ПРИВАТНЕ АКЦІОНЕРНЕ ТОВАРИСТВО
«БАНК ФАМІЛЬНИЙ»

УЗГОДЖЕНО:

Правлінням
ПрАТ «БАНК ФАМІЛЬНИЙ»
(протокол № 84/2023 від 27.04.2023 р.)

Голова Правління
ПрАТ «БАНК ФАМІЛЬНИЙ»

_____ О.С.Квашнін

ЗАТВЕРДЖЕНО:

Наглядовою радою
ПрАТ «БАНК ФАМІЛЬНИЙ»
(протокол № 84/2023 від 27.04.2023 р.)

Голова Наглядової ради
ПрАТ «БАНК ФАМІЛЬНИЙ»

_____ М.Б.Комiссарук

ПОЛІТИКА
ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

м. Київ

ЗМІСТ

ТЕРМІНИ ТА СКОРОЧЕННЯ

Банк – Приватне акціонерне товариство «БАНК ФАМІЛЬНИЙ».
Бізнес-процес – структурована послідовність дій з виконання певного виду діяльності на всіх етапах життєвого циклу банківської діяльності, метою якої є отримання заданого результату, що має цінність для Банку.
Доступність — властивість інформації, яка гарантує те, що забезпечується своєчасний доступ авторизованих осіб і/або процесів до інформації, відсутні простої в процесі її обробки, тобто коли вона знаходиться у вигляді, необхідному користувачеві, в місці, необхідному користувачеві, і в той час, коли вона йому необхідна, а у випадку втрати інформації існує можливість своєчасного відновлення.
Забезпечення інформаційної безпеки - встановлення та підтримання належного рівня властивостей інформаційної безпеки, в тому числі доступності, цілісності, конфіденційності, спостережності.
Загроза – потенційна причина інциденту інформаційної безпеки, який може призвести до шкоди для системи або організації.
Інцидент інформаційної безпеки – одна або серія небажаних чи непередбачуваних подій інформаційної безпеки, що мають значну ймовірність компрометації бізнес-операцій і загрози інформаційній безпеці.
Інформаційна безпека - захист інформації від широкого діапазону загроз з метою забезпечення безперервності бізнесу, мінімізації ризику бізнес-процесів і отримання максимальної рентабельності інвестицій і бізнес-можливостей.
Інформація з обмеженим доступом - відомості, що становлять банківську таємницю, комерційну таємницю та персональні дані.
Клієнт (Клієнт Банку) - особа, яка має рахунок у Банку, або користується його послугами.
Конфіденційність — властивість інформації, яка гарантує те, що доступ до інформації можуть одержати тільки авторизовані особи і/або процеси.
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, зокрема інформація, засоби її зберігання, обробки і передавання, персонал, клієнти, бізнес-процеси та продукти тощо.
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 політики безпеки і/або забезпечення відповідальності за певні дії.
СУІБ – система управління інформаційною безпекою – перелік цілей, принципів керування, методів, заходів з захисту інформації та забезпечення стійкості бізнес-процесів в інформаційній інфраструктурі Банку.
Цілісність — властивість інформації, яка гарантує те, що інформація не містить помилок, є актуальною, вичерпною, будь-які зміни інформації здійснюються авторизованими особами і/або процесами.

1. ЗАГАЛЬНІ ПОЛОЖЕННЯ

1.1. Політика інформаційної безпеки (далі – *Політика*) визначає цілі та принципи функціонування системи управління інформаційною безпекою (далі – СУІБ) Банку.
1.2. Основною метою *Політики* є забезпечення через ефективне функціонування та розвиток системи управління інформаційною безпекою Банку безпечності та надійності функціонування бізнес-процесів, захисту інформації та ресурсів Банку від зовнішніх та внутрішніх загроз та загроз, які пов’язані з навмисними та ненавмисними діями співробітників Банку, а також забезпечення безперервної роботи Банку, сприяння мінімізації ризиків операційної діяльності Банку та створення позитивної репутації Банку при роботі з Клієнтами.

1.3. *Політику* розроблено відповідно до вимог законодавства України, нормативно-правових документів Національного банку України, в тому числі національних стандартів України з питань інформаційної безпеки: «ДСТУ ISO/IEC 27000:2019 «Інформаційні технології. Методи захисту. Система управління інформаційною безпекою. Огляд і словник» (далі – ДСТУ ISO/IEC 27000:2019)», «ДСТУ ISO/IEC 27001:2015 Інформаційні технології. Методи захисту системи управління інформаційною безпекою. Вимоги (ISO/IEC 27001:2013; Cor 1:2014, IDT)» та «ДСТУ ISO/IEC 27002:2015 Інформаційні технології. Методи захисту. Звід практик щодо заходів інформаційної безпеки (ISO/IEC 27002:2013; Cor 1:2014, IDT)», Постанови правління Національного банку України №95 від 28 вересня 2017 р. «Про затвердження Положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі України», Постанови правління Національного банку України № 178 від 12 серпня 2022 р. «Про затвердження Положення про організацію кіберзахисту в банківській системі України та внесення змін до Положення про визначення об'єктів критичної інфраструктури в банківській системі України» тощо.
1.4. *Політика* є обов'язковою для виконання всіма співробітниками Банку.
1.5. *Політика* набирає чинності з дати її затвердження рішенням Правління Банку. Зміни та доповнення до *Політики* затверджуються рішенням Правління Банку.
1.6. Перегляд *Політики* проводиться по мірі необхідності. Підставою для внесення змін до *Політики* можуть бути: зміни в бізнес-процесах, організаційно-штатній структурі, інформаційній інфраструктурі та/або впровадження нових інформаційних технологій, а також зміни в законодавчих, регуляторних та інших нормах тощо.
1.7. У разі невідповідності будь-якої частини цієї *Політики* чинному законодавству України або нормативно-правовим актам Національного банку України, у т.ч. у зв'язку з прийняттям нових законодавчих актів України або нових нормативно-правових актів Національного банку України, ця *Політика* буде діяти лише в тій частині, яка не суперечитиме чинному законодавству України або нормативно-правовим актам Національного банку України.

2. СФЕРА ЗАСТОСУВАННЯ ПОЛІТИКИ

2.1. Ресурси СУІБ Банку, для яких організовується та забезпечується інформаційна безпека:
2.1.1. матеріальні ресурси – 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), приміщення, виробниче обладнання, інші технічні засоби тощо;
2.1.2. інформаційні ресурси – інформація та дані у будь-якому вигляді, що отримуються, зберігаються, обробляються, передаються, у тому числі знання співробітників, партнерів Банку, бази даних та файли, документація, посібники користувача, навчальні матеріали, описи процедур, архівована інформація тощо;
2.1.3. 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 співробітниками та системами для роботи та взаємодії з клієнтами та іншими внутрішніми та зовнішніми системами тощо;
2.1.4. 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 співробітники), послугами яких користується Банк для отримання, використання, передачі та знищення ресурсів.

2.2. В Банку складаються і підтримуються в актуальному стані перелік важливих ресурсів та перелік критичних бізнес-процесів, до яких ці ресурси залучені.

3. ПЕРЕЛІК ОСНОВНИХ ПРИНЦИПІВ ТА ВИМОГ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

3.1. Основними принципами інформаційної безпеки в Банку є:
3.1.1. Системний (комплексний) підхід до забезпечення інформаційної безпеки;
3.1.2. Безперервність процесу удосконалення та розвитку інформаційної безпеки шляхом обґрунтування та реалізації раціональних засобів, методів, заходів із застосуванням найкращого міжнародного досвіду;
3.1.3. Своєчасність та адекватність заходів захисту від реальних та потенційних загроз інформаційній безпеці;
3.1.4. Підтримка та контроль за впровадженням, функціонуванням та розвитком СУІБ з боку Наглядової Ради та Правління Банку;
3.1.5. Достатність ресурсів, в тому числі фінансових, для впровадження, функціонування та сталого розвитку СУІБ;
3.1.6. Ризик-орієнтований підхід до інформаційної безпеки, визначення для кожного ресурсу можливих ризиків інформаційної безпеки та шляхів їх мінімізації.

3.2. Основними вимогами інформаційної безпеки в Банку є:
3.2.1. Чітке визначення спеціальним внутрішнім документом Банку інформації з обмеженим доступом, включаючи зміст інформації, засоби (апаратні, програмні, інші технічні та нетехнічні) її створення, зберігання, передавання засобами інфокомунікацій, копіювання, перетворення, обробки, знищення тощо, типи носіїв (паперові, електронні, вбудовані, змінні, мобільні, письмові, усні, і будь які інші);
3.2.2. Підтримання належного захисту інформації всіх вище перелічених типів інформації для всіх видів носіїв інформації, із забезпеченням її цілісності, конфіденційності, доступності та спостережності;
3.2.3. Ефективний моніторинг функціонування СУІБ, реєстрація та опрацювання інцидентів СУІБ;
3.2.4. Вимірюваність ефективності заходів СУІБ з періодичністю, достатньою для якісного розвитку, вдосконалення та вжиття заходів;
3.2.5. Прогнозування потенційних загроз і забезпечення готовності до їх виникнення через усунення (за можливості), навчання фахівців, складання конкретних планів забезпечення безперервної діяльності Банку в загрозливих умовах;
3.2.6. Забезпечення фізичної безпеки інфраструктури Банку;
3.2.7. Залучення всіх підрозділів, всіх співробітників Банку до забезпечення інформаційної безпеки;
3.2.8. Забезпечення дотримання вимог інформаційної безпеки всіма контрагентами Банку, включаючи аутсорсингових, на основі закріплених в договорах положень, які відповідають цій Політиці і іншим документам СУІБ.
3.3. Вимоги інформаційної безпеки доповнюються та деталізуються та конкретизуються документами СУІБ, які містять також опис практичної реалізації засобів, методів, заходів дотримання цих вимог.

4. ВІДПОВІДАЛЬНІСТЬ

4.1. Наглядова рада і Правління Банку чітко розуміють, що інформаційна безпека Банку є основою життєдіяльності Банку.
4.2. Наглядова рада і Правління Банку сприяють організаційно та фінансово впровадженню, контролю та підтримці прийнятої Політики.
4.3. Документи СУІБ розробляються відділом інформаційної безпеки Банку з залученням інших структурних підрозділів Банку за відповідними напрямками діяльності, погоджуються Комітетом СУІБ та затверджуються Правлінням Банку.

4.4. В Банку створений та постійно працює колективний керівний орган - Комітет СУІБ, який відповідає за впровадження та функціонування СУІБ.
4.5. Рішення Комітету СУІБ є обов'язковими для виконання усіма співробітниками Банку.
4.6. Всі співробітники Банку обов'язково ознайомлюються з Політикою, під підпис.
4.7. Всі співробітники Банку обов'язково ознайомлюються з іншими документами СУІБ, під підпис, у межах їх повноважень, з метою забезпечення розуміння і дотримання вимог інформаційної безпеки.
4.8. Кожний співробітник 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, документами СУІБ та іншими внутрішніми документами Банку.