните системи;

8. Разработва, внедрява и поддържа система за авторизация на служителите на инвестиционния посредник. Служител от отдел „Правен, Нормативно съответствие и Вътрешен одит“ съвместно с отдел „Информационни технологии“ (IT отдел) предоставят авторизация за достъп до информация, данни и софтуер в качеството си на администратори.

9. Отдел „Правен, Нормативно съответствие и Вътрешен одит“ води регистър на издадените електронни подписи на служители на инвестиционния посредник, които могат да задължават посредника;

10. Отдел „Правен, Нормативно съответствие и Вътрешен одит“ следи за издадените указания от надзорния орган във връзка с компютърните и информационни системи на инвестиционния посредник;

11. Преглежда използвания софтуер, хардуер и състоянието на цялата компютърна мрежа на инвестиционния посредник на всеки 6 месеца.

12. Разработва, съвместно с Отдел „Правен, Нормативно съответствие и Вътрешен одит“, „Управление на риска“ и изпълнителния директор на инвестиционния посредник план за действие при извънредни ситуации за запазване на компютърните и информационни системи на инвестиционния посредник и за възстановяване на тяхното нормално функциониране.

(2) Лицата, поддържащи компютърните и информационни системи на ИП трябва да имат завършено висше образование, подходящо за заемането на длъжността, опит по специалността минимум 3 години и да не са осъждани. Преди започването на осъществяване на функции лицата подписват декларация за конфиденциалност.

III. ПРАВА И ЗАДЪЛЖЕНИЯ НА СЛУЖИТЕЛИТЕ НА ИНВЕСТИЦИОННИЯ ПОСРЕДНИК ПО ОТНОШЕНИЕ НА ИНФОРМАЦИОННИТЕ И КОМПЮТЪРНИ СИСТЕМИ

Чл. 5. Права и задължения на лицата, работещи по договор за инвестиционния посредник, във връзка с работата им с компютърни и информационни системи на инвестиционния посредник са следните:

1. Служителите на инвестиционния посредник имат право да работят на служебен компютър, достъпът до съхраняваните данни в него се осъществява с въвеждането на потребителско име и парола;

2. Служителите на инвестиционния посредник имат право на достъп до Интернет предвид необходимостта от получаване, предоставяне на клиенти и сравняване на информация за търгуваните на регулирани и извън регулирани пазари финансови инструменти, техните цени, комисионни и разходи свързани със сделките и др.

3. На служителите на инвестиционния посредник се забранява предоставянето на трети лица на личното потребителско име и парола за влизане в служебния компютър;

4. На служителите на инвестиционния посредник се забранява предоставянето на потребителско име, пароли, кодове и други идентификатори за достъп от служителите,

отговарящи за отношенията с депозитарни институции, места за изпълнение, държавни органи или надзорни институции на други служители в посредника;

5. Служителите на инвестиционния посредник имат право при или по повод изпълнение на служебните си задължения, да създават файлове на служебния си компютър като носят отговорност за правилността и точността на въведените данни и информация в компютърната система или вътрешна мрежа на инвестиционния посредник;

6. Служителите на инвестиционния посредник имат право при или по повод изпълнение на служебните си задължения, да влизат и ползват данни от вътрешна информационна мрежа на инвестиционния посредник.

7. При загуба на данни или информация от служебния си компютър служителите на инвестиционния посредник незабавно уведомяват лицето, поддържащо Информационни технологии, комуникация и бази данни при ИП, който им оказва съответната техническа помощ. Уведомление се прави и до отдел Вътрешен контрол.

8. Служителите на инвестиционния посредник имат право да запазват и архивират файлове, създадени при или по повод изпълнение на служебните им задължения, на служебния си компютър, CD, DVD и други носители. Копията направени на външни харддискове, CD, DVD, флаш памет или други носители се съхраняват в помещения на инвестиционния посредник;

9. На служителите на инвестиционния посредник се забранява изнасянето на хардуер или носители на информация като, но не само, външни харддискове, CD, DVD, флаш памет и др., които съдържат данни и информация за предоставените от инвестиционния посредник инвестиционни или допълнителни услуги на негови клиенти или всяка друга информация, която се квалифицира като служебна или търговска тайна;

10. На служителите на инвестиционния посредник се забранява извършването на опити за достъп до компютърна информация и бази данни, до които не им е даден достъп съобразно заеманата от тях длъжност, както и извършването на каквито и да било действия, които улесняват трети лица за несанкциониран достъп;

11. Служителите на инвестиционния посредник имат право да обменят компютърна информация посредством вътрешната компютърна мрежа на инвестиционния посредник само със служители на инвестиционния посредник, с които имат преки служебни взаимоотношения по съвместен проект, имат отношения на подчиненост, както и при извършвана проверка от отдел „Правен, Нормативно съответствие и Вътрешен одит“ за целите и обхвата на проверката;

12. Служителите на инвестиционния посредник след края на работния ден изключват компютрите си или ги привеждат в режим log off, освен в случаи изрично указани в заповед на Съвета на директорите.

13. Служителите на инвестиционния посредник са уведомени и се съгласяват, че отдел „Правен, Нормативно съответствие и Вътрешен одит“, съвместно с лицето, отговарящо за информационни технологии може да следи за спазването на тези правила. Настоящата клауза не отнема правомощия на звеното по Сигурността, ако ИП е създал такова, да извършва проверка за компютърна сигурност.

14. Други права и задължения на служителите на инвестиционния посредник във връзка с информационните и компютърни системи се посочват в съответните длъжностни характеристики.

Чл. 6. (1) Информацията и данните, които следва да се архивират на електронен носител се предават на лицето отговарящо за информационните технологии, защитени с пароли, за което се изготвя съответен протокол. Паролите, с които са защитени данните са известни на служителя, архивирал данните и на ръководителя на отдел „Правен, Нормативно съответствие и Вътрешен одит“, лицето от звеното за информационни технологии.

(2) Архивираната информация и бази данни се съхраняват на отделни носители, защитени от несанкциониран достъп и физически увреждания.

Чл. 7. На всички служители на инвестиционния посредник се забранява инсталирането и използването на незаконен софтуер, както и софтуер за on line разговори, освен в случаите позволени от СД или изпълнителния директор. Софтуер за on line разговори може да се използва, когато това е необходимо за приемане или предаване на нареждания за сделки с финансови инструменти или обмен на информация с клиенти или други институции.

Чл. 8. Архивирана компютърна информация и данни се предоставят само на служители на инвестиционния посредник, които имат право на достъп съгласно заеманата от тях длъжност или изпълнявана служебна задача при спазване на принципа „необходимост да се знае“.

Чл. 9. Достъпът до компютърна информация, бази данни и софтуер се ограничава посредством технически методи - идентификация на потребител, пароли, отчитане на времето на достъп, въвеждане на забрани за копиране, използване на софтуер за проследяване на несанкциониран достъп, опити за достъп, повреждане, копиране, изменение или изтриване на компютърни данни или информация.

Чл. 10. Инвестиционният посредник въвежда физически мерки за защита на информационните и компютърни системи срещу кражба, пожар, наводнение, прекъсване на електрозахранването и други.

Чл. 11. (1) В случай на несанкциониран достъп в базите данни, съхранявани от инвестиционния посредник, лицето, отговарящо за информационни технологии при ИП незабавно уведомява изпълнителния директор и ръководителя на отдел „Правен, Нормативно съответствие и Вътрешен одит“. В случай, че освен несанкциониран достъп са променени или заличени данни, съхранявани от инвестиционния посредник, лицето, отговарящо за информационни технологии при ИП, осигурява възстановяване на данните в състоянието им преди промяната или заличаването. Ако това не е възможно се ползват архивираните данни, съобразно посоченото в настоящите Правила.

(2) При евентуален срив в ИТ информационните системи за дистанционно приемане на клиентски поръчки /платформата за електронна търговия/, служителите в Дружеството прилагат следните мерки:

Служител от ИТ отдел стартира процедура по установяване на проблемно звено съгласно структурата на системата за дистанционно приемане на клиентски поръчки и конкретното оплакване от клиента и предприема действия, както следва:

1. При установяване на проблем с връзката към БФБ, служителят стартира работата на резервно интернет трасе през алтернативния интернет доставчик и рестартира комуникатора към XETRA; служителят уведомява ръководителя на ИТ отдела и вдига тикет за проблем при интернет доставчика.

2. При установяване на проблем в самия комуникатор /липса на лог файлове/, служителят рестартира комуникатора, в случай, че работата не се възстанови, служителят стартира резервния комуникатор и уведомява ръководителя на ИТ отдела.

3. При установяване на проблем в хардуера /сървър/ с инсталирания комуникатор, служителят стартира резервния сървър /виртуален/ и уведомява ръководителя на ИТ отдела.

4. При установяване на проблем в работата на уеб сървър за комуникация с клиентите, служителят рестартира хардуера и сервизите; в случай, че проблема не е отстранен, служителят стартира резервния сървър /виртуален/, прехвърля

комуникацията към него /подмяна на IP адресите/ и уведомява ръководителя на ИТ отдела

5. При установяване на проблем с работата на сертификационния сървър, служителят стартира резервния сървър /виртуален/, стартира скрипта за зареждане на бекъпа на базата данни с активни и анулирани сертификати /изпълняван на дневна база/, преустановява издаването на нови сертификати и прехвърля комуникацията към него /подмяна на IP адресите/; служителят уведомява своевременно ръководителя на ИТ отдела

6. При установяване на проблем с базата данни, служителят последователно рестартира базата данни и уведомява ръководителя на ИТ отдела; при неуспех стартира резервния сървър, започва процедура по възстановяване на базата данни от последния архив /изпълняван на дневна база/; паралелно с този процес служителят уведомява брокера на БФБ, който следва да сваля от търговската система въведените и канселирани ордери през текущия ден в предлагания от XETRA формат; след приключване на възстановяването на базата данни, служителят стартира процедура по автоматичен импорт на новите и канселирани ордери в базата; след приключването на импорта служителят прехвърля комуникацията към резервния сървър /смяна на IP адреса/ рестартира последователно комуникатора и уеб сервизите, като след това стартира през XETRA функцията за пропуснати бродкасти, която възстановява информацията за сделките на клиентите по въведени ордери за текущия ден.

(3) В случаи на възпрепятствано приемане на ордери чрез електронни платформи клиентите могат да подават ордерите по стандартния ред на гише или чрез дистанционни способи извън търговските платформи – телефон, имейл и други приложими. За целта, паралелно с тук-описаните процеси, всички активни брокери получават задача приоритетно да обслужват клиентски нареждания получени на гише и чрез другите приложими дистанционни способи.

(4) В зависимост от степента на проблема, ръководителят на отдела „Информационни технологии“ взема решение дали работата на системата за дистанционно приемане на клиентски поръчки да бъде прехвърлена към резервната система и/или в алтернативен дейта център.

(5) След възстановяване работата на системата, в края на съответния работен ден, ръководителят на отдел „Информационни технологии“ отдела мигрира обратно работата на платформата към основната ѝ среда, като връща обратно в готовност резервните системи.

IV. ПРАВИЛА ЗА РЕГИСТРИРАНЕ (ЗАПИС) НА ТЕЛЕФОННИТЕ РАЗГОВОРИ ИЛИ ЕЛЕКТРОННИ СЪОБЩЕНИЯ

Чл. 12. Настоящите правила се приемат и прилагат в съответствие с големината и организационната структура на инвестиционния посредник, както и с естеството, мащаба и сложността на неговата стопанска дейност.

Чл. 13. Инвестиционният посредник изготвя и съхранява записи на всички телефонни разговори и съобщения или на разговори и съобщения чрез електронни способи за комуникация, които се отнасят до трансакции във връзка със сключването на сделки за собствена сметка или с приемането, предаването и изпълнението на нареждания на клиенти, независимо от това дали сделката е сключена. Тук се включват телефонни разговори както с клиенти на инвестиционния посредник, така и между служители на инвестиционния посредник.

Чл. 14. (1) Преди да се предоставят инвестиционни услуги или дейности, отнасящи се до приемането, предаването и изпълнението на нареждания на нови и съществуващи клиенти, инвестиционният посредник информира клиента за това, че:

- а) разговорите и съобщенията се записват; и
- б) копие от записите на тези разговори с клиента и съобщения с клиента ще бъде на разположение при поискване за срок от пет години и, когато е поискано от компетентния орган, за срок до седем години.

(2) Информацията по ал. 1 се предоставя на езика или езиците, използвани за предоставянето на инвестиционни услуги на клиенти.

Чл. 15. Инвестиционният посредник предприема необходимите мерки, с цел да не допусне приемането и иницирането на телефонни разговори и електронна комуникация чрез използването на технически средства и апаратура, различни от определените за целта от инвестиционния посредник.

Чл. 16. (1). Инвестиционният посредник уведомява своите клиенти, че телефонните разговори и електронна комуникация с тях ще бъдат записвани. Задължението по изречение първо се счита за изпълнено, ако инвестиционният посредник е уведомил клиента еднократно преди началото на предоставянето на инвестиционните услуги.

(2) Ако инвестиционният посредник не е изпълнил изискването по алинея първа, той няма право да извършва инвестиционни услуги и дейности посредством телефонна или друга комуникация съгласно, свързани с приемането, предаването и изпълнението на нареждания на клиенти.

Чл. 17. Изискванията за запис на телефонните разговори се прилагат и за клоновете и офисите на инвестиционния посредник, извършващи дейност на територията на Република България за сделките и операциите, извършени чрез клоната или офиса.

Чл. 18. На запис подлежат всички относими телефонни разговори и електронна комуникация (тези, които водят или биха могли да доведат до сключване на договор/сделка с финансови инструменти), извършени чрез, изпратени от или получени от технически устройства, предоставени от инвестиционния посредник на негови служители или лица, работещи по договор, или използването на които устройства от служители или лице, работещо по договор, е било прието или разрешено от инвестиционния посредник.

Чл. 19. Когато възникнат изключителни обстоятелства и посредникът не може да регистрира разговора или съобщението на устройствата, които са предоставени, приети или разрешени от посредника, то съответното лице, работещо по договор, е длъжно да изготви писмен доклад за съдържанието на разговора, рецепиента, продължителността на разговора, както и приетите ангажименти, ако има такива от страна на служителя. Докладът за горните обстоятелства се съхраняват от посредника и е достъпен за отдел „Правен, Нормативно съответствие и Вътрешен одит“ и от компетентните надзорни органи.

Чл. 20. (1) Забранява се на служители или лица, работещи по договор за инвестиционния посредник, да извършват, изпращат или получават съответни телефонни разговори и електронни съобщения чрез частно оборудване и частни устройства (компютърни системи, телефони, таблети и други), комуникацията от което оборудване или устройства инвестиционният посредник не е в състояние да запише или копира.

(2) Инвестиционният посредник води и редовно актуализира регистри на лицата, които имат служебни или собствени устройства, одобрени за използване от инвестиционния посредник.

Чл. 21. Управителният орган на ИП осъществява ефективен надзор и контрол върху политиките и процедурите, отнасящи се до регистрирането от посредника на телефонни разговори и електронни съобщения. Механизмите за спазване на изискванията за регистриране, прилага ни от ИП са технологично неутрални.

Чл. 22. С оглед наблюдение за спазването на изискванията за регистриране (запис) и за водене на регистри на съответната комуникация, Отдел „Правен, Нормативно съответствие и Вътрешен одит“ осъществява периодично наблюдение на сделки и нареждания, подлежащи на тези изисквания, включително съответните разговори. Това наблюдение се основава на рисковете, установени от ИП и рисковия профил на клиентите и е пропорционално на предлаганите услуги и дейности.

Чл. 23. Инвестиционният посредник трябва да може да демонстрира начините на приложение на настоящата политика и процедурите и управленския надзор пред компетентните органи при поискване.

Чл. 24.(1) Инвестиционният посредник регистрира на траен носител всяка съществена информация, отнасяща се до съответните преки разговори с клиенти.

Преките разговори с клиенти се провеждат по адреса на управление на ИП, регистрирани клонове и офиси, както и след предварителна уговорка с клиента на място, взаимно уговорено между страните. Без значение от мястото на провеждане на срещата, ако тя е проведена от лице, работещо по договор за ИП, член на управителен или контролен орган или което и да е лице, действащо от името на ИП и/или във връзка с дейността на ИП, то фактът на провеждането на срещата и съдържанието ѝ следва да бъдат регистрирани.

(2) Регистрираната информация за срещите по ал. 1 съдържа като минимум следното:

- а) дата и час на срещите;
- б) място на срещите;
- в) идентификация на участниците;
- г) инициатор на срещите; и
- д) значима информация относно нареждането на клиента, включително цена, обем, вид на нареждането и кога трябва да бъде предадено или изпълнено.

(3) Записите се съхраняват на траен носител, който позволява тяхното възпроизвеждане или копиране, и във формат, който не позволява промяната или изтриването на оригиналния запис. Записите се съхраняват върху носител така, че да бъдат леснодостъпни и налични за клиенти при поискване.

(4) Инвестиционният посредник е длъжен да осигури качеството, точността и пълнотата на регистри на всички телефонни записи и електронни комуникации.

(5) Срокът за съхранение на даден запис започва да тече от датата, на която е създаден записът.

Чл. 25. Политиката по настоящия раздел се разглежда и оценява периодично с оглед ефективността ѝ, като ИП приема такива алтернативни или допълнителни мерки и процедури, които са необходими и целесъобразни. Като минимум такива алтернативни или допълнителни мерки се приемат, когато инвестиционният посредник приеме или позволи използването на ново средство за комуникация.

Чл. 26. Инвестиционният посредник свежда до знанието на съответните служители настоящата процедура за запис са телефонни разговори и електронна комуникация и обучава служителите как да я спазват като посочва технически начините за извършване на запис.

V. ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

§ 1. Съветът на директорите на инвестиционния посредник може да издава заповеди и инструкции по прилагането на тези Правила.

§ 2. Настоящите Правила се предоставят за сведение и изпълнение на служителите на инвестиционния посредник и се прилагат едновременно с Правилата за вътрешна организация и Правилата за вътрешен контрол.

§ 3. Правилата са приети от Съвета на директорите на "КАРОЛ" АД с решение от 22.01 2018 г.