

ПРАВИЛА ЗА УПРАВЛЕНИЕ НА РИСКА НА УПРАВЛЯВАЩО ДРУЖЕСТВО “ЕФ АСЕТ МЕНИДЖМЪНТ” АД

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 “ЕФ Асет Мениджмънт” АД (по-долу “управляващото дружество” или само “УД”) услуги съгласно Закона за дейността на колективните инвестиционни схеми и на други предприятия за колективно инвестиране (ЗДКИСДПКИ).

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 констатираните 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. (1) Съветът на директорите има следните отговорности по управление на риска:

1. Приема правила за управление на риска и следи за тяхната актуализация.

2. (нова, приета с решение на СД от 13.05.2020 г.) Определя рисковата политика на договорните фондове и националните договорни фондове при създаването им.
3. (нова, приета с решение на СД от 13.05.2020 г.) Взема решения за кадрово, софтуерно и друго осигуряване на дейностите по управление на риска.
4. (нова, приета с решение на СД от 13.05.2020 г.) Съвместно с отдела по управление на риска УД следи за текущо за спазването на тези правила и издава заповеди за съобразяване с тях до служителите на УД в случай, че това се налага, като участва активно в процеса по управление на риска.
5. (нова, приета с решение на СД от 13.05.2020 г.) Компетентен е да взема решения относно намаляване на позиции, заемани по решение на инвестиционния консултант и за промяна в диверсификацията на активите на договорните фондове и националните договорни фондове в рамките на инвестиционната политика, залегнала в проспекта на фондовете.

(2) (изм. с решение на СД от 13.05.2020 г., предишна т. 2 и от 11.09.2020 г.) Най-малко веднъж годишно преглежда и оценява правилата за управление на риска на КИС/НИФ, като при непълноти и/или необходимост от подобряване на управлението на риска приема изменения и допълнения в правилата, като не по-късно от 7 дни след датата на приемането им ги представя в КФН за одобрение по реда на чл. 18, ал. 1 и 2 и чл. 179 от Закона за дейността на колективните инвестиционни схеми и на други предприятия за колективно инвестиране (ЗДКИСДПКИ).

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. (изм. с решение на СД от 13.05.2020 г.) Следят за съответствие на използваните от съответните служители 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. (нова, приета с решение на СД от 13.05.2020 г.) Създава организация на работата, която осигурява контрол и спазването на определените лимити и нива на риск на договорните и националните договорни фондове, управлявани от управляващото дружество.

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 СД веднъж годишно доклад за дейността на отдела през годината, в който посочва констатираните непълноти и несъответствия в политиката и процедурите и мерките по чл. 1, т. 2, както и предприетите мерки за отстраняването им.
3. Независимо от изискването по т. 2, Отдел „Управление на риска“ докладва на СД относно нужда от изменения и допълнения в правилата при констатиране на необходимост от това.

4. (нова, приета с решение на СД от 13.05.2020 г.) Консултира СД на УД относно определянето на рисковия профил на клиентите.
5. (нова, приета с решение на СД от 13.05.2020 г.) докладва редовно пред СД на УД и на лицата, осъществяващи надзорни функции, когато е приложимо, относно:
- съответствието между текущото ниво на риск, на което са изложени управляваните от него КИС и НИФ и одобрените им рискови профили;
 - съответствието на КИС и НИФ с вътрешната им система за ограничаване на риска;
 - адекватността и ефективността на процеса за управление на риска и по-специално показващ дали са предприети подходящи коригиращи мерки в случаите, когато са констатирани недостатъци;
6. (нова, приета с решение на СД от 13.05.2020 г.) докладва редовно пред СД, представяйки текущото ниво на риск, на което са изложени КИС и НИФ и за текущите или предвиджани нарушения на ограниченията, като по този начин се осигурява предприемането на навременни и подходящи действия, включително с нормативно определените лимити за общата рискова експозиция и риска на насрещната страна по чл. 46-48, чл. 166, ал. 6 и 11 от Наредба № 44 за изискванията към дейността на колективните инвестиционни схеми, инвестиционните дружества от затворен тип и управляващите дружества (Наредба № 44) ;
7. (нова, приета с решение на СД от 13.05.2020 г.) извършва преглед и подпомага организацията и процедурите за оценка на извънборсовите деривативи по чл. 49 от Наредба №44.
8. (нова, приета с решение на СД от 13.05.2020 г.) Участва в ежедневните процеси по планиране, наблюдение, управление и контрол на рисковете.
- 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 “ЕФ АСЕТ МЕНИДЖМЪНТ” АД

Чл. 7. (изм. с решение на СД от 13.05.2020 г.) 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 политика е да се документират процедурите по установяване, управление, наблюдение и оценка на рисковете, свързани с дейностите, процедурите и системите на УД по реда на ЗДКИСДПКИ и на Наредба № 44.

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

1. Вътрешни - свързани с организацията на работа на УД. 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 УД. Външните рискове се състоят, без да се ограничават до:

- а) Риск на обкръжаващата среда;
б) Риск от физическо вмешателство;
(2) (нова, приета с решение на СД от 13.05.2020 г.) Рисковете се оценяват с една от следните оценки:
1. Нисък – когато всички рискове са покрити с адекватни контролни процедури с висока ефективност и липсват или са налице незначителни отклонения;
2. Среден – когато всички рискове са покрити в известна степен с контролни процедури с недостатъчна ефективност;
3. Висок – когато не всички рискове са покрити с контролни процедури и/или процедурите на предварителния контрол липсват или недействат ефективно, в резултат, на което е нарушено спазването на принципите на добро управление и прозрачност.
(3) (изм., приета с решение на СД от 13.05.2020 г., предишна ал. 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, като служителите, работещи в УД оказват пълно съдействие на отдела за управление на риска.
(4) (предишна ал. 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 УД;
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 УД 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 УД;
7. (нова, приета с решение на СД от 13.05.2020 г.) Извършване на начален и периодичен инструктаж по безопасни условия на труд.

Чл. 10. (1) (Изм. с решение на СД от 13.05.2020 г.) Рискове, свързани с процесите са рисковете, възникващи от накърняване интереса на клиента в резултат на:

1. (изм. с решение на СД от 13.05.2020 г.) Действия в нарушение на определената в Правилата на КИС и НИФ инвестиционна стратегия;
 2. (изм. с решение на СД от 13.05.2020 г.) Извършване на транзакции с инструменти, с които клиента няма право да търгува;
 3. (изм. с решение на СД от 13.05.2020 г.) Недобросъвестно използване на конфиденциална информация, предоставена от клиента (неупълномощен достъп до поверителна информация на клиента), нарушаване на търговска тайна;
 4. Злоупотреба с конфиденциална информация;
 5. Конфликт на интереси;
 6. Грешки при събиране, въвеждане и осчетоводяване на данни;
 7. (изм. с решение на СД от 13.05.2020 г.) Действие в нарушение на политиката за действие в най-добър интерес на клиента;
 8. (изм. с решение на СД от 13.05.2020 г.) Грешки при подаване на информация към клиента;
 9. (изм. с решение на СД от 13.05.2020 г.) Грешки при преценка на активите на клиента;
 10. (изм. с решение на СД от 13.05.2020 г.) Неправилна отчетност и съхранение на активи на клиента;
 11. (нова, приета с решение на СД от 13.05.2020 г. и от 11.09.2020 г.) Виновно причинени вреди, които са в пряка причинна връзка с предоставяне на неверни, неточни или непълни анализи и прогнози в конкретна инвестиционна консултация.
 12. (нова, приета с решение на СД от 11.09.2020 г.) Възможни загуби поради неправилно структуриране на инвестиционния портфейл от финансови инструменти.
 13. (нова, приета с решение на СД от 11.09.2020 г.) Възможни загуби поради липса на достатъчна диверсификация на инвестиционния портфейл от финансови инструменти.
- (2) Процедурите/мерките за управление на рисковете, свързани с процесите, включват:**
1. (изм. с решение на СД от 13.05.2020 г.) Изчерпателно и максимално точно регламентиране на обхвата на управлението и конкретните сделки и действия, които УД е възможно да извършва за сметка на клиента в съответствие с Правилата на клиента (КИС и НИФ);
 2. (изм. с решение на СД от 13.05.2020 г.) УД гарантира, че за всяка сделка, свързана с портфейла на КИС и НИФ, незабавно се извършва запис на информацията, необходима за възпроизвеждане на подробностите по отношение на поръчката и на извършената сделка. Записът съдържа най-малко информацията по чл. 137, ал. 2 от Наредба № 44. Съхраняването на информацията за записите се извършва по реда на чл. 68 от Наредба № 44.
 3. (изм. с решение на СД от 13.05.2020 г.) 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 управляваните КИС и НИФ, от друга страна;
 - всяка от управляваните КИС и НИФ, като в случай че въпреки прилагането на правилата за вътрешната организация на управляващото дружество продължава да съществува риск за интересите на някоя от управляваните схеми, фондове, УД предприема адекватни мерки в зависимост от случая.
 4. УД приема ефективни процедури и мерки за третиране на конфликт на интереси, уредени в Правила за личните сделки с финансови инструменти и за установяване,

разкриване и предотвратяване на конфликти на интереси, със съдържание в съответствие с действащото законодателство и добрите международни практики;

5. (изм. с решение на СД от 13.05.2020 г.) УД прилага подходящи мерки за отделяне на собствения портфейл от финансови инструменти и парични средства от тези на клиентите, чрез които не се допуска смесване. УД приема и прилага Правила за инвестиране на собствени средства.

6. (изм. с решение на СД от 13.05.2020 г.) УД приема Политика за действие в най-добър интерес на клиента, която му позволява да получи най-добър резултат за клиента във връзка с дейността по управление на неговия портфейл.

7. (изм. с решение на СД от 13.05.2020 г.) 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 упражняват дейност по управление на портфейли, извършват финансови и други анализи, както и останалите определени от УД лица, които имат достъп до такъв тип информация, ще пазят търговските и други тайни на клиентите на УД и търговския им 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 УД 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;
7. (нова, приета с решение на СД от 13.05.2020 г.) Употреба на мониторинг системи за нападения (IDS, Intrusion Detection System);
8. (нова, приета с решение на СД от 13.05.2020 г.) Употреба на системи за агрегиране и анализ на логове;

9. (нова, приета с решение на СД от 13.05.2020 г.) Използване на високо надеждни доставчици на софтуерни архитектури и алтернативни комуникационни канали и технологии;
10. (нова, приета с решение на СД от 13.05.2020 г.) Употреба на системи за мониторинг в реално време.

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 УД в съответствие с нормативните изисквания.
2. (изм. с решение на СД от 13.05.2020 г.) При встъпване в трайни отношения (склучване на договор) УД извършва идентификация на клиента в съответствие с изискванията на Закона за мерките срещу изпирането на пари и Закона за мерките срещу финансирането на тероризма, 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. (изм. с решение на СД от 13.05.2020 г.) 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 (която е неразделна част от Политиката на управляващо дружество "ЕФ Асет Мениджмънт" АД за действие в най-добър интерес на клиентите) веднъж годишно, както и при всяка съществена промяна, която може да се отрази на възможността на УД да осигурява най-добри резултати за клиентите.

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. Осигуряване на охрана и 24-часово наблюдение и контрол на помещенията, в които се намират технологичните средства и архивите на УД;

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 УД;
 4. Процедура за докладване на инциденти.
- (3) Детайлна категоризация на рисковете се съдържа в Приложение 1.

Чл. 14. Процедура за идентификация, оценка и контрол на риска. Процедурата по идентификация, оценка и контрол на риск обхваща следните 4 фази:

1. Идентификация на рисковете – контрол и самооценка на риска, идентификация на рисковете, които не са обект на контрол.
2. Оценка на риска – оценка на честота на настъпване и степента на въздействие на рисковете, както и промяна в нивата на риск:
 - а) Отчитане на „съществени рискови показатели“;
 - б) Отчитане за настъпили инциденти.
3. Наблюдение на риска – наблюдение на неприемливите рискове, промяна в рисковете/рисковите нива и процеси за управление на риска от:
 - а) отдел „Управление на риска“;
 - б) Съвет на директорите;
4. (изм. с решение на СД от 13.05.2020 г.)Намаляване на риска – управление за намаляване на риска, съобразно допустимото ниво на риск чрез:
 - а) проследяване на открития риск при извършване при необходимост на проверки от регистрирани одитори;
 - б) установяване на контролни стандарти;
 - в) застраховане срещу определени рискове.

Чл. 15. Идентификация на риска - идентификацията на риска започва с вътрешно за всяко звено изследване, което представлява дейност по установяване на факти. За целта, всеки отдел се задължава да информира по подходящ начин ръководителя на отдел „Управление на риска“ относно броя на засечените инциденти, както и информация за размера на понесените щети, в случаите когато е налична информация за това.

Чл. 16. (1) Контрол и самооценка на риска. Целта на процеса по „контрол и самооценка на риска“ е:

1. да се подобри навременното 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) Резултатите от процеса по „контрол и самооценка на риска“ се използват за определянето на „съществени рискови показатели“ за отделните бизнес функции.

Чл. 17. (1) Оценка на риска - действията, които се предприемат в тази фаза се предопределят от резултатите получени във фазата по 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.

(3) Съгласно тази оценка, 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 ѝ 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, Нормативно съответствие 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 на 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 „контрол и самооценка на риска.“

- (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 възникването/констатирането на „съществените рискови показатели“ отдела по управление на риска уведомява лицата по чл. 4.

IV. 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 ситуацията, които имат за резултат прекъсване на 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, срыв на хардуерни системи, срыв на софтуерни системи, нарушаване на конфиденциалността, интегритета и достъпа до фирмените бази данни и др.;
- Терористични атаки, заплахи;
- Разрастваща се епидемична заплаха;
- Обявено в Република България извънредно и/или военно положение.

(3) (Изм. с решение на СД от 13.05.2020 г.) 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 срыв на телекомуникационните системи - поддържане на дейностите по управление на клиентски портфейли за периода на времетраене на срыва в телекомуникационните системи;
- в случай на срыв на хардуерните или софтуерните системи – възстановяване на изгубената информация;
- в случай на нарушаване на конфиденциалността и изтичане на информация – минимизиране на възможните загуби за УД и за клиентите и предотвратяване на последващо неототоризирано разкриване на информация;
- в случай на терористична заплаха и/или атака – своевременна евакуация на персонала на УД; прехвърляне на информацията, съхранявана от УД, на носители, които

не са застрашени от атаката/заплахата, с цел предотвратяване на изгубването/унищожаването ѝ.

2. Лицата, запознати с процедурите за действие в плана за действие при възникване на кризисни ситуации, са посочени в Приложение 3 към настоящите правила.

3. Представляващият/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/те директор/и на УД.

4. Изпълнителният/те директор/и 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;
- отправка 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 2 (два) часа, 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 Нормативно съответствие, 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 организирани 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.

(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 са приети с решение на Съвета на директорите на „ЕФ Асет Мениджмънт“ АД от 17.07.2013 г. и отменят всички предходни правила уреждащи аналогична материя. Настоящите правила са изменени с решение на Съвета на директорите на „ЕФ Асет Мениджмънт“ АД от 13.05.2020 г. и от 11.09.2020 г.

за УД “ЕФ Асет Мениджмънт” АД:

Иван Овчаров
/Изпълнителен директор/

Ивелина Иванова
/ Прокуриснт/

**Приложение №1 към чл. 13, ал. 3
(изм. с решение на СД от 13.05.2020 г.)**

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 управление на портфейл
		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
Криминални действия на външни лица	Кражби и измами на външни лица	Манипулиране на системите от 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	Стачни действия от страна на служителите Неправомерно прекратяване на трудов договор Конфликти между служители Неправомерни действия срещу служители
	Безопасност на трудовата среда	Безопасност на работната среда
	Различия и дискриминация	Сексуален тормоз Дискриминация
Клиенти, продукти, услуги и търговска практика	Подходящи услуги и разкриване на информация	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
	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
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



EF Asset Management AD
Tel.: + 359 (02) 9021 944
office@efam.bg

43 Christopher Columbus Blvd. 1592 Sofia, Bulgaria
Fax: +359 (0) 2 981 14 96
www.efam.bg

Приложение № 2 към чл. 22, ал. 4

Дневник на настъпили инциденти

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



EF Asset Management AD
Tel.: + 359 (02) 9021 944
office@efam.bg

43 Christopher Columbus Blvd. 1592 Sofia, Bulgaria
Fax: +359 (0) 2 981 14 96
www.efam.bg

Приложение № 3 към чл. 22, ал. 3, т. 2

Лицата, запознати с процедурите за действие в плана за действие при възникване на кризисни ситуации.

Длъжност	e-mail	Личен телефон
Изпълнителен директор	i.ovcharov@efam.bg	02/9021937
Ръководител Нормативно съответствие	office@efam.bg	02/9021944