БАНК 3/4
приватний банкінг

ЗАТВЕРДЖЕНО
Голова Правління
_____ В.А. Іщенко
«15» червня 2017 року

ПОЛІТИКА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПУБЛІЧНОГО АКЦІОНЕРНОГО ТОВАРИСТВА «БАНК 3/4»

Київ – 2017

1. ВСТУП

1.1. Політика інформаційної безпеки ПУБЛІЧНОГО АКЦІОНЕРНОГО ТОВАРИСТВА «БАНК 3/4» (далі — Політика) описує та регламентує функціонування системи управління інформаційною безпекою (далі — СУІБ) відповідно до стандартів Національного банку України СОУ Н НБУ 65.1 СУІБ 1.0:2010 та СОУ Н НБУ 65.1 СУІБ 2.0:2010, відповідає вимогам законодавства України та нормативно-правовим актам Національного банку України, а також вимогам міжнародних та внутрішньодержавних платіжних систем та систем переказу коштів.

1.2. Положення даної Політики ґрунтуються на вимогах галузевих стандартів Національного банку України з управління інформаційною безпекою в банківській системі України та рекомендаціях кращих міжнародних практик в галузі захисту інформації.

2. ТЕРМІНИ ТА СКОРОЧЕННЯ

Банк - ПУБЛІЧНЕ АКЦІОНЕРНЕ ТОВАРИСТВО «БАНК 3/4», включаючи відокремлені структурні підрозділи.

Бізнес-процес – послідовність логічно зв'язаних процедур, що має кілька входів і виходів, яка призначена для одержання заданого кінцевого результату (результатів).

Загроза – потенційна причина небажаного інциденту, який може призвести до шкоди для Банку, його кредиторів та вкладників .

Інформаційна безпека - це захист інформації від широкого діапазону загроз з метою забезпечення безперервності бізнесу, мінімізації бізнес-ризику і отримання максимальних рентабельності інвестицій і бізнес-можливостей.

Інформація з обмеженим доступом – конфіденційна (в тому числі персональні дані, комерційна таємниця), таємна (в тому числі інформація, що містить банківську таємницю) та службова інформація,.

Клієнт (Клієнт Банку) – будь-яка фізична особа чи суб'єкт господарювання (в т.ч. банківська установа), що користується послугами Банку.

Критичний бізнес-процес – бізнес-процес, який обробляє інформацію з обмеженим доступом , розголошення якої може нанести шкоду Банку.

Ресурси СУІБ – все, що має цінність для Банку.

СУІБ – система управління інформаційною безпекою – перелік цілей, принципів керування, методів, заходів з захисту інформації та забезпечення стійкості бізнес-процесів в інформаційній інфраструктурі Банку.

3. ЦІЛЬ ПОЛІТИКИ

3.1. Ціллю Політики є впровадження, ефективне функціонування, регулювання та підтримка системи управління інформаційною безпекою, яка забезпечує захист інформації та ресурсів Банку від зовнішніх і внутрішніх загроз та загроз, які пов'язані з навмисними та ненавмисними діями працівників Банку, забезпечує безперервну роботу Банку, сприяє мінімізації ризиків операційної діяльності Банку та створює позитивну репутацію Банку при роботі з клієнтами.

3.2. Стратегія розвитку Банку узгоджується з цією Політикою. Досягнення стратегічних цілей Банку має проводитись у суворій відповідності з Політикою інформаційної безпеки.

4. СФЕРА ЗАСТОСУВАННЯ

4.1. Дія Політики поширюється на весь Банк в цілому. Всі працівники Банку, незалежно від рівнів доступу до інформації та ресурсів Банку, мають дотримуватись вимог цієї Політики.

4.2. Політика використовується для усіх критичних бізнес-процесів/банківських продуктів/програмно-технічних комплексів Банку.

4.3. Банк контролює дотримання вимог цієї Політики при наданні послуг третіми особами, які в процесі надання таких послуг одержують доступ до інформаційних ресурсів Банку. Представники (користувачі) третіх осіб мають негайно повідомляти Банк

про події порушення інформаційної безпеки Банку та/або слабкі місця інформаційної безпеки Голові Правління або Заступнику Голови Правління Банку.

4.4. Банк захищає власні інформаційні ресурси фізичними, апаратними, програмними, нормативними та цивільно-правовими шляхами. Банк розмежовує інформацію з обмеженим доступом від іншої інформації.

5. ПРЕДМЕТ ДОКУМЕНТУ ТА ОПИС ДІЙ

5.1. Основними принципами Політики є підтримання належного захисту інформації із забезпеченням цілісності, конфіденційності, доступності та спостережності, насамперед конфіденційної інформації.

Цілісність - властивість захищеності, безпомилковості та повноти ресурсів СУІБ.

Конфіденційність - властивість інформації не ставати доступною та розкритою для несанкціонованих осіб, об'єктів або процесів.

Доступність - властивість доступності та можливості використання ресурсів СУІБ на вимогу санкціонованого об'єкта.

Спостережність - властивість системи (автоматизованої, контролю доступу, моніторингу тощо) фіксувати діяльність ідентифікованих користувачів і процесів.

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

5.3. Керівництво Банку та керівники структурних підрозділів сприяють у створенні, впровадженні, постійному контролі й супроводі Політики.

5.4. Банк приділяє особливу увагу забезпеченню захисту, схоронності та запобіганню незаконному розголошенню інформації з обмеженим доступом. Репутація Банку – один з найважливіших ресурсів Банку, тому невиконання обов’язку Банку зі збереження інформації, що містить інформацію з обмеженим доступом, несе не лише правову відповідальність, а й значні репутаційні ризики.

5.5. Всі працівники Банку, до того, як вони приступають до виконання свої обов’язків дають зобов’язання про нерозголошення банківської таємниці, яке залишається чинним протягом всього періоду роботи в Банку та після звільнення необмежений час.

5.6. При забезпеченні інформаційної безпеки Банк керується ризик-орієнтованим підходом, який забезпечує розуміння, моніторинг та зменшення ризиків діяльності. Банк обробляє ризики інформаційної безпеки відповідно до внутрішньої методології, на підставі оцінки ймовірності реалізації ризиків та важкості їх наслідків, визначає три рівні ризиків: високий, середній та низький. Банк має право прийняти ризик будь-якого рівня, проте рішення про прийняття високого рівня ризику має прийматись керівництвом на підставі повної поінформованості, аналізу загроз та, за умов здійснення дієвих заходів зі зменшення рівня ризику (в тому числі впровадження компенсаційних заходів).

5.7. Банком використовуються наступні підходи щодо забезпечення інформаційної безпеки:

- створено та затверджено перелік відомостей та носіїв інформації, що містить конфіденційну інформацію та банківську таємницю;
- створено та затверджено перелік критичних бізнес-процесів за якими проводиться оцінка ризиків інформаційної безпеки та подальша їх обробка;
- встановлено правила доступу до інформаційних ресурсів та програмно-технічних комплексів;
- забезпечується контроль фізичного та логічного доступу до всіх визначених ресурсів СУІБ у Банку;
- забезпечується парольний захист програмних та сервісних ресурсів;
- забезпечується антивірусний захист та захист від зловмисного коду;
- забезпечується захист мережі;
- забезпечується ідентифікація та автентифікація всіх визначених ресурсів;
- забезпечується криптографічний захист інформації;
- проводяться процедури для визначення, чи мала місце якась компрометація ресурсів СУІБ, внутрішні аудити СУІБ та аналіз СУІБ з боку керівництва Банку;

- проводяться процедури захисту інформації при її передачі третім особам, укладаються угоди про конфіденційність, та здійснюються заходи для забезпечення повернення чи знищення інформації та ресурсів СУІБ по закінченні або в погоджений момент часу протягом дії угоди
- моніторинг та вдосконалення СУІБ.

5.8. Банк вимагає від всього персоналу бути обізнаними та виконувати вимоги інформаційної безпеки в роботі, сприяє створенню належного інформаційного поля для підвищення півня знань працівників. Вимоги щодо освітнього рівня працівників Банку встановлюються в їх посадових інструкціях і для персоналу, задіяного у критичних бізнес-процесах, встановлюється критерій наявності вищої освіти.

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

5.10. Працівники Банку та особи, що одержують доступ до інформаційних ресурсів Банку, обов'язково проходять вступний документований інструктаж з питань інформаційної безпеки. Банк у вступних інструктажах, пам'ятках, угодах про конфіденційність попереджає про відповідальність за порушення вимог з інформаційної безпеки, аж до кримінальної.

5.11. Функціонування веб-сайту Банку, його технологічна підтримка є важливим елементом інформаційної політики, оскільки регулятори та банківська практика вимагають оприлюднювати значний обсяг інформації про Банк. Тому керівництво заохочує пропозиції працівників щодо покращення функціонування веб-сайту та вимагає проведення моніторингу інформації, що розміщена на веб-сайті.

5.12. Інформаційні системи та внутрішні мережі Банку відповідають вимогам стандартів з інформаційної безпеки, керівництво сприяє проведенню модернізації обладнання.

5.13. Банк забезпечує виконання усіх вимог з інформаційної безпеки, які наявні в угодах з третіми сторонами, зокрема стосовно асоційованої участі у міжнародних платіжних системах та участі в системі електронних переказів Національного банку України.

5.14. У Банку складаються, діють, тестуються та оновляються плани забезпечення безперебійного функціонування на випадок непередбачених критичних ситуацій. Приймаючи ризик-орієнтований підхід до планування діяльності, Банк ідентифікує та оцінює альтернативні варіанти оброблення ризиків та обирає конкретний захід безпеки в процесі забезпечення безперебійної діяльності виходячи з імовірності настання загроз, швидкості та ефективності заходу з оброблення ризиків та особистого професійного досвіду фахівців Банку.

5.15. Для зменшення ризиків виникнення інцидентів інформаційної безпеки керівництво Банку створює умови для систематичного навчання працівникам нормам та заходам інформаційної безпеки. Враховуючи невеликий розмір Банку, керівництво Банку зобов'язує керівників структурних підрозділів вести постійну роз'яснювальну роботу та здійснювати неухильний контроль за дотриманням підлеглими вимог з інформаційної безпеки.

5.16. Банк вимагає дотримання вимог з інформаційної безпеки під час обміну інформацією з використанням всіх засобів комунікацій. Обмін інформацією, що містить банківську таємницю, по незахищеним каналам зв'язку не допускається. Усне обговорення питань з використанням персоніфікованих даних, що містять банківську таємницю або іншу конфіденційну інформацію, поза межами Банку забороняється (крім обговорення інформації клієнта на території клієнта), а у межах Банку має здійснюватись таким чином, щоб сторонні особи не були присутні під час та кого обговорення (випадково чи навмисно).

5.17. Банк застосовує процедури захисту обміну інформації:

- обізнаність персоналу — прийняття кожним окремим працівником зобов'язань про нерозголошення інформації з обмеженим доступом та обізнаність (усвідомлення)

персоналу з відповідальністю за незаконне використання та розголошення інформації з обмеженим доступом;

- застосування дисциплінарних процесів щодо порушників інформаційної безпеки;
- апаратні, програмні засоби , в тому числі засоби відеоспостереження;
- розмежування та контроль доступів, ієрархія санкціонування доступів та періодичний перегляд доступів до інформаційних систем Банку;
- використання застережень про нерозголошення та захист інформації з обмеженим доступом та дотримання вимог цієї Політики у відносинах з третіми особами, що одержують доступ до інформаційних ресурсів Банку;
- ідентифікація всіх осіб, що одержують доступ до інформаційних систем Банку;
- інші заходи на розсуд Банку.

6. РОЛІ ТА ВІДПОВІДАЛЬНІСТЬ

6.1. Керівництво Банку чітко розуміє, що інформаційна безпека Банку є основою життєдіяльності Банку.

6.2. Акціонером Банку затверджений Кодекс Корпоративної етики, який зобов'язує Банк дотримуватись найвищих стандартів у сфері інформаційної безпеки та здійснює різноманітні заходи з захисту інформації, що містить банківську таємницю, захищати конфіденційність клієнта та захищати інформацію про клієнтів. Кодекс розміщується на сайті Банку, є доступним не лише для працівників та акціонерів Банку, а й для всіх зацікавлених осіб. Кодекс є обов'язковим для виконання працівниками та власниками Банку.

6.3. У Банку створена та постійно діє Робоча група з питань інформаційної безпеки, яку очолює Заступник Голови Правління, та до складу якої входять керівники підрозділів, що є власниками, або активними учасниками критичних бізнес-процесів.

6.4. Керівництво Банку сприяє створенню, впровадженню, контролю та підтримці Політики інформаційної безпеки.

6.5. Політика розробляється фахівцем з інформаційної безпеки, а за його відсутності – Управлінням інформаційних технологій з залученням інших структурних підрозділів Банку за відповідними напрямками діяльності.

6.6. Постійний контроль впровадження, виконання, вдосконалення та підтримки Політики в актуальному стані покладається на відділ інформаційної безпеки.

6.7. Кожен співробітник Банку забезпечує підтримку відповідного рівня інформаційної безпеки Банку. В своїй роботі всі підрозділи та працівники дотримуються вимог Політики інформаційної безпеки та несуть відповідальність за їх порушення згідно з чинним законодавством України та внутрішньобанківськими нормативними документами. Всі працівники Банку зобов'язані негайно звітувати керівництву про інциденти інформаційної безпеки, а керівництво приймає на себе зобов'язання негайно реагувати на такі інциденти шляхом усунення наслідків та причин їх виникнення.

6.8. Для зменшення ризиків виникнення інцидентів інформаційної безпеки керівництво Банку створює працівникам умови для систематичного навчання нормам та заходам інформаційної безпеки.

7. ПЕРЕГЛЯД ПОЛІТИКИ

7.1. Політика підтримується в актуальному стані та переглядається за необхідністю, але не менш ніж один раз на рік.

7.2. Причинами внесення змін до Політики є зміни в інформаційній інфраструктурі та/або впровадження в Банку нових інформаційних технологій, а також змінах в законодавчих, регуляторних та інших нормах.

8. ІСТОРІЯ ЗМІН

Дата	Автор	Зміст змін

06.12.2016	УІТ	Попередня редакція Політики інформаційної безпеки