Додаток 1
до Постанови Правління №П-153/2 від 10.08.2018 р.

Політика інформаційної безпеки АТ «Райффайзен Банк Аваль»

Зміст

1. Загальні положення

1.1. Вступ

Безпека і захищеність інформації є основними передумовами для забезпечення очікуваної ефективності бізнесу, його сталого розвитку та стійкості до зовнішніх та внутрішніх загроз Інформаційної безпеки.

Інформаційна безпеки є невід'ємною складовою діяльності АТ «Райффайзен Банк Аваль» (надалі - Банк) і стосується кожного працівника, технології, інфраструктури, продукту, процесу.

Політика інформаційної безпеки АТ «Райффайзен Банк Аваль» (надалі - Політика) регламентує функціонування системи управління інформаційною безпекою відповідно до законодавства України, з урахуванням вимог міжнародних та внутрішньодержавних платіжних систем та систем переказу коштів, а також нормативних документів Raiffeisen Bank International Group (надалі – Група RBI).

Ця Політика є основою для загальних процесів забезпечення Інформаційної безпеки у Банку та встановлює основний підхід до забезпечення безпеки активів Банку: Інформаційних ресурсів та систем, Інфраструктури Банку, персоналу, процесів, продуктів і послуг, що надаються клієнтам, з метою забезпечення їх Конфіденційності, Цілісності та Доступності.

1.2. Сфера регулювання

Процес забезпечення Інформаційної безпеки охоплює усі аспекти діяльності Банку та застосовуються до всіх бізнес-процесів/банківських продуктів Банку.

Ця Політика є обов'язковою до виконання усіма працівниками Банку, а також призначена для застосування клієнтами, партнерами, постачальниками та іншими контрагентами Банку.

1.3. Терміни

У цій Політиці терміни викладені в наступному значенні:

Банк – АТ «Райффайзен Банк Аваль»

Доступність - властивість інформації, яка полягає в тому, що авторизований користувач і/або процес може отримати доступ до інформації у визначений проміжок часу.

Загроза Інформаційної безпеки - наявні чи потенційно можливі явища, випадкові чинники (помилка персоналу, неправильне функціонування технічних засобів, природні чинники,

наприклад, пожежа або стихійні лиха), або навмисні дії, які можуть привести до порушень основних властивостей активів та ресурсів.

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

Інформаційна система - програмний (програмно-апаратний) комплекс для забезпечення створення, обробки, передачі та зберігання належної Банку інформації у електронному вигляді.

Інформаційний ресурс - інформація (у будь-якому форматі та вигляді, як електронний або паперовий, та/або Інформаційна система, в якій ця інформація обробляється та зберігається.

Інфраструктура Банку - сукупність взаємопов'язаних обслуговуючих структур таких як Інформаційні системи та ресурси, телекомунікаційні мережі, засоби захисту та інші, які складають та/або забезпечують основу для вирішення завдань щодо функціонування Банку.

Конфіденційність - властивість інформації, яка полягає в тому, що інформація не може бути отримана неавторизованим користувачем і/або процесом.

Підрозділ Інформаційної безпеки – працівники Управління інформаційної безпеки Департаменту правового забезпечення, комплаєнсу та інформаційної безпеки.

Підрозділи інформаційних технологій – Департамент підтримки IT систем, Департамент розробки та тестування програмного забезпечення, Департамент планування та стратегії інформаційних технологій.

Цілісність - властивість інформації, яка полягає в тому, що інформація не може бути модифікована неавторизованим користувачем і/або процесом.

1.4. Законодавство. Нормативні документи Банку

Ця Політика розроблена відповідно до:

- Закону України «Про банки і банківську діяльність» від 07.12.2000 р. № 2121-III;
- Нормативного документу Групи РБІ REG-2016-0065 Group IT Security.

2. Цілі та завдання Інформаційної безпеки

Усі дії щодо забезпечення Інформаційної безпеки повинні відповідати потребам бізнесу, бути обґрунтованими з комерційної, технічної та організаційної точок зору.

Основними цілями Інформаційної безпеки є:

- Конфіденційність інформації та даних;
- Цілісність інформації, даних та процесів;
- Доступність інформації, даних, систем, процесів і усіх необхідних ресурсів;
- підтримка реалізації бізнес-стратегії Банку щодо аспектів Інформаційної безпеки;
- захист Інформаційних ресурсів Банку від зовнішніх та внутрішніх, навмисних та ненавмисних загроз Інформаційної безпеки;
- захист законних інтересів Банку від протиправних дій, розголошення, втрати, витоку, спотворення та знищення класифікованої інформації, порушення роботи Інформаційних систем, технічних засобів та бізнес-процесів.

3. Принципи Інформаційної безпеки

3.1. Основні принципи Інформаційної безпеки

Основними принципами Інформаційної безпеки є:

- системний, комплексний, процесний та ризик-орієнтований підхід до забезпечення Інформаційної безпеки;

- безперервний процес удосконалення та розвитку Інформаційної безпеки, адаптація до нових інформаційних технологій та рішень;
- планування та реалізація рішень з Інформаційної безпеки як складової частини архітектури Інформаційних систем, сервісів та послуг;
- впровадження як превентивних заходів так і процедур оперативного реагування на непередбачені обставини;
- підтримка Інформаційної безпеки як частини корпоративної культури Банку та щоденного бізнесу.

3.2. Основні правила та вимоги Інформаційної безпеки

У Банку має бути:

- забезпечений постійний контроль ефективності впроваджених заходів Інформаційної безпеки та механізмів забезпечення безпеки в Інформаційних системах.
- визначений перелік критичних бізнес-процесів, Інформаційних ресурсів, які забезпечують їх функціонування, та заходів, необхідних для їх належного захисту;
- визначені вимоги та параметри безпеки до Інформаційних систем, бізнес-додатків, які впроваджуються в Банку;
- забезпечений відповідний рівень захисту для кожної з властивостей інформації (Цілісність, Конфіденційність, Доступність), в залежності від класифікації інформації. У першу чергу, це стосується "банківської таємниці", персональних даних клієнтів, "комерційної таємниці" та іншої конфіденційної інформації, класифікованої згідно з встановленими вимогами.

Доступ персоналу Банка до Інформаційних систем повинен бути заснований на ролевій моделі доступу з урахуванням принципу надання мінімальних повноважень, необхідних для виконання функціональних обов'язків та завдань.

Розробка, введення в експлуатацію та виведення з експлуатації Інформаційних систем та обладнання повинно здійснюватися за встановленою процедурою.

Для зберігання та обробки даних, а також забезпечення функціонування окремих банківських сервісів можуть використовуватися хмарні технології у відповідності до законодавства України та з реалізацією належного рівня захисту інформації.

Банк повинен розробляти вимоги з Інформаційної безпеки для третіх сторін, які надають Банку послуги з IT аутсорсингу, розробки, впровадження, аудиту Інформаційних систем і ресурсів, а також отримують від Банку інформацію з обмеженим доступом. Ці вимоги, відповідальність та контроль за їх виконання вищезазначеними третіми сторонами визначаються в угодах (договорах) з цими сторонами.

3.3. Дотримання вимог законодавства

Банк неухильно дотримується вимог законодавства України, нормативно-правових актів та регулятивних документів Національного банку України, нормативних документів Групи RBI, договірних умов з клієнтами та третіми сторонами.

У випадку виникнення суперечностей між законодавством України та корпоративними вимогами Групи RBI, перевага надається законодавству України.

4. Ролі та відповідальність

4.1. Управління Інформаційною безпекою

Правління Банку затверджує цю Політику та інші нормативні документи Банку з Інформаційної безпеки, здійснює контроль та приймає рішення щодо виділення необхідних ресурсів і фінансування заходів та/або проектів з Інформаційної безпеки Банку.

Підрозділ Інформаційної безпеки визначає та впроваджує вимоги з Інформаційної безпеки Банку, забезпечує функціонування та використання засобів Інформаційної безпеки, організовує належне навчання з питань Інформаційної безпеки для працівників Банку,

здійснює контроль виконання, вдосконалення та підтримку цієї Політики в актуальному стані, а також аналіз та звітування щодо стану Інформаційної безпеки.

Підрозділи інформаційних технологій у лінійній та проектній діяльності повинні керуватися основними вимогами Інформаційної безпеки та забезпечувати відповідність процесів розробки, налаштування, підтримки функціонування Інформаційних систем у відповідності до деталізованих вимог нормативних документів Групи RBI та нормативних документів Банку з питань Інформаційної безпеки.

4.2. Відповідальність працівників за Інформаційну безпеку

Працівники Банку несуть персональну відповідальність за виконання вимог законодавства України та нормативних документів Банку з питань Інформаційної безпеки, зокрема збереження банківської таємниці, персональних даних клієнтів та іншої конфіденційної інформації Банку, підтримку відповідного рівня Інформаційної безпеки при виконанні своїх посадових обов'язків.

5. Перегляд Політики

Політика переглядається щорічно в першому кварталі року. Причинами позачергового внесення змін до Політики можуть бути зміни в організації операційної діяльності, Інфраструктурі Банку та/або впровадженні нових Інформаційних технологій, а також змінах в законодавстві України, регуляторних та інших документах.