

ПРАВИЛА ЗА УПРАВЛЕНИЕ НА РИСКА НА УД "ЕКСПАТ АСЕТ МЕНИДЖМЪНТ" ЕАД

С настоящите правила се уреждат организационната структура, нивата на отговорност и политиките по установяване, наблюдение, оценяване и управление на рисковете, свързани с дейностите, процедурите и системите по предоставяни от УД "Експат Асет Мениджмънт" ЕАД (по-долу "управляващото дружество" или само "УД") услуги съгласно чл. 2, ал. 2 от Наредба № 26 от 22.03.2006 г. за изискванията към дейността на управляващите дружества ("Наредба 26").

I. ОСНОВНИ ПОЛОЖЕНИЯ

Чл. 1. Настоящите правила за управление на риска съдържат:

1. Организационна структура, нива на отговорност и отчетност, по управлението на рисковете в УД.
2. Политика за управление на риска на УД, която включва:
 - а) процедури за установяване на рисковете, свързани с дейностите, процедурите и системите на управляващото дружество и за определяне на допускано ниво на риск, ако такова може да бъде установено;
 - б) процедури и мерки за управление на рисковете, свързани с дейностите, процедурите и системите на управляващото дружество;
 - в) механизми за осъществяване на наблюдение върху адекватността и ефективността на политиката и процедурите по б. "а" и върху спазването от управляващото дружество и лицата, които работят по договор за управляващото дружество, на процедурите и мерките по б. "б";
 - г) механизми за наблюдение върху адекватността и ефективността на предприетите мерки за отстраняване на констатирани непълноти и несъответствия в политиката и процедурите по т. 1 и процедурите и мерките по т. 2, вкл. невъзможност за спазването им от лицата.
3. Основни положения и рамка на план за действие при възникване на кризисни ситуации.

II. ОРГАНИЗАЦИОННА СТРУКТУРА

Чл. 2. (1) Организационната структура в управляващото дружество, свързана с управлението на риска включва:

1. Съвет на директорите.
2. Лицето/ата, представляващ/и управляващото дружество.
3. Служители, работещи по договор в управляващото дружество.

(2) Когато организационната структура, определената в ал.1, е друга или се промени, следва да се гарантира спазването на основния принцип за разделянето на отговорностите между служителите с цел предотвратяване конфликти на интереси.

Чл. 3. Съветът на директорите има следните отговорности по управление на риска:

1. Приема правила за управление на риска и следи за тяхната актуализация.
2. Най-малко веднъж на 3 месеца преглежда и оценява правилата, като при непълноти и/или необходимост от подобряване на управлението на риска приема изменения и допълнения в правилата.

Чл. 4. Представляващите управляващото дружество имат следните отговорности по управлението на риска:

1. Организируют работата по правилно провеждане на приетата от Съвета на директорите политика по управление на риска.
2. Следят за съответствие на използваните от съответните служители и приетите политика и процедури за установяване на рисковете, свързани с дейностите на управляващото дружество и механизмите за наблюдението върху адекватността и ефективността им.
3. Вземат решения за кадрово, материално-техническо и методическо осигуряване на дейностите по управление на риска.
4. Представят пред Съвета на директорите най-малко веднъж на 3 месеца преглед и оценка на правилата, като при непълноти предлагат мерки за подобряване на управлението на риска.

Чл. 5. Отделът по управление на риска действа независимо от другите звена в управляващото дружество, отчита се пряко пред управителния орган и има следните функции:

1. Внедрява и наблюдава политиката и процедурите за установяване на рисковете, свързани с дейностите, процедурите и системите на управляващото дружество.
2. Изготвя и представя на управителния орган, до 10-о число на всеки месец доклад за дейността на отдела през предходния месец, в който посочва констатирани непълноти и несъответствия в политиката и процедурите по чл. 1, т. 1 и процедурите и мерките по чл. 1, т. 2, както и предприетите мерки за отстраняването им.

Чл. 6. Служителите, работещи по договор в управляващото дружество, извън лицата по чл. 3, 4 и 5, са задължени да се запознаят и да спазват процедурите, описани в настоящите правила по Управление на риска.

III. ПОЛИТИКА ЗА УПРАВЛЕНИЕ НА РИСКА НА УД "ЕКСПАТ АСЕТ МЕНИДЖМЪНТ" ЕАД

Чл. 7. Политиката по управление на риска е част от вътрешноорганизационната структура на УД и действа и се прилага интегрирано с другите вътрешно-нормативни документи на дружеството. Целта на тази политиката е да се документират процедурите по установяване, управление, наблюдение и оценка на рисковете, свързани с дейностите, процедурите и системите на УД по реда на Наредба No.26.

Чл. 8. (1) Управляващото дружество разграничава следните видове рискове, свързани с дейностите, процедурите и системите:

1. Вътрешни- свързани с организацията на работа на Управляващото Дружество. Вътрешните рискове се състоят, без да се ограничават до:

- а) Рискове, свързани с персонала;
- б) Рискове, свързани с процесите;
- в) Рискове, свързани със системите.

2. Външни- свързани с макроикономически, политически и други фактори, които оказват и/или могат да окажат влияние върху дейността на Управляващото Дружество. Външните рискове се състоят, без да се ограничават до:

- а) Риск на обкръжаващата среда;
- б) Риск от физическо вмешателство.

(2) Оценката на рисковете се отчита от отдела за управление на риска, въз основа на резултатите от описаната по-долу "Процедура по идентификация, оценка и контрол на риска", прилагана от всички функционални звена на УД.

(3) Въз основа на отчетените резултати, съгласно процедурата, УД установява допустимо ниво на риск за организацията и осигурява извършването на дейността да бъде в рамките на определеното допустимо ниво.

Чл. 9. (1) Рискове, свързани с персонала, са рискове от загуби във връзка с:

1. Измами и кражби на лица, работещи по договор за УД;
2. Недобросъвестно поведение от страна на служителите на УД, както и некоректно отношение на ръководния персонал към служителите;
3. Недостатъчна квалификация и липса на подготовка на лицата, работещи по договор за УД;
4. Неблагоприятни изменения в трудовото законодателство;
5. Неосигурена безопасност на трудовата среда;
6. Текучество.

(2) Процедурите/мерките за управление на рисковете, свързани с персонала, включват:

1. Ясно дефиниране на вътрешни правила относно правата и задълженията на служителите;
2. Ясно дефинирани вътрешни правила за достъп до информационните системи и бази данни на Управляващото Дружество;
3. Регулярни обучения на персонала по теми, свързани с финансова теория и практика, управление на риска, нормативната база, имаща отношение към дейността на УД, информационни технологии и сигурност и други;
4. Регулярни срещи между отделните звена на Управляващото Дружество за обмяна на опит, впечатления и препоръки по отношение на източниците на риск и търсене на решения за управлението и минимизирането им;
5. Ежегодни събеседвания и оценка на персонала;
6. Поддържане на отворени, открити комуникации между различните звена в Управляващото Дружество.

Чл. 10. (1) Рискове, свързани с процесите са рисковете, възникващи от накарняване интереса на клиента в резултат на:

1. Действия в нарушение на определената в договора инвестиционна стратегия;
2. Неправилна преценка за рисковия профил на клиента и избор на неподходяща и неуместна за клиента инвестиционна стратегия;
3. Вреди, причинени от предоставяне на неверни, неточни или непълни анализи и прогнози по конкретна инвестиционна консултация;
4. Извършване на трансакции с инструменти, с които Клиента няма право да търгува;
5. Недобросъвестно използване на конфиденциална информация, предоставена от клиента (неупълномощен достъп до поверителна информация на клиента), нарушаване на търговска тайна;
6. Злоупотреба с конфиденциална информация;
7. Конфликт на интереси;
8. Грешки при събиране, въвеждане и осчетоводяване на данни;
9. Действие в нарушение на политиката за най-добро изпълнение и дължима грижа към клиента;
10. Грешки при подаване на информация към клиента;
11. Грешки при преоценка на клиентски активи;
12. Неправилна отчетност и съхранение на клиентски активи.

(2) Процедурите/мерките за управление на рисковете, свързани с процесите, включват:

1. Изчерпателно и максимално точно уговаряне с клиента при сключване на договора обхваща на управлението и конкретните сделки и действия, които УД ще бъде овластено да извършва;
2. С цел коректната оценка рисковия профил на клиента УД класифицира клиентите си съгласно Правила за определяне на клиентите като професионални, непрофесионални или приемлива насрещна страна;

3. Изискване към клиентите и потенциалните клиенти да представят в писмена форма информация за установяване на съществени факти относно финансовите им възможности, инвестиционните цели, знания, опит относно услугите по управление на портфейл и предоставяне на инвестиционни консултации и за готовността им да рискуват; УД изисква от клиента да актуализира тази информация при настъпване на промяна;

4. Поддържане на системи и процедури, които осигуряват трайното и конфиденциално съхранение на получената от клиентите информация за техните финансови възможности, инвестиционни цели, знания, опит и готовност да рискуват, както и за дадените им съвети и препоръки, заедно с мотивите;

5. Предварително запознаване на клиентите с вида и характеристиките на видовете финансови инструменти, с които УД ще сключва сделки, както и с рисковете, свързани с тези инструменти;

6. Предварително уговаряне, при сключване на договора, на ред и срок за отчитане пред клиента в съответствие с профила на клиента и законоустановените изисквания, която да гарантира навременното и точно подаване на изискуемата информация. При предоставяне на информация до клиента, УД се стреми да предоставя максимално релевантна такава, която да осигури на клиента възможност да направи преценка за обекта на инвестициите:

- метода и периодичността на оценка на финансовите инструменти в клиентския портфейл;
- данни за всяко делегиране на управлението на всички или на част от финансовите инструменти и/или пари в клиентския портфейл;
- характеристики и сведения за всеки еталон, по който резултатите от управлението на портфейла ще бъдат сравнявани;
- видовете финансови инструменти, които могат да се включат в клиентския портфейл, и видовете сделки, които могат да се сключват с тях, включително всички ограничения;
- целите на управлението, нивото на риск, съдържащо се в преценката на управляващия портфейла, както и всички специфични ограничения на тази преценка;

7. УД създава вътрешна организация и условия за установяване на потенциалните конфликти на интереси между:

- УД, включително членовете на управителни и контролни органи и всички други лица, които могат да сключват самостоятелно или съвместно с друго лице сделки за сметка на УД, всички други лица, които работят по договор за УД, и свързаните с УД чрез контрол лица, от една страна, и клиентите, от друга страна;
- отделните клиенти на УД, като в случай че въпреки прилагането на правилата за вътрешната организация на управляващото дружество продължава да съществува риск за интересите на клиента, УД информира клиента за общото естество и/или източници на потенциалните конфликти на интерес.

8. УД приема ефективни процедури и мерки за третиране на конфликт на интереси, уредени в Правилата за управление на конфиденциална информация и предотвратяване конфликта на интереси, със съдържание в съответствие с действащото законодателство и добрите международни практики;

9. В случай, че УД съхранява финансови инструменти и парични средства на клиентите, то прилага подходящи мерки за отделянето на собствения портфейл от финансови инструменти от този на инвеститорите, които му позволяват да отчита отделно паричните средства на клиентите от сделки с финансови инструменти и да гарантира запазване на имуществените права на клиентите, свързани с принадлежащите им финансови инструменти и парични средства;

10. УД приема и прилага Политика, която да осигурява постигането на най-добър резултат за клиента, отчитайки факторите по чл. 30, ал. 1 ЗПФИ, като политиката определя по отношение на всеки клас финансови инструменти лицата, до които УД ще подава нарежданията;

11. УД организира права и нива на достъп до клиентска информация, които осигуряват превенция на лицата, работещи по договор за УД да разгласяват и да ползват за облагодетелстване на себе си или на други лица факти и обстоятелства, засягащи наличностите и операциите по паричните сметки и по сметките за финансови инструменти на клиенти на УД, както и всички други факти и обстоятелства, представляващи търговска тайна, които са узнали при изпълнение на служебните и професионалните си задължения. В определени ситуации УД може да предприеме съответни мерки, включително като сключва договори или изисква подписване на декларации за опазване на тайна, които да гарантират, че лицата, които управляват портфейла на клиента, извършват финансови и други анализи, както и останалите определени от УД лица, които имат достъп до информацията за клиента, ще пазят търговските и други тайни на клиента и неговия търговски престиж.

Чл. 11. (1) Рискове, свързани със системите:

1. Достоверност и пълнота на данните, липса на прецизност в методите на обработка;
2. Грешки на софтуерни продукти;
3. Несъвършенство на използваните технологии;
4. Срыв на информационните и комуникационни системи.

(2) Процедурите/мерките за управление на технологичните рискове включват:

1. Архивиране на информационната система на УД, поддържане на "back-up" системи;
2. Процедура за възстановяване на работоспособността на информационната система;
3. Организация и управление на достъпа на служителите до информационната система, която да не позволява неволни или умишлени нарушения в интегритета на системите, ползвани от УД;
4. Дефиниране на различни класове информация, съхранявана в УД;
5. Дефиниране на нива на достъп на служителите на Управляващото Дружество според длъжностната им характеристика;
6. УД разработва и разполага с план за действие в кризисни ситуации, който осигурява продължаването и поддържането за достатъчно дълъг период нормалната работа на дружеството при спазване на законоустановените норми за дейността.

Чл. 12. (1) Рисковете на обкръжаващата среда включват:

1. Неблагоприятни промени в нормативната уредба;
2. Риск, свързан с финансови средства с незаконен произход;
3. Рискове, свързани с прехвърлянето на важни дейности на трета страна изпълнител;
4. Политически изменения;
5. Изменения в данъчната уредба.

(2) Процедури/мерки за управление на рисковете, свързани с обкръжаващата среда:

1. УД поддържа актуална база данни с нормативната регламентация, имаща отношение към дейността на УД; организира мерки за следене на съответствието на прилаганите политики с изискванията на законодателството и използва външни консултанти в случай на необходимост за привеждане на дейността на Управляващото Дружество в съответствие с нормативните изисквания;

2. При встъпване в трайни отношения (сключване на договор) УД извършва идентификация на клиента в съответствие с изискванията на Закона за мерките срещу изпирането на пари (ЗМИП) и Закона за мерките срещу финансиране на тероризма (ЗМФТ), както и актовете по прилагането им. УД изисква от клиентите декларация за произход на средствата и съхранява събраните по идентификация на клиента данни и документи по начин, който позволява да бъдат достъпни при поискването им по законоустановения ред;

3. УД взема активно участие в публичното обсъждане на промени в нормативната уредба, касаеща дейността на управляващите дружества;

4. УД следи за ефективността и качеството на изпълнение от страна на лицата, до които е подало нареждания за изпълнение, и когато е необходимо взема мерки за отстраняване на установени нередности. Извършва проверка на Политиката по изпълнение на нареждания веднъж годишно, както и при всяка съществена промяна, която може да се отрази на възможността на УД да осигурява най-добри резултати за своите клиенти.

Чл. 13. (1) Рискът от физическо вмешателство включва:

1. Природни бедствия;
2. Пожар;
3. Външни измами и кражби;
4. Терористични актове;
5. Непозволено проникване в информационните системи.

(2) Процедури/мерки за управление на риска от физическо вмешателство:

1. Сключване на договор с охранителна фирма за осъществяване на 24-часов наблюдение и контрол на помещенията в които се намират технологичните средства и архивите на Управляващото Дружество;
2. Профилактика на регулярна база на въведените системи за наблюдение и контрол;
3. Разработване на процедура за евакуация на служителите в случаите на непосредствено физическо вмешателство в дейността на Управляващото Дружество;
4. Процедура за докладване на инциденти.

(3) Детайлна категоризация на рисковете се съдържа в Приложение №1.

Чл. 14. (1) Процедура за идентификация, оценка и контрол на риска - обхваща 4 фази, както следва:

1. Идентификация на рисковете – идентификация на рисковете, които не са обект на контрол. Риск и Контрол самооценка;
2. Оценка на риска – оценка на честота на настъпване и степента на въздействие на рисковете, както и промяна в нивата на риск:
 - а) Отчет за Съществени Рискови Показатели;
 - б) Отчет за настъпили инциденти.
3. Наблюдение на риска – наблюдение на неприемливите рискове, промяна в рисковете/рисковите нива и процеси за управление на риска:
 - а) отдел за управление на риска;
 - б) Съвет на директорите.
4. Намалване на риска – управление за намаляване на риска, съобразно допустимото ниво на риск:
 - а) проследяване на открития при одит проверки;
 - б) установяване на контролни стандарти;
 - в) застраховане срещу риска.

(2) Във фазата “Идентификация” се идентифицират основните рискове. Допуска се определени (малко на брой) рискове да не бъдат проследени (неидентифицирани). По дефиниция това са рискове, които не могат да бъдат разпознати.

(3) Резултатът от фазата “Оценка” е набор от приемливи и неприемливи рискове.

(4) По време на фазата “Ограничаване на риска” се прилагат подходящи мерки (контрол, прехвърляне или избягване) за ограничаване на неприемливите рискове.

Чл. 15. (1) Риск и Контрол самооценка: целта на процеса по Риск и Контрол самооценката е:

1. да се подобри своевременното установяване на неидентифицирани рискове;

2. да се подобри преценката за приемливостта на нивото на идентифицираните рискове;
3. да се доразвият и подобрят алтернативни механизми за контролиране на неприемливите рискове;
4. да се улесни прилагането на навременни и адекватни действия за ограничаване на риска;
5. да се ангажират отделните функционални звена в УД в процеса по установяване и оценка на риска, като по този начин се постига по-голяма отговорност на служителите на дружеството за управлението на рисковете.

(2) Процесът по Риск и Контрол самооценка е периодичен и се извършва веднъж годишно. Всеки последващ цикъл е свързан с предходните особено във фазата "Идентификация". Наборът от вече идентифицираните рискове служи като отправна точка, като в хода на процеса се проверява доколко те са актуални, междуременно ограничени или невалидни.

(3) Резултатите от процеса по Риск и Контрол самооценка се използват за определяне на Съществени Рискови Показатели за отделните бизнес функции. Крайните резултати се свеждат до знанието на съответно отговорните лица.

Чл. 16. (1) Идентификация на риска - идентификацията на риска започва с вътрешно за всяко звено изследване, което представлява дейност по установяване на факти. В случай на възникване на рисково събитие, те се описват от съответния отдел в дневник, съгласно Приложение №2.

(2) Дневниците на различните отдели се събират и съхраняват от отдела по управление на риска в т.нар. "рискова библиотека". Събирането на данни в рисковата библиотека е динамичен процес, който се актуализира при необходимост.

Чл. 17. (1) Оценка на риска - действията, които се предприемат в тази фаза се предопределят от резултатите получени във фазата идентификация. Оценката се определя съвместно от съответния отдел, който идентифицира риска и звеното по управление на риска.

(2) Идентифицираните рискове се анализират от гледна точка на следните 2 характеристики:

1. честота на възникване;
2. степен на въздействие.

| | | | | | | |
|-----------------------|------------------|-----------------------|-------|---------|----------|---------------|
| честота на възникване | често / обичайно | | | | | |
| | вероятно | | | | | |
| | случайно | | | | | |
| | рядко | | | | | |
| | малко вероятно | | | | | |
| | | незначително | слабо | умерено | критично | катастрофично |
| | | степен на въздействие | | | | |

(3) Съгласно оценката по ал.1, рисковете се категоризират на приемливи и неприемливи, съобразно определеното за допустимо ниво на риск в дружеството.

Чл. 18. (1) Ограничаване на риска - въз основа на резултатите от оценката на риск се определят възможни мерки за ограничаването му. Необходимо е да се оцени и остатъчният риск след предприемането на ограничителните мерки.

(2) Ограничаването на риска се налага в случаите, когато идентифицираните нива на риск надхвърлят приетите за допустими. Ограничаването на риска може да бъде осъществено по няколко начина, по-важните от които са следните:

1. избягване на риска чрез прекратяване на дейността, която го поражда или заменянето и с алтернативна;
2. намаляване на възможността на проява на риска – чрез внедряването на контролни процеси, подобряване на надзора върху дейността, обучения;
3. намаляване на ефекта от проявяването на риска – чрез застраховане;
4. прехвърляне на риска към трети страни, които по същество са обект на същия тип риск;
5. предварително установяване и приемане на част от ефекта на риска, като присъща за решението на управителните органи за продължаване на съответната дейност.

(3) Ограничителните мерки се одобряват от лицата по чл. 4.

(4) Извършване на действия съобразно одобрените ограничителни мерки.

Чл. 19. Наблюдение на риска- предприемането на конкретни действия по ограничаването на риска е отговорност на упълномощените лица в съответните звена. Отделите по управление на риска, вътрешен контрол и сигурността подпомагат внедряването на контролните механизми и установяването на вътрешни контролни стандарти. Отговорните лица се отчитат пред звеното за управление на риска.

Чл. 20. Отчитане на настъпили инциденти – политиката по управление на риска изисква незабавно отчитане инциденти, които са значими; имат заплашителен характер; имат отношение към репутацията на дружеството; имат незаконно или осквернително действие.

Чл. 21. (1) Отчитане на Съществените Рискови Показатели - тези показатели дават информация на ръководния персонал дали специфичните рискове са в предварително определените граници и дали е необходимо предприемането на действия за ограничаването им до допустимото ниво за дружеството.

(2) Наличието на Съществените Рискови Показатели се определя на базата на резултати от процеса по Риск и Контрол Само-оценка.

(3) Отделите сами идентифицират Съществените Рискови Показатели, свързани с тяхната дейност с помощта на звеното по управление на риска.

(4) След оценката на Съществените Рискови Показатели, звеното по управление на риска и функционалните единици определят реалистични нива на рискова поносимост.

(5) При възникване/констатиране на Съществени Рискови Показатели отдела по управление на риска уведомява лицата по чл. 4.

III. ПЛАН ЗА ДЕЙСТВИЕ ПРИ ВЪЗНИКВАНЕ НА КРИЗИСНИ СИТУАЦИИ

Чл. 22. (1) Планът за действие при кризисни ситуации установява процедурите по възстановяване работоспособността на информационните и комуникационни системи на УД и на организацията като цяло в случаите на възникване на извънредни неблагоприятни обстоятелства. Планът за действие в кризисни ситуации е неразделна част от политиката по управление на риска и непосредствен резултат от процедурите по установяване, оценка, наблюдение и управление на рисковете в УД. Планът има за цел да сведе до минимум времето на прекъсване на обичайните бизнес-процеси и да предпази критичните за дейността на организацията функционални и информационни центрове от отрицателните въздействия на възникнали кризисни ситуации.

(2) Кризисни ситуации са ситуациите, които имат за резултат прекъсване бизнес-процесите в УД, загуба или нанасяне на щети върху съоръжения, функционален или информационен център на УД, загуба на персонал и др. Без да се изчерпват, кризисните ситуации се свеждат до:

- Пожари, земетресения, наводнения и други природни бедствия;
- Спиране на тока, прекъсване на комуникациите, срив на хардуерни системи, срив на софтуерни системи, нарушаване на конфиденциалността, интегритета и достъпа до фирмените бази данни и др.;
- Терористични атаки, заплахи.

(3) УД изготвя план за действие за всяка идентифицирана кризисна ситуация или заплаха.

1. Планът за действие в кризисни ситуации има следните основни цели, в зависимост от конкретната ситуация:

- в случай на природно бедствие – запазване, доколкото е възможно, на работоспособността на информационните и комуникационни системи на УД и на информацията и последващото им възстановяване в случай на загуби;

- в случай на срив на телекомуникационните системи- поддържане на дейностите по управление на клиентски портфейли и предоставяне на инвестиционни консултации за периода на времетраене на срива в телекомуникационните системи;

- в случай на срив на хардуерните или софтуерните системи – възстановяване на изгубената информация;

- в случай на нарушаване на конфиденциалността и изтичане на информация – минимизиране на възможните загуби за клиентите и за самото УД и предотвратяване на последващо неоторизирано разкриване на информация;

- в случай на терористична заплаха и/или атака – своевременна евакуация на персонала на УД; прехвърляне на информацията, съхранявана от управляващото дружество, на носители, които не са застрашени от атаката/заплахата, с цел предотвратяване на изгубването/унищожаването ѝ.

2. Имената на лицата, запознати с процедурите за действие в плана за действие при възникване на кризисни ситуации, са посочени в Приложение №3 към настоящите правила.

3. Представяващият/ите управляващото дружество са овластени да се разпореждат със системата в случай на кризисна ситуация. Дейностите по преодоляване на възникнала кризисна ситуация се ръководят от Изпълнителния директор на УД.

4. Изпълнителният директор на УД следи действията и процедурите, предвидени в плана, да се изпълняват от лица с нужната квалификация.

5. Факторите, които могат да доведат до кризисна ситуация, са включително, но не само следните:

- земетресение, пожар, наводнение или друго природно бедствие;

- срив на телефонните линии, на факс/принтер линиите; прекъсвания на електрозахранването (пълно или частично); физически повреди на телекомуникационните линии;

- грешки в софтуерните системи;
- кражби/подправяне на информация от персонала на УД или от външни лица; разкриване на конфиденциална информация на неоторизирани лица;
- нападение на помещенията и/или персонала на УД; отправяне на заплаха за извършване на терористичен атентат.

6. Показателите, които сигнализират за възникване на кризисна ситуация, са включително, но не само следните:

- по-слаби или по-силни земни трусове, проникване на вода или течове в помещенията на УД или възникване на пожар;
- спад в броя на входящи обаждания; трудности или невъзможност за извършване на изходящо обаждане; невъзможност за отпечатване на справки/отчети; невъзможност на модемите да установят връзка; получаване на съобщения за невъзможност за изпращане/получаване на факс съобщения;
- установяване наличието на информация, която е конфиденциална, в пресата или възпроизвеждане на такава информация от други средства за масово осведомяване; установяване знанието на конфиденциална информация от неоторизирани лица; установяване на пробиви в информационните системи на УД;
- получаване на заплахи за атаки/атентати срещу УД и/или негови служители.

7. В зависимост от характера и вида на възникналата кризисна ситуация, могат да бъдат засегнати следните звена, процеси и съоръжения:

- в случай на природно бедствие – всички звена и системи на УД, както и материалната база;
- в случай на срив на телекомуникационните системи- комуникациите вътре в организацията, както и комуникациите с клиенти и/или доставчици на УД;
- в случай на срив на хардуерните или софтуерните системи- събирането, въвеждането и осчетоводяването на данни; подаването на информация към или от клиентите и/или генерирането на информация;
- в случай на нарушаване на конфиденциалността и изтичане на информация- базите данни на УД и процесът по съхранение на информация;
- в случай на терористична заплаха и/или атака всички звена на УД и неговата материална база, както и цялата извършвана от УД дейност.

8. Целевият времеви интервал за възстановяване на системата е 1 (един) час, считано от появата на един или повече от показателите, които сигнализират за възникване на кризисна ситуация. След изтичане на времето по предходното изречение се пристъпва към изпълнението на Плана с цел избягване на сериозни смущения в бизнес процесите.

9. Отговорните длъжностни лица, които следва да бъдат уведомени при възникването на кризисна ситуация, са Изпълнителният директор на УД и другите лица, представляващи УД (ако има такива), ръководителят на отдела за вътрешен контрол, както и ИТ специалистите, отговарящи за поддръжката на хардуерните и/или софтуерните системи на УД.

10. Уведомяването на отговорните длъжностни лица се осъществява чрез използването на мобилни телефони и вътрешни телефонни линии, както и чрез изпращане на e-mail или факс в случай, че не е възможно осъществяването на телефонно обаждане.

11. Отговорните длъжностни лица в УД извършват проверка на резервните ресурси и/или съоръжения (генератори, UPS системи, хранилища за документи и др.) и при необходимост предприемат действия за възстановяване на тяхната функционалност.

12. При възникване на кризисна ситуация, компетентните длъжностни лица на УД предприемат следните действия за справяне със ситуацията:

- при възможност дават оценка за очакваната продължителност на действие на възникналата ситуация;
- дадената оценка за продължителността на действие се сравнява с целевия интервал за възстановяване на системата;
- ако очакваната продължителност на действие на кризисната ситуация е по-малка целевия интервал за възстановяване на системата, започва дейност по мониторинг на кризисната ситуация;
- ако очакваната продължителност на действие на кризисната ситуация е по-голяма целевия интервал за възстановяване на системата, започват първоначални дейности по справяне с кризисната ситуация.

13. Дейностите по мониторинг на кризисната ситуация са включително, но не само следните:

- определяне на процедури за нормално провеждане на бизнес операциите до отминаване на кризисната ситуация;
- определяне на лицата и отговорностите по извършване на процедурите.

14. Първоначални дейности по справяне с кризисната ситуация са включително, но не само следните:

- определяне на алтернативни дейности за провеждане на бизнес операциите;
- определяне на лицата и отговорностите по извършване на алтернативните дейности.

15. След приключване на първоначалните дейности по т. 14 по-горе се преминава към поддържащи дейности по преодоляване на кризисната ситуация, а именно мониторинг на възникналата кризисна ситуация и периодична оценка на всеки кръгъл час. След изтичане на 6-тия час отговорните длъжностни лица преминават към изпълнение на поддържащите мерки и дейности.

16. Поддържащи дейности за преодоляване на кризисната ситуация, са организиране на работни станции за извършване на рутинните дейности, изготвяне на график за работа на смени и при необходимост възлагане на дейности на външни изпълнители до отминаване на кризисната ситуация. Изпълнителният директор на УД определя служителите и отговорностите им по извършване на поддържащи дейности, в зависимост от характера и обхвата на възникналата кризисна ситуация.

17. При потвърждение, че кризисната ситуация е отминала, започват дейности по възстановяване нормалния ход на бизнес операциите. Лицата, отговорни за изпълнението на Плана, следва да се уверят, че са налице всички предпоставки за безпрепятствено функциониране на системите и звената/отделите в УД. Ръководителят на отдела за вътрешен контрол изисква необходимата информация от отдела по управление на риска и докладва на Изпълнителния директор на УД относно изправността на системите и готовността за функциониране на отделите на УД.

(4) С цел повишаване културата по управление на рискови ситуации и оценка на адекватността и ефективността на предприеманите мерки, УД изготвя Дневник на регистрираните инциденти- Приложение №2 към настоящите правила.

ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

§1. Настоящите Правила за управление на риска са приети на основание чл. 82 от Наредба №38 от 25.07.2007г. за изискванията към дейността на инвестиционните посредници, във връзка с чл.34а от Наредба №26 от 22.03.2006г. за изискванията към дейността на управляващите дружества, на заседание на Съвета на директорите на “Експат Асет Мениджмънт” ЕАД от 24.01.2008 г.

**Съвет на директорите на
“Експат Асет Мениджмънт” ЕАД:**

1. Неделчо Василев Неделчев -
2. Никола Симеонов Янков -
3. Марина Пламенова Тодорова -
4. Драгомир Огнянов Бояджиев -

Приложение №1 към чл. 13, ал. 3

| Ниво 1 | Ниво 2 | Ниво 3 |
|--|---|--|
| Неупълномощени действия | Неупълномощени действия | Неупълномощени одобрения Незаконни сделки Неотчетени сделки Погрешно отчетени сделки Неоторизирана търговия Прехвърляне на пълномощения Съответствие |
| Вътрешни криминални действия | Кражби и измами от страна на персонала | Нарушение на задължения по договор Нарушение на дължима грижа при изпълнение на договор за доверително управление Нарушаване на патент Дискриминация при предоставяне услуги на клиенти Нарушение на законодаелството Злоупотреба, незаконно присвояване Фалшифициране и подправяне на документи от страна на персонала Кражба от страна на персонала Изнудване Отвличане за откуп от страна на персонала Избягване или заобикаляне на данъчни задължения Подкуп Злоупотреба с вътрешна информация Други вътрешни криминални действия |
| Срив на системите за информационна сигурност | Вътрешни системи за сигурност | Компютърна измама от страна на персонала Непозволен достъп в системата от страна на персонала Манипулиране на вътрешните системи от страна на персонала Компютърна измама от външни лица Непозволен достъп в системата от външни лица Манипулиране на системите от външни лица |
| Криминални действия на външни лица | Кражби и измами на външни лица | Фалшифициране и подправяне на документи от външни лица Неоповестяване на задължителна информация от страна на клиента Кражба от външни лица Изнудване от външни лица Отвличане и искане за откуп – от външни лица Подкуп – от външни лица Палеж – от външни лица Заплахи Терористични действия Вандализъм Индустриален шпионаж от външни лица Други криминални действия на външни лица |
| Отношения с персонала и работна среда | Отношения с персонала Безопасност на трудовата среда Различия и дискриминация | Стачни действия от страна на служителите Неправомерно прекратяване на трудов договор Конфликти между служители Неправомерни действия срещу служители Безопасност на работната среда Сексуален тормоз Дискриминация |
| Клиенти, продукти, услуги и търговска практика | Подходящи услуги, разкриване на информация и доверително управление | Конфликт с клиенти Неправомерни действия срещу клиенти Подвеждащи търговски практики и прикриване на съществена информация Регулаторни отношения Нарушение на установени правила Неправилно тълкуване на информация Други |

| Ниво 1 | Ниво 2 | Ниво 3 | | |
|------------------------------|--|--|---------|--------------------------|
| | Неподходящи бизнес и пазарни практики | Злоупотреба с вътрешна информация | | |
| | | Пазарна манипулация | | |
| | | Пране на пари | | |
| | | Антитръст | | |
| | | Други | | |
| | Грешки на продукти/услуги | Неразкриване на съществена информация | | |
| | | Неуместен продукт | | |
| | | Погрешен модел | | |
| | Подбор и експозиция към клиенти | Пропуски в интерпретирането на информация за клиента | | |
| | | Нарушение на лимит към клиент | | |
| Консултантски услуги | Конфликт при предоставяне на консултация | | | |
| Нарушения на дейността | Природни бедствия и други сътресения | Земетресение | | |
| | | Наводнение | | |
| | | Свличане | | |
| | | Светкавица | | |
| | | Буря | | |
| | | Торнадо | | |
| | | Други природни бедствия | | |
| | | Стълкновения | | |
| | | Експлозия | | |
| | | Пожар | | |
| | | Срив на системите | Системи | Системна инфраструктура |
| | | | | Мрежи |
| | | | | Морално остарели системи |
| Срив на хардуерните системи | | | | |
| Грешки в софтуерните системи | | | | |
| Развитие на системите | | | | |
| Износени хардуер | | | | |
| Нарушения във връзките | | | | |
| Проблеми в инфраструктурата | | | | |

| Описание на събитието: | | | |
|------------------------|-----|------------------------------------|---------------------------------|
| Местоположение: | | | |
| Дата | Час | Лице, регистрирало инцидента | Отговорно лице/Изпълнени задачи |
| | | | |

Приложение №3 към чл. 22, ал. 3, т. 2

Имена на лицата, запознати с процедурите за действие в плана за действие при възникване на кризисни ситуации:

Никола Янков – Председател на СД;
Неделчо Неделчев – Изпълнителен директор;
Марина Тодорова – Член на СД;
Драгомир Бояджиев – Прокурисит и Портфолио мениджър;
Петя Лазарова – Ръководител отдел Вътрешен контрол;
Светла Дечева – Главен счетоводител;
Тереза Трифонова – Инвестиционен консултант;
Виктория Андреева – Бек-офис.