«ЗАТВЕРДЖЕНО»
Протокол №05/06 засідання Наглядової ради
ПрАТ «СК «ПЕРЕМОГА» від 28.06.2024р.

ПОЛІТИКА
УПРАВЛІННЯ РИЗИКАМИ
ПРИВАТНОГО АКЦІОНЕРНОГО ТОВАРИСТВА
«СТРАХОВА КОМПАНІЯ
« ПЕРЕМОГА »

Київ – 2024

*Ця Політика управління ризиками розроблена з метою забезпечення стабільності та стійкості діяльності ТДВ "Страхова компанія "*ПЕРЕМОГА*" (далі - Товариство). Політика визначає основні принципи, процедури та заходи щодо ідентифікації, оцінки, моніторингу та управління ризиками, яким піддається Товариство у своїй діяльності. Відповідно до вимог чинного законодавства України та міжнародних стандартів, ця Політика спрямована на захист інтересів клієнтів, акціонерів та інших зацікавлених сторін шляхом мінімізації негативного впливу ризиків на фінансовий стан та репутацію Товариства.*

Стаття 1. Мета та завдання політики управління ризиками

1.1. Метою цієї Політики є встановлення єдиних принципів та підходів до управління ризиками в Товаристві.

1.2. Основні завдання включають:

а) Забезпечення фінансової стійкості та безперервності діяльності Товариства;

б) Зниження ймовірності та наслідків реалізації ризиків;

в) Підвищення ефективності процесів управління ризиками.

Стаття 2. Принципи управління ризиками

2.1. Управління ризиками базується на таких принципах:

а) Системність: ризики вивчаються в комплексі, з урахуванням їх взаємозв'язків;

б) Прозорість: всі процеси управління ризиками мають бути відкритими та зрозумілими;

в) Відповідальність: кожен співробітник відповідає за управління ризиками в межах своєї компетенції;

г) Адаптивність: система управління ризиками повинна бути гнучкою та здатною до адаптації в умовах змінного середовища.

Стаття 3. Структура системи управління ризиками

3.1. Система управління ризиками Товариства складається з наступних компонентів:

а) Ідентифікація ризиків - виявлення потенційних ризиків, які можуть вплинути на діяльність Товариства. До цього процесу залучаються всі підрозділи Товариства, які систематично аналізують внутрішнє і зовнішнє середовище для виявлення нових або змінюючих ризиків. Основними інструментами ідентифікації є:

1. Перевірка внутрішніх процесів та процедур.

2. Аналіз зовнішніх факторів, таких як ринкові умови, законодавчі зміни, економічні тенденції.

3. Використання спеціалізованих програмних засобів для автоматичного виявлення ризиків.

4. Проведення регулярних обговорень та воркшопів з метою обміну інформацією між різними підрозділами.

б) Оцінка ризиків - аналіз і визначення ступеня впливу виявлених ризиків на діяльність Товариства. Цей процес включає в себе:

1. Визначення ймовірності виникнення кожного ризику.

2. Оцінку можливих фінансових втрат у разі реалізації ризику.

3. Визначення часу, необхідного для реагування на ризик.

4. Використання кількісних і якісних методів оцінки ризиків, таких як аналіз сценаріїв, моделювання, експертні оцінки.

в) Моніторинг ризиків - постійне спостереження за ідентифікованими ризиками та оцінку їх актуальності. Основними елементами моніторингу є:

1. Регулярний перегляд і оновлення реєстру ризиків.

2. Аналіз змін у внутрішньому і зовнішньому середовищі, які можуть вплинути на ризики.

3. Використання систем раннього попередження для швидкого реагування на нові ризики.

4. Проведення регулярних аудитів і перевірок.

г) Управління ризиками - розробку і впровадження заходів для мінімізації або усунення впливу ризиків на діяльність Товариства. Основними підходами до управління ризиками є:

1. Прийняття ризиків – прийняття ризиків, які не мають значного впливу на діяльність Товариства.

2. Уникнення ризиків – зміна процесів або умов для повного усунення ризиків.

3. Зменшення ризиків – впровадження заходів для зниження ймовірності або впливу ризиків.

4. Передача ризиків – передача ризиків третім особам, наприклад, через перестрахування.

д) Звітування про ризики - регулярне інформування керівництва та відповідних підрозділів про стан ризиків і ефективність заходів щодо їх управління. Основні аспекти звітування включають:

1. Регулярна підготовка звітів про ідентифіковані ризики та їх оцінку.

2. Надання інформації про виконані заходи з управління ризиками.

3. Оцінка ефективності впроваджених заходів і надання рекомендацій щодо покращення процесу управління ризиками.

4. Використання автоматизованих систем для збору, аналізу та звітування про ризики.

3.2. Всі компоненти системи повинні працювати інтегровано та ефективно взаємодіяти між собою.

Стаття 4. Процедури ідентифікації ризиків

4.1. Ідентифікація ризиків включає визначення всіх можливих ризиків, які можуть вплинути на діяльність Товариства.

4.2. Процедури ідентифікації ризиків включають:

а) Аналіз внутрішніх і зовнішніх факторів;

б) Аналіз бізнес-процесів та операцій;

в) Аналіз історичних даних та інцидентів.

Стаття 5. Методи оцінки ризиків

5.1. Оцінка ризиків включає кількісний та якісний аналіз виявлених ризиків.

5.2. Основні методи оцінки ризиків включають:

а) Статистичний аналіз - використовується для оцінки частоти та величини ризиків на основі історичних даних. Включає збір та аналіз даних про попередні випадки ризиків, визначення закономірностей та трендів, які можуть вказувати на майбутні ризики. Використовуються методи регресійного аналізу, кореляційного аналізу та інші статистичні методи;

б*) Експертний аналіз* - здійснюється шляхом опитування фахівців з різних підрозділів Товариства, які мають досвід та знання у сфері управління ризиками. Експерти надають свої оцінки ймовірності та впливу ризиків, а також рекомендації щодо управління ними. Результати експертного аналізу використовуються для доповнення даних статистичного аналізу;

в) Стрес-тестування - моделювання екстремальних ситуацій для оцінки стійкості Товариства до ризиків. Включає створення сценаріїв, які можуть мати значний негативний вплив на діяльність Товариства, і аналіз того, як Товариство буде реагувати на такі події. Стрес-тестування дозволяє виявити слабкі місця та розробити заходи для підвищення стійкості;

г) Аналіз сценаріїв - розробка різних можливих сценаріїв розвитку подій, що можуть вплинути на діяльність Товариства. Сценарії включають як позитивні, так і негативні події, що дозволяє оцінити широкий спектр ризиків. Аналіз сценаріїв допомагає визначити потенційні наслідки ризиків та розробити плани дій на випадок їх настання.

Стаття 6. Процеси моніторингу ризиків

6.1. Моніторинг ризиків здійснюється на постійній основі для своєчасного виявлення змін у ризиковому профілі Товариства.

6.2. Процеси моніторингу включають:

а) Регулярний аналіз даних та показників ризиків;

б) Порівняння поточного стану ризиків з встановленими лімітами;

в) Виявлення відхилень та аналіз їх причин.

Стаття 7. Заходи з управління ризиками

7.1. Управління ризиками включає розробку та впровадження заходів з метою зниження їхнього впливу на діяльність Товариства.

7.2. Основні заходи включають:

а) Уникнення ризиків;

б) Зменшення ризиків;

в) Передача ризиків (перестрахування);

г) Прийняття ризиків на основі визначеного ризикового апетиту.

Стаття 8. Класифікація ризиків

8.1. В Товаристві ідентифіковані наступні основні категорії ризиків:

Стаття 8.1. Фінансові ризики

а) Валютний ризик - ризик зміни вартості активів та зобов'язань унаслідок коливань валютних курсів. Управління валютним ризиком здійснюється через хеджування валютних операцій та диверсифікацію валютного портфеля;

б) Процентний ризик - ризик зміни вартості активів та зобов'язань унаслідок змін процентних ставок. Управління процентним ризиком здійснюється через встановлення лімітів на процентні ставки та використання деривативів для хеджування процентного ризику;

в) Ризик зміни цін на активи - ризик зниження вартості інвестиційних активів унаслідок коливань ринкових умов. Управління цим ризиком здійснюється через диверсифікацію інвестиційного портфеля та моніторинг ринкових умов.

Стаття 8.2. Операційні ризики

а) Ризик втрат унаслідок недоліків або помилок у внутрішніх процесах. Управління цим ризиком здійснюється через впровадження систем внутрішнього контролю та аудиту;

б) Ризик втрат унаслідок дій персоналу. Управління цим ризиком здійснюється через навчання та підвищення кваліфікації персоналу, а також впровадження програм мотивації та контролю за виконанням обов'язків;

в) Ризик втрат унаслідок зовнішніх подій, включаючи шахрайство та техногенні катастрофи. Управління цим ризиком здійснюється через впровадження заходів безпеки та страхування від зовнішніх ризиків.

Стаття 8.3. Стратегічні ризики

а) Ризик втрат унаслідок неправильної стратегії або невідповідності стратегії ринковим умовам. Управління цим ризиком здійснюється через регулярний перегляд та коригування стратегії розвитку Товариства;

б) Ризик втрат унаслідок змін у зовнішньому середовищі, включаючи економічні та політичні зміни. Управління цим ризиком здійснюється через аналіз ринкових умов та впровадження стратегічного планування.

Стаття 8.4. Репутаційні ризики

а) Ризик втрат унаслідок негативного впливу на репутацію Товариства. Управління цим ризиком здійснюється через підтримку високого рівня обслуговування клієнтів, моніторинг громадської думки та впровадження програм корпоративної соціальної відповідальності;

б) Ризик втрат клієнтів та партнерів через втрату довіри до Товариства. Управління цим ризиком здійснюється через прозорість діяльності та регулярне інформування зацікавлених сторін про досягнення та плани Товариства.

Стаття 8.5. Андеррайтинговий ризик

а) Ризик збитку внаслідок неправильного оцінювання страхових зобов'язань. Управління цим ризиком здійснюється через вдосконалення методологій оцінки ризиків, підвищення кваліфікації андеррайтерів та впровадження систем контролю якості андеррайтингу;

б) Ризик недостатності премій та резервів. Управління цим ризиком здійснюється через регулярний перегляд та коригування тарифів та резервів, а також впровадження систем моніторингу та контролю за виконанням андеррайтингових процесів;

в) Ризик виникнення непередбачуваних страхових подій. Управління цим ризиком здійснюється через впровадження програм перестрахування та розробку сценаріїв реагування на можливі страхові події.

Стаття 9. Визначення та затвердження ризикового апетиту

9.1. Ризиковий апетит визначає допустимий рівень ризику, який Товариство готове прийняти у своїй діяльності.

9.2. Визначення ризикового апетиту включає:

а) Встановлення цільових рівнів ризику для кожної категорії ризиків;

б) Визначення допустимих відхилень від цільових рівнів.

9.3. Ризиковий апетит затверджується Наглядовою Радою і переглядається щорічно.

Стаття 10. Встановлення лімітів ризиків

10.1. Ліміти ризиків встановлюються для кожної категорії ризиків та затверджуються Наглядовою Радою.

10.2. Основні види лімітів включають:

а) Ліміти на фінансові ризики: ліміти на валютні, процентні ризики, ризики ліквідності;

б) Ліміти на операційні ризики: ліміти на ризики внутрішніх процесів та систем;

в) Ліміти на стратегічні ризики: ліміти на ризики, пов'язані з реалізацією стратегічних ініціатив.

Стаття 11. Структура ризикового профілю

11.1. Ризиковий профіль включає детальний опис усіх виявлених ризиків, їхніх характеристик та заходів з управління ними.

11.2. Основні компоненти ризикового профілю:

а) Опис ризиків: види ризиків, джерела, ймовірність настання та вплив;

б) Оцінка ризиків: кількісні та якісні показники ризиків;

в) Заходи з управління ризиками: стратегії, плани та процедури.

Стаття 12. Склад та функції Комітету

12.1. Комітет з управління ризиками складається з членів Наглядової Ради та ключових керівників Товариства.

12.2. Функції Комітету включають:

а) Розробку та перегляд політики управління ризиками: Комітет займається розробкою нових політик управління ризиками та регулярним переглядом існуючих, щоб забезпечити їхню відповідність змінним умовам та вимогам;

б) Моніторинг виконання політики: Комітет забезпечує, що всі процеси управління ризиками відповідають затвердженій політиці та встановленим стандартам, здійснюючи регулярний моніторинг та аудит;

в) Оцінка ризиків: Комітет здійснює періодичну оцінку всіх категорій ризиків, використовуючи різні методи аналізу, включаючи статистичний аналіз, експертну оцінку, стрес-тестування та аналіз сценаріїв;

г) Надання рекомендацій щодо управління ризиками: Комітет розробляє рекомендації щодо зниження рівня ризиків, включаючи впровадження нових заходів та коригування існуючих;

д) Взаємодія з головним ризик-менеджером: Комітет тісно співпрацює з головним ризик-менеджером, обговорюючи результати оцінок та плани дій, а також контролює виконання його обов'язків;

е) Затвердження лімітів ризиків: Комітет визначає та затверджує ліміти ризиків для кожної категорії, враховуючи рекомендації головного ризик-менеджера та результати оцінок;

ж) Підготовка звітів для Наглядової Ради: Комітет готує регулярні звіти про стан ризиків, ефективність заходів з управління ризиками та дотримання встановлених лімітів, які подаються на розгляд Наглядовій Раді;

з) Впровадження систем внутрішнього контролю: Комітет розробляє та впроваджує системи внутрішнього контролю для мінімізації операційних ризиків та підвищення ефективності управління ризиками;

и) Організація навчання для співробітників: Комітет забезпечує проведення навчання та підвищення кваліфікації співробітників Товариства у сфері управління ризиками, щоб підвищити їхню обізнаність та компетенції.

Стаття 13. Обов'язки головного ризик-менеджера

13.1. Головний ризик-менеджер відповідає за впровадження та контроль за дотриманням політики управління ризиками.

13.2. Основні обов'язки включають:

а) Виявлення та оцінка ризиків;

б) Розробка заходів з управління ризиками;

в) Моніторинг ефективності заходів;

г) Звітування перед Наглядовою Радою та Правлінням.

Стаття 14. Основні функції головного ризик-менеджера

14.1. Головний ризик-менеджер виконує такі функції:

а) Виявлення та оцінка ризиків;

б) Розробка та впровадження заходів з управління ризиками;

в) Моніторинг ризиків та їх звітування.

Стаття 15. Відповідальність Правління за управління ризиками

15.1. Правління забезпечує реалізацію політики управління ризиками на всіх рівнях Товариства.

15.2. Основні функції Правління включають:

а) Впровадження стратегії та політики управління ризиками;

б) Підготовка та подання звітів про ризики;

в) Координація дій з управління ризиками між підрозділами Товариства.

Стаття 16. Процедури звітування

16.1. Звітування про ризики здійснюється на регулярній основі для забезпечення своєчасного інформування керівництва Товариства.

16.2. Основні процедури звітування включають:

а) Щоквартальні звіти про стан ризиків;

б) Щорічні звіти про оцінку та управління ризиками;

в) Позапланові звіти у разі суттєвих змін у ризиковому профілі.

Стаття 17. Програми навчання

17.1. Для підвищення ефективності управління ризиками, Товариство забезпечує регулярне навчання та підвищення кваліфікації співробітників.

17.2. Програми навчання включають:

а) Навчальні семінари та тренінги;

б) Участь у професійних конференціях та форумах;

в) Внутрішні навчальні програми.

Стаття 18. Захист інформації

18.1. Для забезпечення належного рівня інформаційної безпеки, Товариство впроваджує заходи щодо захисту конфіденційної інформації.

18.2. Основні заходи включають:

а) Встановлення систем контролю доступу до інформаційних ресурсів: це включає використання багаторівневих систем аутентифікації, розмежування прав доступу до даних відповідно до посадових обов'язків, впровадження систем логування та моніторингу доступу до конфіденційної інформації;

б) Впровадження систем резервного копіювання даних: це передбачає регулярне резервне копіювання всіх критично важливих даних, зберігання копій в окремих фізичних та хмарних місцях, а також перевірку цілісності резервних копій;

в) Проведення регулярних аудитів інформаційної безпеки: це включає внутрішні та зовнішні аудити систем інформаційної безпеки, оцінку вразливостей, перевірку дотримання політик та процедур, а також вжиття заходів для усунення виявлених недоліків;

г) Забезпечення навчання співробітників з питань інформаційної безпеки: це передбачає проведення регулярних тренінгів та семінарів для співробітників, спрямованих на підвищення їхньої обізнаності про загрози інформаційної безпеки та методи їхньої профілактики, а також розробку внутрішніх політик з інформаційної безпеки;

д) Впровадження системи управління інцидентами інформаційної безпеки: це включає розробку планів реагування на інциденти, моніторинг та аналіз інцидентів, своєчасне інформування керівництва про інциденти та впровадження заходів щодо їх усунення;

е) Захист від шкідливого програмного забезпечення: це включає використання антивірусного програмного забезпечення, систем виявлення та запобігання вторгненням, а також регулярне оновлення систем безпеки для захисту від нових загроз;

ж) Шифрування конфіденційної інформації: це передбачає використання сучасних методів шифрування для захисту даних під час їх зберігання та передачі, а також впровадження криптографічних протоколів для забезпечення цілісності та конфіденційності інформації;

з) Впровадження політики управління паролями: це включає встановлення вимог до створення складних паролів, регулярну зміну паролів, використання двофакторної аутентифікації та контроль за дотриманням політики управління паролями.

Стаття 19. Заключні положення

19.1. Ця Політика набирає чинності з дня її затвердження Наглядовою Радою і залишається чинною до її скасування або внесення змін.

19.2. Всі зміни та доповнення до цієї Політики затверджуються Наглядовою Радою та набирають чинності з дня їх затвердження.

19.3. Ця Політика доводиться до відома всіх співробітників Товариства, які залучені до процесів управління ризиками, та забезпечується їхня обізнаність про зміни та доповнення до Політики.

19.4. У разі виникнення конфліктів між положеннями цієї Політики та іншими внутрішніми документами Товариства, пріоритет мають положення цієї Політики.

Голова Наглядової ради ПрАТ «СТРАХОВА КОМПАНІЯ «ПЕРЕМОГА» _____
/ Лазарєв С. В /

Член Наглядової ради ПрАТ «СТРАХОВА КОМПАНІЯ «ПЕРЕМОГА» _____
/Вродзинська О.С./