ПРАВИЛА ЗА УПРАВЛЕНИЕ НА РИСКА НА УД “АЛФА 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 “Алфа Асет Мениджмънт” ЕАД (по-долу “Управляващото дружество” или само “УД”) услуги.

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 т. а) и върху спазването от управляващото дружество и лицата, които работят по договор за управляващото дружество, на процедурите и мерките по т. 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. Изпълнителен директор.

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 както и последващите им актуализации.

2. Най-малко веднъж годишно преглежда и оценява правилата, като при непълноти и/или необходимост от подобряване на управлението на риска приема изменения и допълнения в правилата.

Чл. 4. Изпълнителният директор има следните отговорности по управлението на риска:

1. Организира работата по правилно провеждане на приетата от Съвета на директорите политика по управление на риска.

2. Следи 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. Взема решения за кадрово, материално-техническо и методическо осигуряване на дейностите по управление на риска.

Чл. 5. Отдел „Контрол и управление на риска“ действа независимо от другите звена в управляващото дружество, отчита се пряко пред изпълнителния директор, а при необходимост и пред Съвета на директорите, 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, процедурите и мерките по чл. 1, т. 2, както и предприетите мерки за отстраняването им.

Чл. 6. Служители, 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*

Чл. 7. (1) Политиката по управление на риска е част от вътрешноорганизационната стурктура на УД действа и се прилага интегрирано с всички вътрешно-нормативни документи на дружеството. (2) Целта на настоящата политика е да се документират процедурите по установяване, управление, наблюдение и оценка на рисковете, свързани с дейността на УД по реда на Наредба № 44 от 20.11.2011 г. за изискванията към дейността колективните инвестиционни схеми, инвестиционните дружества от затворен тип и на управляващите дружества.

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 по 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, свързани със загуби от:

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) Процедури/мерки за управление на рисковете, свързани с персонала включват:

1. Ясно дефиниране на вътрешни правила относно правата и задълженията на служителите, както и изготвяне и запознаване на служителите с индивидуални длъжностни характеристики;

2. Ясно дефинирани нива 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;

7. Извършване на начален и периодичен инструктаж, свързан с безопасните условия на труд

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

1. Действия в нарушение на определената инвестиционна стратегия;

2. Неправилна преценка за рисковия профил на клиента и избор на неподходяща и неуместна за клиента инвестиционна стратегия;

3. Виновно причинени вреди, които са в пряка причинна връзка с предоставяне на неверни, неточни или непълни анализи и прогнози в конкретна инвестиционна консултация;

4. Извършване на транзакции с инструменти, с които Клиента няма право да търгува;

5. Недобросъвестно използване на поверителна информация, предоставена от клиента (неупълномощен достъп до поверителна информация на клиента), нарушаване на търговска тайна;

6. Злоупотреба с поверителна 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) Процедури/мерки за управление на рисковете, свързани с процесите, включват:

1. Изчерпателно и максимално точно уговаряне в договорните отношения с клиента обхватът на управлението и конкретните сделки и действия, които УД е овластено да извършва;

2. С цел коректната оценка на рисковия профил на клиента УД класифицира клиентите си съгласно Методика за определяне на клиентите като професионални, непрофесионални или приемлива насрещна страна.

3. Изискване към клиентите и потенциалните клиенти 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. При промяна на горепосочените факти Клиента се задължава своевременно да уведоми УД.

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.

5. Предварително подробно запознаване на клиентите с вида и характеристиките на конкретния вид финансов инструмент и на конкретните рискове, свързани с него;

6. Разработване на система за отчитане пред клиента в съответствие с профила на клиента и законоустановените изисквания, която да гарантира навременното и точно подаване на изискуемата информация. При предоставя на информация до клиента, УД се стреми да предоставя максимално релевантна такава, която да осигури на клиента възможност да направи преценка за обекта инвестициите.

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

8. УД приема ефективни процедури и мерки за третиране на конфликт на интереси, съгласно чл. 127 и чл. 148 от Наредба 44 от 01.11.2011 г. за изискванията към дейността на колективните инвестиционни схеми, инвестиционните дружества от затворен тип и управляващите дружества, както и в съответствие с действащото законодателство и добрите международни практики

9. УД прилага подходящи мерки за съхраняване на финансовите инструменти и паричните средства на клиентите и за отделяне на собствения портфейл от финансови инструменти от този на инвеститорите, да отчита отделно паричните средства на клиентите от сделки с финансови инструменти

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 подава нарежданията или на които предава нарежданията за изпълнение

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.

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. Срив на информационните и комуникационни системи.

(2) Процедури/мерки 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 потребителите 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) Рискове на обкръжаващата среда включва:

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 окръжаващата 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 и юридически кантори в случай на необходимост за привеждане на дейността на Управляващото Дружество в съответствие с нормативните изисквания и промените в тях;

2. При встъпване в трайни отношения (сключване на договор), УД извършва идентификация на клиентите в съответствие с изискванията на Закона за мерките срещу изпирането на пари и Закона за финансиране 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 публичните обсъждания по отношение планирани промени в нормативната уредба, касаеща дейността на Управляващото Дружество;

4. При възлагане за изпълнение на съществени функции, УД постоянно следи за ефективността и качеството на изпълнение от страна на лицата, до които УД подава или предава нареждания за изпълнение, и когато е необходимо взема мерки за отстраняване на установени нередности.

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 подходящ начин на 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 всички видове рискове се съдържа в Приложение 1, неразделна част от настоящите правила.

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 – риск и контрол самооценка, 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:

а) отдел „Контрол и управление на риска“;

б) Съвет на директорите;

4. Намаляване на риска – управление за намаляване на риска, съобразно допустимото ниво на риск:

а) проследяване на открития риск при извършване на проверки от регистрирани одитори;

б) установяване на контролни стандарти;

в) застраховане срещу риска.

Чл. 15. (1) Идентификация на риска – в тази фаза 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. 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 „Контрол и управление на риска” относно броя на засечените инциденти, както и информация за размера на понесените щети, в случаите когато е налична информация за това.

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

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

Чл. 16. (1) Риск и Контрол Самооценка. Целта на процеса по Риск и Контрол Самооценката 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) Процесът по Риск и Контрол Само-оценка е периодичен. 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, междувременно ограничени или невалидни.

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

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.

(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 предприемане на ограничителните мерки.

(2) Ограничаването на риска се налага в случаите когато, идентифицираните нива на риск надхвърлят приетите за допустими. Ограничаването може да бъде осъществено по няколко начина, някои от които са: често / обичайно вероятно случайно рядко малко вероятно слабо умерено критично катастрофично незначително степен на въздействие честота на възникване

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 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 отдел „Контрол и управление на риска“

(4) Последната стъпка е 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. Отделът по “Контрол и управление на риска” подпомага внедряването на контролните механизми и установяването на вътрешни контролни стандарти. Отговорните лица се отчитат пред отдела за управление на риска.

Чл. 20. (1) Отчитане на настъпили инциденти – отчитането на настъпили инциденти цели:

1. да спомага за формирането на информационна база за загуби, предизвикани от операционни инциденти;

2. да спомага за увеличаване на риск културата, съответно подобряване на процеса по управление на риска и възможностите за ограничаване чрез подобряване на информацията за действителната цена на операционния риск;

3. периодично да измерва стойността на възникващите следствие операционен риск инциденти, осигурявайки по-добра възможност на мениджмънта за ограничаване на разходите;

4. да подобри възможността за реагиране при значителни операционни инциденти;

5. да приведе в съответствия изискванията на нормативната уредба на ниво функционална единица.

6. да създаде изцяло синхронизирана процедура за събиране на данни и отчитане, както и избягване на дублиране на информация и празноти.

(2) 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. Отчитане на Съществените Рискови Показатели:

1. Съществените Рискови 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 Самооценка;

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, отделът за управление на риска и функционалните единици определят реалистични нива на рискова поносимост;

5. Съветът на директорите се уведомява при възникването/констатирането на Съществени рискови показатели.

IV. ПЛАН ЗА ДЕЙСТВИЕ ПРИ ВЪЗНИКВАНЕ НА КРИЗИСНИ СИТУАЦИИ

Чл. 22. (1) Основни положения: 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.

1. 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.

2. Планът има за цел да сведе до минумум времето на прекъсване на обичайните бизнес-процеси и да предпази критичните за дейността на организацията функционални/информационни центрове от отрицателните въздействия на възникнали кризисни ситуации.

(2) Дефиниране на кризисни ситуации. Като кризисни ситуации се определя тези, които имат за резултат прекъсване бизнес-процесите в УД, загуба/нанасяне на щети върху съоръжения, функционален/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) Конструктивни елементи на Плана за действие в кризисни ситуации:

1. Основна цел на плана: кратко описание на целите на плана.
    - в случай на срив във телекомуникационните системи това може да бъде: "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 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 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. Запознати лица: списък на лицата (вътрешни или външни за организацията), които със запознати с процедурите за действие в настоящия план и техните координати за връзка.

3. Лица, отговорни за изпълнение на плана:

а) Определяне на лицето/лицата, които разполагат с правомощия за разпореждане със системата в случай на кризисна ситуация, както и лицето/лицата, които ще ръководят дейностите по преодоляване на възникналата ситуация – обикновено това е изпълнителния директор на УД.

б) Определяне на лицето/лицата, които ще следят за това описаните в плана процедури и действия да се изпълняват от достатъчно квалифициран персонал: това може също да е изпълнителния директор на УД или мениджър от по-висок ранг.

4. Определяне на причините/факторите, които могат да доведат до възникване на кризисна ситуация. Това могат да бъдат, но не само:

а) Срив на телефонните линии/интернет достъп;

б) Срив на факс/принтер линиите;

в) Прекъсвания на електрозахранването: пълно или частично;

г) Физически повреди по телекомуникационните линии;

д) земетресение, пожар, наводнение или друго природно бедствие;

е) грешки в софтуерните системи;

ж) кражби/подправяне на информация от персонала на УД или от външни лица; разкриване на конфиденциална информация на неоторизирани лица;

з) нападение на помещенията и/или персонала на УД; отправяне на заплаха за извършване на терористичен атентат.

5. Определяне на показателите, които сигнализират за възникване на кризисна ситуация. Това могат да бъдат, но не само:

а) Спад в броя на входящи обаждания;

б) Трудности или невъзможност за извършване на изходящо обаждане;

в) Невъзможност за отпечатване на справки/отчети.

г) Невъзможност на модемите да установят връзка.

д) Получаване на съобщения за невъзможност за изпращане/получаване на факс съобщения.

е) по-слаби или по-силни земни трусове, проникване на вода или течове в помещенията на УД или възникване на пожар;

ж) 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;

з) получаване на заплахи за атаки/атентати срещу УД и/или негови служители.

6. Определяне на засегнатите функционални звена, процеси, съоръжения. 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.

7. Определяне на целеви времеви интервал за възстановяване на системата: това е времевият интервал, в който системата се наблюдава и след изтичането на който се пристъпва към изпълнението на настоящия план с цел избягване на сериозни смущения в бизнес процесите.

8. Известяване: изискване на съдействие и уведомяване на отговорните лица. Тази част от плана съдържа лицата (вътрешни или външни за организацията), които следва да бъдат уведомени в случай на възникване на кризисна ситуация и след изтичане на времевия интервал за възстановяване на системата. Това могат да бъдат: пряк ръководител, изпълнителен директор на УД, IT специалист.

9. Изброяване на средствата за известяване: това могат да бъдат мобилни телефони, вътрешни телефонни линии и др.

10. Проверка на резервни ресурси/съоръжения: генератори, UPS системи, хранилища за документи и др. В тази фаза се извършва проверка на състоянието на резервните ресурси съоръжения и при необходимост възстановяване на тяхната функционалност.

11. Първоначални действия по справяне с кризисната ситуация:

а) При възможност оценка на очакваната продължителност на действие на съответната ситуация (А) и сравняване с определения целеви интервал за възстановяване на системата (Б). Ако (А) < (Б), премини към дейностите по мониторинг на кризисната ситуация. Ако (А) > (Б), премини към първоначални дейностите по справяне с кризисната ситуация.

б) Дейности по мониторинг на кризисната ситуация: определяне на процедури за нормално провеждане на бизнес операциите до отминаване на кризисната ситуация. Определяне на лицата и отговорностите по извършване на процедурите.

в) Първоначални дейности по справяне с кризисната ситуация: определяне на алтернативни дейности за провеждане на бизнес операциите. Определяне на лицата и отговорностите по извършване на алтернативните дейности.

12. Поддържащи дейности по преодоляване на кризисната ситуация: мониторинг на ситуацията и периодична оценка на определен интервал от време (например: оценка на ситуацията на всеки кръгъл час. На 6-ия час премини към изпълнение на поддържащите мерки).

а) Поддържащи дейности: 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.

б) Определяне на лицата и отговорностите им по извършване на поддържащи дейности.

13. Фаза на възстановяване на работоспособността на системите/функционалността на съоръженията. При потвърждение, че кризисната ситуация е отминала, следва да се започнат 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. Посочват се лицата, от които да се изисква необходимата информация, както и нивата на нейното докладване.

(4) Оценка на възникналата рискова ситуация и на адекватността и ефективността на предприетите мерки: с цел повишаване културата по управление на рискови ситуации и оценка на адекватността и ефективността на предприманите мерки УД следва да изготвя Дневник на регистрирани инциденти.

Настоящите правила са приети на заседание на Съвета на директорите на Дружеството на 04.03.2016 г.

Приложение 1

Ниво 1	**Ниво 2**	**Ниво 3**
Неупълномощени действия	Неупълномощени действия	Неупълномощени одобрения
		Незаконни сделки
		Неотчетени сделки
		Погрешно отчетени сделки
		Неоторизирана търговия
		Прехвърляне на пълномощия
		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 законодателството
		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	Непозволен достъп в системата от страна на персонала
		Компютърна измама от външни лица
		Манипулиране на вътрешните системи от страна на персонала
		Компютърна измама от страна на персонала

		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	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, 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
	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

Приложение 2

Дневник на настъпили инциденти

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