ЗАТВЕРДЖЕНО
Рішенням Загальних зборів Учасників
ТОВ «КУА «АЛЬФА ЕССЕТ МЕНЕДЖМЕНТ»

протокол № 31 від "27" червня 2014 р.
Директор

_____ Майборода В.В.

ПОЛІТИКА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В ТОВ «КУА «АЛЬФА ЕССЕТ МЕНЕДЖМЕНТ»

Київ, 2014

1. Вступ

Політика інформаційної безпеки ТОВ «КУА «АЛЬФА ЕССЕТ МЕНЕДЖМЕНТ» (надалі - Політика)
– це внутрішній нормативний документ, який описує та регламентує систему управління інформаційною безпекою ТОВ «КУА «АЛЬФА ЕССЕТ МЕНЕДЖМЕНТ» (надалі – КУА). Політику складено у відповідності до Зводу правил для управління інформаційною безпекою» (ISO/IES 27002:2005, MOD), а також міжнародних стандартів
ISO/IEC 27001:2005 та ISO/IEC 27002:2005.

Інформація є ресурсом, який, як і інші важливі бізнес-ресурси, має певну цінність для КУА а, отже, потребує відповідного захисту.

Інформаційна безпека передбачає захист інформації від різноманітних загроз для підтримки безперервності бізнесу, скорочення збитків, збільшення прибутку на інвестований капітал і розширення можливостей бізнесу.

Яку б форму не обрала інформація, і які б кошти не використовувалися для її передачі та зберігання, необхідно завжди забезпечувати відповідний рівень її захисту.

В рамках даної Політики під інформаційною безпекою мається на увазі забезпечення наступних характеристик інформації:

- ***конфіденційність:*** надання доступу до інформації тільки тим, у кого є на це право;
- ***цілісність:*** захист точності і повноти інформації і методів її обробки;
- ***доступність:*** забезпечення доступу до інформації і пов'язаних з нею ресурсів авторизованими користувачами по мірі необхідності.

Інформаційна безпека досягається шляхом впровадження сукупності необхідних засобів захисту, в число яких можуть входити політики, рекомендації, інструкції, організаційні структури та програмні функції.

У разі невідповідності будь-якої частини цієї Політики чинному законодавству України, нормативно-правовим актам Національного банку України, у т.ч. у зв'язку із внесенням до них змін та доповнень, прийняттям нових законодавчих актів України, КУА керується даною Політикою у частині, що не суперечить чинному законодавству.

Політика описує прийняту та впроваджену КУА політику щодо захисту інформаційної безпеки.

Політика інформаційної безпеки КУА є обов'язковою для використання всіма робітниками КУА.

2. Ціль політики

Ціллю Політики є впровадження та ефективне функціонування системи управління інформаційною безпекою, яка буде забезпечувати безпечність та надійність функціонування бізнес-процесів, захист інформації та ресурсів КУА від зовнішніх та внутрішніх загроз та загроз, які пов'язані з навмисними та ненавмисними діями співробітникіі КУА, забезпечувати безперервну роботу КУА, сприяти мінімізації ризиків діяльності КУА та створювати позитивну репутацію КУА при роботі на фондовому ринку.

Основним завданням інформаційної безпеки є захист інформаційних ресурсів КУА від зовнішніх та внутрішніх, навмисних та ненавмисних загроз.

3. Сфера застосування

Дія Політики розповсюджується на всю КУА у цілому та використовується для всіх бізнес-процесів КУА, які можуть негативно впливати на результати її діяльності своєю відсутністю або функціонуванням з помилками.

4. Предмет політики та опис дій

Дана політика визначає основні принципи і заходи щодо забезпечення та розвитку інформаційної безпеки в ТОВ «КУА «АЛЬФА ЕССЕТ МЕНЕДЖМЕНТ, що дозволяють гарантувати захист інформаційних ресурсів для забезпечення ефективності та безперервності бізнес-діяльності відповідно до рекомендацій серії стандартів інформаційної безпеки ISO 27000, а також відповідає вимогам міжнародних стандартів ISO/IEC 27001:2005 та ISO/IEC 27002:2005.

Основними принципами інформаційної безпеки, яких дотримується КУА, є підтримання належного захисту інформації із забезпеченням її:

- **Конфіденційності** - властивість інформації не ставати доступною та розкритою для несанкціонованих осіб, об'єктів або процесів.
- **Доступності** - властивість доступності та можливості використання інформації КУА на вимогу санкціонованого об'єкта.
- **Спостережності** - властивість системи (автоматизованої, контролю доступу, моніторингу тощо) фіксувати діяльність ідентифікованих користувачів і процесів.

Це в першу чергу стосується інформації з обмеженим доступом, до якої відносяться відомості що становлять комерційну таємницю, персональні дані та іншу конфіденційну інформацію.

Серед основних об'єктів на які розповсюджується дія інформаційної безпеки КУА розглядаються наступні види ресурсів:

- **інформаційні ресурси** - інформація та дані у будь-якому вигляді, що отримуються, зберігаються, обробляються, передаються, оголошуються, у тому числі знання співробітників КУА, бази даних та файли, документація, посібники користувача, навчальні матеріали, описи процедур, архівована інформація тощо;
- **програмне забезпечення** - прикладне програмне забезпечення, системне програмне забезпечення, сервісне програмне забезпечення та будь-яке інше програмне забезпечення, незалежно від форми отримання (придбання, власної розробки, таке, що вільно розповсюджується), яке використовується у КУА співробітниками та системами для роботи та взаємодії з клієнтами та іншими внутрішніми та зовнішніми системами тощо;
- **фізичні ресурси** - співробітники, апаратні засоби IT (сервери, робочі станції, міжмережеві екрани, принтери, копіювальні апарати, телекомунікаційне обладнання, обладнання зв'язку,

маршрутизатори, АТС, факси, модеми тощо), носії даних (стрічки, диски тощо), меблі, приміщення, виробниче обладнання, інші технічні засоби тощо;

- **сервісні ресурси** - обчислювальні та комунікаційні сервіси (Інтернет, електронна пошта, канали зв'язку тощо), інші технічні сервіси (опалення, освітлення, енергозбереження, кондиціювання повітря, системи сигналізації та моніторингу), усі послуги, пов'язані з отриманням, наданням, використанням, передачею та знищенням ресурсів, усі юридичні та фізичні особи, організації, установи та підприємства (а також їх співробітники), послугами яких користується Банк для отримання, використання, передачі та знищення ресурсів.

Для кожного ресурсу визначаються можливі ризики інформаційної безпеки та шляхи їх мінімізації, тобто КУА використовує ризик-орієнтований підхід, який забезпечує розуміння, моніторинг та зменшення ризиків операційної діяльності.

Політика базується на вимогах законодавчих, регуляторних та нормативних документів з інформаційної безпеки.

КУА використовує наступні підходи щодо забезпечення інформаційної безпеки:

- створено та затверджено перелік відомостей, що містять інформацію з обмеженим доступом;
- створено та затверджено перелік критичних бізнес-процесів;
- встановлено правила доступу до інформаційних ресурсів та програмно-технічних комплексів;
- забезпечується контроль фізичного та логічного доступу до всіх визначених ресурсів;
- забезпечується парольний захист програмних та сервісних ресурсів;
- забезпечується антивірусний захист програмних та сервісних ресурсів;
- забезпечується захист мережі;
- забезпечується віддалений доступ до ресурсів мережі (локальної, мережі Інтернет, мереж інших організацій);
- забезпечується ідентифікація та автентифікація всіх визначених ресурсів;
- забезпечується криптографічний захист інформації.

Всі співробітники КУА обізнані та виконують вимоги інформаційної безпеки в роботі.

Під час розроблення, впровадження та функціонування програмно-технічних комплексів враховуються вимоги інформаційної безпеки.

Публічний сервіс КУА відповідає вимогам стандартів з інформаційної безпеки.

КУА забезпечує виконання усіх вимог інформаційної безпеки, які наявні в угодах з третіми сторонами стосовно участі у системах переказу коштів.

Для зменшення ризиків виникнення інцидентів інформаційної безпеки Керівництво КУА створює співробітникам умови для систематичного навчання нормам та заходам інформаційної безпеки.

В КУА складаються, діють, систематично тестуються та оновлюються плани безперебійного функціонування її діяльності на випадок різних непередбачуваних критичних ситуацій.

5. Ролі та відповідальність

Керівництво КУА чітко розуміє, що інформаційна безпека є основою життєдіяльності КУА та сприяє (організаційно та фінансово) впровадженню, контролю та підтримці вимог прийнятої Політики.

Документи системи управління інформаційною безпекою розробляються керівництвом КУА

та доступні співробітникам КУА у межах їх повноважень і призначені надавати допомогу у виконанні вимог інформаційної безпеки.

Постійний контроль впровадження, виконання, вдосконалення та підтримки Політики в актуальному стані покладається на Керівництво КУА.

Кожний співробітник КУА бере участь у підтримці відповідного рівня інформаційної безпеки КУА в межах своїх обов'язків та повноважень, несе відповідальність за їх порушення в межах, встановлених чинним законодавством України.

6. Перегляд документу

Перегляд даної Політики повинен проводитися не рідше, ніж 1 раз на 12 місяців.

Внесення змін/доповнень до Політики інформаційної безпеки здійснюється після узгодження

- власником ресурсу/процесу;
- відповідальним за інформаційну безпеку.

Внесення змін/доповнень до Політики інформаційної безпеки здійснюється відповідальною особою у наступних випадках:

- при змінах в документах, на підставі яких розроблено Політику;
- при впровадженні нових документів, що змінюють/впливають на процеси, описані в Політиці;
- при зміні ролей, відповідальності та процесів, що встановлює дана Політика;
- щорічно, за необхідності актуалізації найменувань документів, на які посилається дана Політика;
- у разі прийняття відповідного рішення Загальними зборами учасників.

Цей документ набуває чинності на наступний робочий день з дня затвердження, якщо інше не зазначено у рішенні Загальних зборів учасників КУА, яким документ затверджується.

Зміни та доповнення до цього документу набувають чинності на наступний робочий день з дня затвердження, якщо інше не зазначено у рішенні Загальниз зборів учасників КУА, яким документ затверджується. Усі зміни та доповнення до цього документу є його невід'ємною частиною.

Дана редакція цього документу втрачає свою чинність з дати набрання чинності наступної/ нової редакції цього документу або на підставі рішення загалних зборів учасників КУА.

7. Перелік взаємопов'язаних документів

Ця Політика пов'язана з наступними документами (розроблене на підставі та посилається): Стандарт організації України:

- Система управління інформаційною безпекою, СОУ Н НБУ 65.1 СУІБ 1.0:2010, Вимоги (ISO/IEC 27001:2005, MOD);
- Звід правил для управління інформаційною безпекою, СОУ Н НБУ 65.1 СУІБ 2.0:2010 (ISO/IEC 27002:2005, MOD).

Прошнуровано, пронумеровано
та скріплено відбитком печатки
та підписом керівника 5
(п'ять) аркушів

ТОВАРИСТВО З ОБМЕЖЕНОЮ ВІДПОВІДАЛЬНІСТЮ * м.КИЇВ * УКРАЇНА
"КОМПАНІЯ З УПРАВЛІННЯ АКТИВАМИ "АЛЬФА ЕССЕТ МЕНЕДЖМЕНТ"
Ідентифікаційний код 38213230