Universal Bank

Партнер сьогодні. Партнер назавжди.

ПОЛІТИКА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ АТ «УНІВЕРСАЛ БАНК»

Київ, 2021

Політика інформаційної безпеки

TAS Universal Bank
Партнер сьогодні. Партнер назавжди.

Основними принципами

Політики інформаційної безпеки є:

- ✔ підтримання належного захисту інформації із забезпеченням її цілісності, конфіденційності, доступності. Це в першу чергу стосується інформації з обмеженим доступом, яка відноситься до категорії “банківська таємниця”, “комерційна таємниця” та іншої конфіденційної інформації;

- ✔ мінімальна достатність прав і повноважень, необхідних працівникам для виконання своїх службових обов’язків (обмеження доступу персоналу до ресурсів Банку (інтернет, ОДБ,електронна пошта, програмне забезпечення, канали зв’язку, апаратні засоби, приміщення тощо)).

Повна версія документу →

Ïîë³òèêà ²Á

Політика інформаційної безпеки

TAS Universal Bank
Партнер сьогодні. Партнер назавжди.

Цілями Політики інформаційної безпеки є:

- ❖впровадження та ефективне функціонування СУІБ, спрямованої на захист інформаційних ресурсів та активів Банку від зовнішніх і внутрішніх загроз та загроз, які пов’язані з навмисними та ненавмисними діями його працівників чи третіх осіб;
- ❖забезпечення безперервної роботи Банку;
- ❖забезпечення цілісності, доступності та конфіденційності інформації;
- ❖мінімізацію операційних ризиків і ризиків ІБ;
- ❖впровадження необхідних заходів для запобігання виникненню інцидентів в майбутньому;
- ❖створення і підтримка позитивної репутації Банку при роботі з клієнтами.

Політика інформаційної безпеки

TAS Universal Bank
Партнер сьогодні. Партнер назавжди.

Політика інформаційної безпеки є багатовимірною та такою, що спрямована на реалізацію заходів безпеки для захисту ресурсів Банку від загроз принаймні у наступних площинах:

- ✔ організація інформаційної безпеки (полягає зокрема в розробці стратегії розвитку СУІБ, створенні інструментів та політик, необхідних для запобігання, виявлення, документування та протидії загрозам інформації);
- ✔ управління ресурсами Банку в сфері інформаційної безпеки;
- ✔ управління людськими ресурсами (заходи безпеки при прийому на роботу персоналу, визначення рівня компетентності та обізнаності працівників у питаннях ІБ , навчання та комунікації з питань СУБ);
- ✔ фізична безпека та безпека інфраструктури;
- ✔ управління комунікаціями та функціонуванням (забезпечення захисту інформації в мережах та захист засобів оброблення інформації, що їх підтримує; забезпечення процесного підходу до розробки, реалізації, експлуатації, моніторингу, аналізу, супроводу та вдосконалення СУІБ);
- ✔ контроль доступу (доступу в приміщення, до інформації, допуску до роботи, до систем тощо);
- ✔ придбання, розроблення та підтримка інформаційних систем захисту ІБ;
- ✔ управління інцидентами інформаційної безпеки;
- ✔ сприяння управлінню безперервністю бізнесу;
- ✔ відповідність – виконання вимог правового і організаційного характеру.

Політика інформаційної безпеки

TAS Universal Bank
Партнер сьогодні. Партнер назавжди.

Основними об’єктами застосування Політики інформаційної безпеки є наступні активи Банку:

- ***інформаційні активи***: інформація і дані в будь-якому вигляді, що отримуються, зберігаються, обробляються, передаються, в т.ч. знання працівників і партнерів Банку, бази даних і файли, документація, інструкції для користувачів та учбові матеріали, описи процедур, архівована інформація тощо;
- ***програмне забезпечення***: прикладне, системне, сервісне та інше програмне забезпечення, незалежно від форми отримання (придбане, власної розробки, таке, що знаходиться у вільному доступі), що використовується в Банку працівниками та системами для роботи і взаємодії з клієнтами та іншими системами, як внутрішніми, так і зовнішніми;
- ***людські ресурси***: штатні та позаштатні працівники Банку;
- ***фізичні активи***: апаратні засоби ІТ (сервери, робочі станції, міжмережеві екрани, принтери, копіювальне та телекомунікаційне обладнання, маршрутизатори, АТС, факси, модеми тощо), носії даних (диски, флеш-пам’ять та інші накопичувачі інформації), меблі, приміщення, виробниче обладнання тощо;
- ***сервісні активи:*** обчислювальні та комунікаційні сервіси (Інтернет, електронна пошта, канали зв’язку тощо), інші допоміжні сервіси (опалення, освітлення, енергопостачання, кондиціонування повітря, системи сигналізації та спостереження тощо), всі послуги, пов’язані з отриманням, наданням, використанням, передачею і знищенням активів, а також всі фізичні та юридичні особи (та їх працівники), які надають такі послуги Банку.

Політика інформаційної безпеки

TAS Universal Bank
Партнер сьогодні. Партнер назавжди.

Вимоги до паролю:

- довжина пароля має бути не менше 8 символів;
- пароль має містити символи мінімум 3-х груп: маленькі та або великі літери, цифри та символи (@, #, $, &, *, % ;
- пароль не повинен містити комбінації символів, що легко вгадуються або є
- стандартними (ім’я, прізвище користувача, набори символів, що розташовані
- підряд на клавіатурі чи в алфавіті, слова на зразок USER, PASSWORD і т.д.);
- пароль повинен бути відомий тільки його власнику!
- Зберігати паролі в явному вигляді на засобах обчислювальної техніки (комп'ютер, планшет, ноутбук, смартфон та інше), а також на паперовому носії – **ЗАБОРОНЕНО.**

Політика інформаційної безпеки

TAS Universal Bank
Партнер сьогодні. Партнер назавжди.

- Особисті паролі користувачів визначаються користувачами самостійно (при першому вході користувача в систему або наступній заміні пароля) або встановлюються централізовано при створенні облікового запису, після чого повідомляється користувачу.
- Під час введення паролів співробітникам необхідно виключити можливість його підглядання сторонніми особами. У разі компрометації або підозри компрометації пароля необхідно повідомити про це Управління інформаційної безпеки і негайно змінити пароль.
- Логін користувача формується як перша літера його імені та п‘ять перших літер його прізвища на англійській мові. Даний ідентифікатор доповнюється табельним номером працівника, який видається системою кадрового обліку Банку.
- **Користувач не має права повідомляти свій особистий пароль та передавати інші засоби аутентифікації будь-кому та будь якими засобами коммунікацій.**
- Користувач несе персональну відповідальність за збереження свого пароля та/або інших засобів аутентифікації.
- **Користувач несе персональну відповідальність за будь-які дії в системі, що виконані з використанням засобів аутентифікації цього користувача.**

Політика інформаційної безпеки

TAS Universal Bank
Партнер сьогодні. Партнер назавжди.

- Пароль змінюється особисто користувачем при його першому вході в систему.
- Пароль для першого входу генерується адміністратором служби Активного каталогу та повідомляється користувачу.
- При зміні пароля, нове значення пароля повинно відрізнятися від старого значення як мінімум в одному символі, і не повинно повторювати значення п‘яти останніх паролів.
- Штатна заміна паролів повинна проводитись користувачами регулярно, але не рідше, ніж раз на 42 дні.
- Автоматичне блокування облікового запису користувача відбувається після 3-х невдалих спроб вводу пароля.

Політика інформаційної безпеки

TAS Universal Bank
Партнер сьогодні. Партнер назавжди.

Політика «Чистого робочого столу» та «Чистого екрану» спрямована на забезпечення додаткового захисту інформації в приміщеннях Банку, а саме:

- «чистого столу» відносно робочих місць працівників Банку; паперових носіїв інформації; змінних електронних носіїв інформації (флеш-диски, дискети, CD, токени тощо);
- «чистого екрану» відносно автоматизованих робочих місць працівників Банку; засобів обробки інформації (автоматизованих робочих місць) з метою зменшення ризиків неавторизованого доступу; втрати й ушкодження інформації як під час операційного банківського дня, так і при позаплановій роботі.

- Працівники Банку повинні утримувати своє робоче місце в чистоті.
- Всі працівники Банку повинні дотримуватися правила, що на робочому столі сутні тільки документи, необхідні в даний час для виконання функціональних ків.
- Носії інформації з обмеженим доступом (копії документів, знімні і мобільні строї, носії ключової інформації) повинні зберігатися в упорядкованому вигляді в ізованих місцях зберігання (наприклад, сейфах, шафах, що закриваються на ощо).
- Працівники Банку не повинні залишати і не повинні зберігати на робочих місцях нагляду, як у робочий, так і в неробочий час документи та носії інформації з ним доступом, а також іншу цінну інформацію.

Політика інформаційної безпеки

TAS Universal Bank
Партнер сьогодні. Партнер назавжди.

- При необхідності покинути робоче місце працівники Банку мають завершити сеанс роботи в ІС (заблокувати або закрити додаток), а також захистити екран і клавіатуру механізмом блокування, який контролюється паролем, токеном або подібним механізмом аутентифікації користувача (відключити токен або, при його відсутності, натиснути Ctrl-Alt-Del і вибрати пункт «Блокувати комп'ютер»). У час, коли комп'ютери і термінали не використовуються, вони повинні бути захищені блокуванням клавіатури, паролями або іншими заходами безпеки. Після завершення роботи персональні комп’ютери повинні бути вимкненими.
- При роботі з інформацією з обмеженим доступом повинна виконуватися умова, що зображення на моніторі не потрапляє у поле зору сторонніх, не допущених до такої інформації осіб.
- У Банку забезпечується безпека інформації в точках прийому/відправки кореспонденції Банку, а також безпека використання принтерів, сканерів, факсів, копіювальних апаратів, іншої офісної техніки.
- Техніка, на якій роздруковується інформація з обмеженим доступом, розміщується в захищеному місці або розташовується безпосередньо біля робочого місця працівника Банку, який працює з такою інформацією.

TAS Universal Bank
Партнер сьогодні. Партнер назавжди.