ПОГОДЖЕНО
Рішенням Керівного органу з питань впровадження та функціонування СУІБ
АТ «БАНК 3/4»
Протокол №15 від 28.12.2019р.

ПОЛІТИКА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ АКЦІОНЕРНОГО ТОВАРИСТВА «БАНК 3/4»

Київ – 2019

1. ВСТУП

1.1. Політика інформаційної безпеки АКЦІОНЕРНОГО ТОВАРИСТВА «БАНК 3/4» (далі — Політика) встановлює цілі інформаційної безпеки та принципи АТ «БАНК 3/4» (далі – Банк) щодо управління власними цілями інформаційної безпеки, правила та вимоги інформаційної безпеки в Банку, сферу застосування цієї Політики, а також ролі та відповідальності за забезпечення інформаційної безпеки в Банку.

1.2. Ця Політика розроблена відповідно до Положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі України, затвердженого постановою Правління Національного банку України від 28.09.2017 № 95, Національних стандартів України ДСТУ ISO/IEC 27000:2015 «Методи захисту система управління інформаційною безпекою. Огляд і словник», ДСТУ ISO/IEC 27001:2015 «Методи захисту системи управління інформаційною безпекою. Вимоги», ДСТУ ISO/IEC 27002:2015 «Звід практик щодо заходів інформаційної безпеки», вимог законодавства України та нормативно-правових актів Національного банку України, а також вимог міжнародних та внутрішньодержавних платіжних систем та систем переказу коштів.

1.3. Керівництво Банку впроваджує цю Політику інформаційної безпеки, яка:

а) відповідає цілям Банку;

б) містить цілі інформаційної безпеки або зазначає основні положення для визначення цілей інформаційної безпеки;

в) містить зобов’язання відповідати застосованим вимогам, пов’язаним з інформаційною безпекою;

г) містить зобов’язання щодо постійного вдосконалення системи управління інформаційною безпекою.

1.4. Положення даної Політики ґрунтуються на вимогах Національних стандартів України з управління інформаційною безпекою та рекомендаціях кращих міжнародних практик в галузі захисту інформації.

2. ТЕРМІНИ ТА СКОРОЧЕННЯ

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

Бізнес-процес – сукупність взаємопов'язаних або взаємодіючих видів діяльності, спрямованих на створення певного продукту або послуги;

Загроза – потенційна причина небажаного інциденту, який може спричинити шкоду для системи чи Банку.

Інформаційна безпека - це стан захищеності систем обробки і зберігання даних, при якому забезпечено збереження конфіденційності, доступності і цілісності інформації.

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.

Критичні бізнес-процеси Банку - бізнес-процеси діяльності Банку, визначені Банком критичними щодо інформаційної безпеки за результатом їх оцінювання Банком за такими критеріями: конфіденційність, цілісність, доступність.

Ресурси СУІБ – все, що має цінність для Банку, активи, інформація, людські ресурси тощо, які повинні враховуватися для забезпечення ефективного управління інформаційною безпекою, включаючи інформацію в електронному та паперовому вигляді, в т.ч. інформацію з обмеженим доступом, програмне і апаратне забезпечення та персонал, які забезпечують їх обробку.

СУІБ –система управління інформаційною безпекою - це системний підхід для розроблення, впровадження, функціонування, моніторингу, підтримування і вдосконалення інформаційної безпеки в Банку для досягнення бізнес-цілей.

3. ЦІЛЬ ПОЛІТИКИ

3.1. Цілями інформаційної безпеки Банку є збереження конфіденційності, цілісності, доступності інформації. захист інформаційних ресурсів Банку від зовнішніх та внутрішніх загроз.

3.2. Ціллю цієї 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, а також контрагентів Банку, третіх осіб, забезпечує безперервну роботу Банку, сприяє мінімізації ризиків операційної діяльності Банку та створює позитивну репутацію Банку при роботі з клієнтами.

3.3. 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. Ця Політика має бути доступною як документована інформація; розповсюдженою всередині Банку і бути доступною зацікавленим сторонам.

4.2. 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.

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

4.4. Банк контролює дотримання вимог цієї Політики при наданні послуг третіми особами, які в процесі надання послуг одержують доступ до інформаційних ресурсів Банку. Представники (користувачі) третіх осіб повинні ознайомитися з цією Політикою, оприлюдненою на веб-сайті Банку, виконувати її вимоги, самостійно відслідковувати зміни до неї, та мають негайно повідомляти Банк про події порушення інформаційної безпеки Банку та/або слабкі місця інформаційної безпеки Голові Правління або Заступнику Голови Правління Банку.

4.5. Банк вимагає від постачальників послуг (контрагентів) знання і дотримання вимог з інформаційної безпеки, зокрема, укладає угоди, включає застереження в договори про те, що контрагент гарантує, що одержаний ним доступ до інформаційних активів Банку буде використано виключно з метою надання послуг за окремим договором, укладеним між Банком та цим контрагентом, та контрагент не чинитиме будь-яких спроб на доступ до таких активів або втручання в них у строки, формі, спосіб, що не визначено письмовими договірними відносинами між сторонами.

Контрагент на вимогу Банку зобов’язаний надати перелік власних працівників, що допущені до надання послуг Банку та забезпечити виконання ними вимог з інформаційної безпеки.

Після закінчення надання послуг Банку, контрагент має знищити будь-яку інформацію, що має ознаки інформації з обмеженим доступом, не утворювати та не зберігати будь-які креслення, відомості, записи щодо функціонування інформаційних активів Банку, крім загальновідомої.

4.6. 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 інформації з обмеженим доступом.

Цілісність – властивість точності та повноти інформації.

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

Доступність – властивість досяжності й можливості використання на вимогу авторизованого об'єкта, яка полягає в тому, що користувач і/або процес, який володіє відповідними повноваженнями, може отримати доступ до інформації або використовувати ресурс відповідно до правил, встановлених цією Політикою, у визначений проміжок часу.

Спостережність – властивість системи, що дозволяє фіксувати діяльність користувачів і процесів, використання пасивних об'єктів, а також однозначно установлювати ідентифікатори причетних до певних подій користувачів і процесів з метою запобігання порушення цієї Політики і/або забезпечення відповідальності за певні дії.

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

5.3. Всі працівники Банку до того, як вони приступають до виконання своїх обов'язків, дають письмове зобов'язання щодо збереження банківської таємниці та іншої інформації з обмеженим доступом, яке залишається чинним протягом всього періоду роботи в Банку та після їх звільнення необмежений час.

5.4. При забезпеченні інформаційної безпеки Банк керується ризик-орієнтованим підходом, який забезпечує розуміння, моніторинг та зменшення ризиків діяльності.

5.5. Банк обробляє ризики інформаційної безпеки відповідно до внутрішньої методології, на підставі оцінки імовірності 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).

5.6. Банком використовуються наступні методи 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;
- забезпечується формування та збереження відокремлених електронних даних;
- забезпечується резервне копіювання інформації та утворення резерву апаратних комплексів
- моніторинг та вдосконалення СУІБ.

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

5.8. 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.

5.9. Для дистанційного обслуговування клієнтів функціонує інформаційна система Інтернет-банкінг. Високий рівень інформаційної безпеки під час експлуатації Інтернет-банкінгу забезпечується наступними механізмами:

а) Автентифікація серверу Інтернет-банкінгу -для захисту від атак, спрямованих на підміну банківського Web-сервера і модифікації його контенту (під час передачі даних застосовується протокол SSL (Secure Sockets Layer).

б) Автентифікація клієнтів Інтернет-банкінгу, - для безпечного доступу до системи застосовується технологія двофакторної аутентифікації користувачів.

в) Шифрування даних - для забезпечення конфіденційності даних, якими обмінюються користувачі з Банком по каналах Інтернет-банкінгу, ці дані шифруються. Таким чином, виключається можливість перехоплення та несанкціонованого читання платіжної та іншої інформації.

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

5.11. 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 платежів Національного банку України.

5.12. У Банку розроблюється, діє, тестується та оновлюється план забезпечення безперервної діяльності, у якому враховано пріоритет Банку щодо забезпечення безперервної діяльності критично важливих інформаційних систем, заходи відновлення інформаційних систем після збоїв.

5.13. 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.

5.14. Банк вимагає від всього персоналу бути обізнаними та виконувати вимоги інформаційної безпеки в роботі, сприяє створенню належного інформаційного поля для підвищення рівня 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.

5.15. 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.

5.16. Для зменшення ризиків виникнення інцидентів інформаційної безпеки керівництво Банку створює умови для систематичного навчання працівників нормам та заходам інформаційної безпеки. Враховуючи 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.

5.17. 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 такого обговорення (випадково чи навмисно).

5.18. Банк застосовує процедури захисту інформації:

- обізнаність персоналу — надання кожним окремим працівником зобов'язання щодо збереження банківської таємниці та іншої 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 сканування інформаційних систем, 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;
- резервне копіювання, архівування та 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. Наглядовою радою Банку затверджений Кодекс корпоративної етики, який зобов'язує працівників Банку дотримуватись найвищих стандартів у сфері інформаційної безпеки та здійснювати 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, керівниками та власниками Банку.

6.3. У Банку створений та постійно діє Керівний орган з питань впровадження та функціонування СУІБ , який очолює Голова Правління, та до складу якого 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 співробітниками Відділу інформаційної безпеки та Управління 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 Керівний орган з питань впровадження та функціювання СУІБ.

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 рідше 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 зміни в законодавчих, регуляторних та інших нормах.