ЗАТВЕРДЖЕНО
Рішенням Правління АТ «БТА БАНК»
протокол № ____від «___» _____ 2022 р.

Голова Правління АТ «БТА БАНК»

_____ Є.О. Безвушко

ПОЛІТИКА
інформаційної безпеки АТ «БТА БАНК»

Версія 3.00

м. Київ – 2022 рік

ЗМІСТ

1. ЗАГАЛЬНІ ПОЛОЖЕННЯ

1.1. Політика інформаційної безпеки АТ «БТА БАНК» (далі – Політика) розроблена відповідно до вимог чинного законодавства України, зокрема нормативно-правових актів Національного банку України (в тому числі стандартів СОУ Н НБУ 65.1 СУІБ 1.0:2010 Методи захисту в банківській діяльності. Система управління інформаційною безпекою. Вимоги (ISO/IEC 27001:2005, MOD) та СОУ Н НБУ 65.1 СУІБ 2.0:2010 Методи захисту в банківській діяльності. Звід правил для управління інформаційною безпекою (ISO/IEC 27002:2005, MOD)), Методичних рекомендацій щодо впровадження системи управління інформаційною безпекою та методики оцінки ризиків відповідно до стандартів Національного банку України, введених в дію листом НБУ від 03.03.2011 N 24-112/365, внутрішніх документів АТ «БТА БАНК» (далі – Банк).

1.2. Документ описує прийняту та впроваджену Банком політику щодо захисту інформаційної безпеки.

1.3. Метою Політики є впровадження та ефективне функціонування системи управління інформаційною безпекою, яка буде забезпечувати безпечність та надійність функціонування бізнес-процесів, захист інформації та ресурсів Банку від зовнішніх та внутрішніх загроз та загроз, які пов’язані з навмисними та ненавмисними діями працівників Банку, забезпечувати безперервну роботу Банку, сприяти мінімізації ризиків інформаційної безпеки Банку, операційної діяльності та створювати позитивну репутацію Банку при роботі з клієнтами.

1.4. Основним завданням інформаційної безпеки є захист ресурсів Банку від зовнішніх та внутрішніх, навмисних та ненавмисних загроз. Більш детальні та вимірювані цілі інформаційної безпеки щорічно виносяться на розгляд та затвердження Робочої групи з питань системи управління інформаційною безпекою АТ «БТА БАНК» за поданням Управління інформаційної безпеки Департаменту банківської безпеки Банку.

1.5. Дія Політики розповсюджується на весь Банк у цілому та використовується для всіх бізнес-процесів Банку, які можуть негативно впливати на результати діяльності Банку своєю відсутністю або функціонуванням з помилками.

1.6. Дія Політики розповсюджується також на треті сторони – юридичні або фізичні особи, які володіють достатнім рівнем знань та кваліфікації для надання необхідних Банку послуг (постачальники / провайдери / партнери). Правила інформаційної безпеки для такого випадку викладено в документі ***Процедура управління інформаційною безпекою при роботі з третіми сторонами ПАТ «БТА БАНК».***

2. ТЕРМІНИ ТА СКОРОЧЕННЯ

2.1. Інформація з обмеженим доступом – відомості, що становлять банківську та комерційну таємницю, персональні дані та іншу конфіденційну інформацію.

2.2. Бізнес-процес – структурована послідовність дій з виконання певного виду діяльності на всіх етапах життєвого циклу предмета діяльності, метою якої є дотримання заданого результату, що має цінність для Банку.

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

2.4. Загроза – будь-які обставини або події, що можуть бути причиною порушення політики безпеки інформації і/або нанесення збитків автоматизованій системі або Банку.

2.5. Несанкціонована особа, об'єкт або процес – особа, об’єкт або процес, які не контролюються Банком та/або не задовольняють вимоги, які до них висуваються.

2.6. Ресурси СУІБ – все, що має цінність для Банку.

2.7. Робоча група з питань системи управління інформаційною безпекою АТ «БТА БАНК» – є постійно діючим колегіальним органом Банку, який забезпечує процес розроблення, впровадження, функціонування, моніторингу, перегляду, підтримування та вдосконалення системи управління інформаційною безпекою шляхом прийняття відповідних рішень.

2.8. Санкціонований об'єкт – об’єкт, який контролюється Банком та/або задовольняє вимоги, які до нього висуваються.

2.9. СУІБ – система управління інформаційною безпекою – частина загальної системи управління, яка ґрунтується на підході, що враховує бізнес-ризики, призначена для розроблення, впровадження, функціонування, моніторингу, перегляду, підтримування та вдосконалення інформаційної безпеки.

3. ПРИНЦИПИ ТА ПІДХОДИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ БАНКУ

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

– Цілісності – властивість захищеності, безпомилковості та повноти ресурсів СУІБ.

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

– Доступності – властивість доступності та можливості використання ресурсів СУІБ на вимогу санкціонованого об'єкта.

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

3.2. В першу чергу ці принципи стосуються інформації з обмеженим доступом, до якої відносяться відомості, що становлять банківську та комерційну таємницю, персональні дані та іншу конфіденційну інформацію.

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

– інформаційні ресурси – інформація та дані у будь-якому вигляді, що отримуються, зберігаються, обробляються, передаються, оголошуються, у тому числі знання працівників, партнерів Банку, бази даних та файли, документація, 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 Банку працівниками та системами для роботи та взаємодії з Клієнтами та іншими внутрішніми та зовнішніми системами тощо;

– фізичні ресурси – працівники, апаратні засоби ІТ (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;

3.4. 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 працівники), послугами яких користується Банк для отримання, використання, передачі та знищення ресурсів.

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

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

3.7. Банком використовуються 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.

3.8. Всі працівники Банку обізнані та виконують вимоги інформаційної безпеки в роботі.

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

3.10. Публічні сервіси Банку та внутрішні мережі Банку відповідають вимогам стандартів з інформаційної безпеки.

3.11. Банк забезпечує виконання усіх вимог інформаційної безпеки, які наявні в угодах з третіми сторонами стосовно участі у міжнародних платіжних системах та системах переказу коштів.

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

3.13. У Банку складаються, діють, систематично тестуються та оновлюються плани безперебійного функціонування діяльності Банку на випадок різних непередбачуваних критичних ситуацій.

4. РОЛІ ТА ВІДПОВІДАЛЬНОСТІ

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

4.2. У Банку створена та постійно працює Робоча група з питань системи управління інформаційною безпекою АТ «БТА БАНК», рішення якої є обов’язковими для виконання усіма працівниками Банку.

4.3. Документи системи управління інформаційною безпекою розробляються Управлінням інформаційної безпеки Департаменту банківської безпеки та іншими структурними підрозділами Банку за відповідними напрямками діяльності.

4.4. Документи системи управління інформаційною безпекою доступні працівникам Банку у межах їх повноважень і призначені надавати допомогу у виконанні вимог інформаційної безпеки.

4.5. Постійний контроль впровадження, виконання, вдосконалення та підтримки Політики покладається на Управління інформаційної безпеки Департаменту банківської безпеки.

4.6. Кожний працівник Банку бере участь у підтримці відповідного рівня інформаційної безпеки Банку в межах своїх обов’язків та повноважень, несе відповідальність за їх порушення в межах, встановлених чинним законодавством України та внутрішніми документами Банку.

5. ПЕРЕГЛЯД ДОКУМЕНТА

5.1. Банком забезпечується підтримка Політики в актуальному стані. Політика переглядається один раз на рік та/або за необхідністю.

5.2. Причинами внесення змін до Політики є зміни в актах чинного законодавства України, в тому числі нормативно-правових актах НБУ, та інших документах, що регламентують питання функціонування СУІБ.

6. ЗАКЛЮЧНІ ПОЛОЖЕННЯ

6.1. Політика набуває чинності з моменту її затвердження рішенням Правління Банку.

6.2. Зміни та доповнення до Політики затверджуються Правлінням Банку за поданням Управлінням інформаційної безпеки Департаменту банківської безпеки та оформлюються шляхом її викладення в новій редакції.

6.3. У разі внесення змін до чинного законодавства України, в тому числі нормативно-правових актів Національного банку України, до приведення Політики у відповідність до вимог чинного законодавства України, в тому числі нормативно-правових актів Національного банку України, ця Політика діє лише в тій частині, що не суперечить таким змінам.