

Wymagania Polityki bezpieczeństwa informacji w SPÓŁCE AKCYJNEJ „KREDOBANK”

W celu zapewnienia możliwie najwyższego poziomu bezpieczeństwa usług i produktów bankowych dostarczanych Klientom Banku oraz wewnętrznych procesów, infrastruktury, ICT i przetwarzanych informacji Bank wdrożył System Zarządzania Bezpieczeństwem Informacji (SZBI) odpowiednio do:

- normatywnych aktów prawnych Narodowego Banku Ukrainy,
- standardów: DSTU ISO/IEC 27001:2023 (ISO/IEC 27001:2022, IDT) „Bezpieczeństwa informacyjnego, cyberbezpieczeństwo oraz ochrona poufności. System Zarządzania Bezpieczeństwem Informacji. Wymagania”; DSTU ISO/IEC 27002:2023 (ISO/IEC 27002:2022, IDT) Bezpieczeństwa informacyjnego, cyberbezpieczeństwo oraz ochrona poufności. Środki sprawowania kontroli za bezpieczeństwem informacji;
- wymagań przewidzianych w obowiązującym ustawodawstwie oraz w przepisach wewnętrznych SPÓŁKI AKCYJNEJ KREDOBANK (dalej – Bank);
- wymagań organizacji kartowych i systemów płatniczych, których Bank jest uczestnikiem;
- międzynarodowych standardów w zakresie bezpieczeństwa informacji, cyberbezpieczeństwa oraz bezpieczeństwa informacji w środowisku chmurowym, powszechnie stosowanych w międzynarodowej praktyce zasad zapewnienia bezpieczeństwa informacji oraz cyberochrony;
- wymagań wynikających z zawartych umów.

Poprzez wdrożenie, wspieranie i rozwój SZBI, Bank zobowiązuje do wykonywania wymogów bezpieczeństwa informacji i stałego udoskonalenia SZBI.

1. Zarząd Banku jest świadomy, że obecna i przyszła pozycja Banku na rynku finansowym zależy od:
 - szybkości, efektywności i dokładności identyfikacji zagrożeń/cyberzagrożeń oraz sprzyjających warunków dla działalności Banku;
 - oszacowania prawdopodobieństwa ich wystąpienia;
 - oceny ich wpływu na ciągłość, jakość i zgodność z ustawodawstwem procesów biznesowych Banku, a także wpływu na pozycję rynkową i wizerunek Banku;
 - efektywności doboru i wdrażania odpowiednich działań zapobiegających zagrożeniom/ cyberzagrożeniom lub ograniczających ich negatywne skutki;
 - trafności doboru i implementacji rozwiązań zwiększających prawdopodobieństwo wykorzystania możliwości;
 - głębokiej transformacji cyfrowej we wszystkich aspektach działalności, odważnych zmian w modelu operacyjnym i modelu dystrybucji;
 - dywersyfikacji i dyscypliny w zakresie zarządzania ryzykiem i cyberbezpieczeństwa, odporności na szoki rynkowe.
2. Ze względu na to, że charakter zagrożeń w działalności bankowej zmienia się w kierunku cyberzagrożeń, to Zarząd Banku szczególną uwagę kieruje na zapewnienie bezpieczeństwa informacji i cyberochronę ICT Banku oraz przetwarzanych w nich danych, a także uznaje za konieczne przyjęcie całościowego, systemowego podejścia do zarządzania bezpieczeństwem informacji w Banku.
3. Funkcjonowanie systemu cyberochrony opiera się na następujących zasadach:
 - 1) proporcjonalność i adekwatność podejmowanych działań w zakresie cyberochrony w stosunku do rzeczywistych oraz potencjalnych cyberzagrożeń;
 - 2) priorytetyzacja działań zapobiegawczych;
 - 3) minimalizacji cyberryzyka w działalności banku;
 - 4) przestrzegania wymogów normatywnych aktów prawnych Narodowego Banku w kwestiach bezpieczeństwa informacji i cyberochrony, rekomendacji Narodowego Banku na podstawie wyników kontroli;

5) ciągłe wsparcie ze strony Zarządu Banku cyberodporności banku poprzez organizację efektywnego zarządzania cyberryzykiem.

4. Cele bezpieczeństwa informacji

Zasady wdrożone przez Bank, wynikające z Systemu Zarządzania Bezpieczeństwem Informacji, powinny zapewnić osiągnięcie następujących celów bezpieczeństwa informacji:

- **Zgodność z wymaganiami ustawodawstwa.** Podczas przetwarzania informacji przez Bank, a zwłaszcza organizacja jej ochrony, powinna być zgodna z obowiązującym ustawodawstwem Ukrainy.
- **Dostępność informacji.** Informacja i środki jej opracowania są dostępne dla osób upoważnionych. Bank zapewnia akceptowalny poziom dostępności informacji z uwzględnieniem wymagań ustawodawstwa oraz działalności operacyjnej Banku.
- **Poufność informacji.** Informacja jest dostępna wyłącznie dla osób i procesów, które mają odpowiednie prawa dostępu do nich. Prawa te wynikają w szczególności z przynależności informacji (informacja Klientów Banku), a także z obowiązków i zadań wykonywanych na rzecz Banku, przez pracowników i usługodawców Banku.
- **Integralność informacji.** Bank stosuje środki organizacyjne i techniczne, które chronią dokładność i kompletność informacji oraz chronią prawidłowe funkcjonowanie mechanizmów przetwarzających informacje. W szczególności informacje są chronione przed nieautoryzowanymi zmianami.
- **Nadzór.** Zapewnienie możliwości identyfikowania użytkowników i procesów, a także zapisywania działań użytkowników i procesów dotyczących tych informacji w celu zapobiegania i/lub badania naruszeń polityki bezpieczeństwa.
- **Zastosowanie zasad bezpiecznego przetwarzania informacji.** Przetwarzanie informacji i wykorzystanie środków jej przetwarzania odbywa się zgodnie z ustalonymi zasadami. Zasady obowiązujące zewnętrzne podmioty gospodarcze są realizowane na podstawie umów zawartych z Bankiem.
- **Nadzór nad ochroną informacji.** Bank kontroluje czy sposób przetwarzania informacji jest zgodny z wymaganiami w zakresie ochrony informacji. W przypadku potwierdzenia niezgodności w odpowiednim terminie podejmowane są działania zmierzające do jej usunięcia.
- **Odpowiednia ochrona informacji i środków jej przetwarzania w zakresie poziomu ryzyka.** Dobór środków ochrony wynika z zarządzania ryzykiem informacyjnym w Banku. Dzięki takiemu podejściu możliwe jest zapewnienie efektywności procesów informacyjnych.
- **Odpowiednia optyimizacja środków ochrony odpowiednio do potrzeb Banku.** Poprzez zarządzanie ryzykiem, audytem, przeglądem i pomiarem efektywności, Bank ustala czy środki ochrony organizacyjnej i technicznej są optymalne dla wymagań bezpieczeństwa i działalności operacyjnej Banku.
- **Zapewnienie szybkiej i efektywnej reakcji na naruszenie bezpieczeństwa informacji.** Bank niezwłocznie reaguje na wszelkie oznaki naruszenia bezpieczeństwa informacji/cyberbezpieczeństwa, co pozwala zminimalizować prawdopodobne negatywne skutki zdarzenia i podjąć natychmiastowe działania naprawcze.

5. Podstawowe zasady zapewnienia bezpieczeństwa informacji

Organizacja bezpieczeństwa informacji Banku opiera się na następujących fundamentalnych zasadach:

- **Zasada minimalnych uprawnień:** dostęp pracowników Banku i innych użytkowników systemów informatycznych do zasobów informacyjnych sieci komputerowej Banku jest zorganizowany w taki sposób, aby nadawać tylko te uprawnienia, które są niezbędne do wykonania zadań służbowych.
- **Zasada wiedzy koniecznej:** każdy pracownik lub osoba współpracująca z Bankiem posiada wiedzę o informacji lub o zasobach informacyjnych Banku, środkach ich przetwarzania oraz sposobach ich ochrony, która jest niezbędna do wykonywania powierzonych zadań i obowiązków. Osoby postronne mają dostęp wyłącznie do tych informacji, które Bank określi jako publiczne (jawne).
- **Zasada podziału obowiązków:** wykonanie zadań krytycznych z punktu widzenia bezpieczeństwa zasobów finansowych i informacyjnych Banku, systemów informacyjno-telekomunikacyjnych i usług bankowych są tak organizowane, aby ich realizacja wymagała udziału więcej, niż jednej osoby („zasada dwóch rąk”).
- **Zasada sankcjonowania działań:** zabronione są te działania pracowników Banku, które są jawnie niedozwolone przez ustawodawstwo, dokumenty normatywne NBU, wewnętrznymi rozporządzeniami lub przepisami wewnętrznymi.
- **Zasada prawomocności:** SZBI Banku bierze pod uwagę wymagania obowiązującego ustawodawstwa Ukrainy, a także wymagania międzynarodowych wymogów normatywnych w zakresie bezpieczeństwa informacji.

- **Zasada spójności i jedności:** cele i zadania bezpieczeństwa informacji odpowiadają strategicznym celom i zadaniom biznesowym Banku, a zarządzanie bezpieczeństwem informacji jest nieodłączną częścią zarządzania Bankiem.
 - **Zasada adekwatności i efektywności:** środki ochrony zasobów informacyjnych wprowadzane są odpowiednio do kategorii krytyczności, tj. kategorie klasyfikacji i poziomu ryzyka zasobu informacyjnego, opierając się na zasadach oceny ryzyka przyjętego przez Bank.
 - **Zasada praktyczności:** środki ochrony zasobów informacyjnych powinny być praktyczne i zachowywać równowagę między zdolnością do pracy i ochroną systemów informatycznych
 - **Zasada ciągłości:** bezpieczeństwo informacji jest nieprzerwanym procesem przeciwstawiania się zagrożeniom/cyberzagrożeniom i zarządzania ryzykami charakterystycznymi dla obszaru działalności Banku.
 - **Zasada odpowiedzialności:** kierownictwo Banku wszystkich poziomów, pracownicy, dostawcy i inne trzecie strony, które mają dostęp do zasobów informacyjnych Banku, są zobowiązani przestrzegać wymagań przepisów wewnętrznych Banku w zakresie bezpieczeństwa informacji i ponoszą osobistą odpowiedzialność za ich wykonanie
 - **Zasada ciągłego udoskonalenia:** wdrożony w Banku System Zarządzania Bezpieczeństwem Informacji zawiera mechanizmy i wskaźniki do pomiaru i kontroli efektywności systemu zarządzania oraz wdrożonych zabezpieczeń, co umożliwia Bankowi racjonalne planowanie i realizowanie działań doskonalących.
 - **Zasada ochrony wielopoziomowej:** organizacja bezpieczeństwa informacji przewiduje stworzenie szeregu następujących po sobie poziomów ochrony zasobów informacyjnych i personelu Banku przed prawdopodobnymi zagrożeniami/cyberzagrożeniami:
 - poziom organizacyjno-prawny, który określa prawne i normatywne wymagania oraz zobowiązania personelu, użytkowników zasobów informacyjnych i kontrahentów Banku w zakresie bezpieczeństwa informacji;
 - poziom ochrony fizycznej, który ma na celu zapobieganie nieautoryzowanemu fizycznemu dostępowi, uszkodzeniu i wtargnięciu do służbowych pomieszczeń Banku w celu nieautoryzowanego dostępu do informacji;
 - poziom oprogramowania aplikacyjnego i narzędziowego, który odpowiada za interakcję z użytkownikiem zasobów informacyjnych;
 - poziom systemu zarządzania bazami danych, który odpowiada za przechowywanie i opracowanie danych;
 - poziom systemu operacyjnego, który odpowiada za bezpieczną i niezawodną obsługę oprogramowania aplikacyjnego i narzędziowego oraz systemów zarządzania bazami danych;
 - poziom sieci, który odpowiada za współdziałanie węzłów systemu informatycznego Banku.
 - **Zasada kompleksowości i systemowości:** bezpieczeństwo informacji Banku jest zapewniane kompleksowo, to znaczy uwzględnia wszystkie aspekty ochrony informacji, a w szczególności:
 - strategię i cele bezpieczeństwa,
 - zarządzanie zasobami informacyjnymi oraz nośnikami informacji,
 - bezpieczeństwo zasobów ludzkich,
 - zarządzanie bezpieczeństwem fizycznym i bezpieczeństwem środowiskowym,
 - zabezpieczenie relacji z dostawcami,
 - bezpieczeństwo procesów komunikacji wewnętrznych i zewnętrznych
 - zarządzanie zgodnością z wymaganiami prawnymi, regulacyjnymi i wynikającymi z umów,
 - zarządzanie incydentami bezpieczeństwa,
 - zarządzanie ciągłością biznesu,
 - bezpieczeństwo w procesach projektowania, poszukiwania, rozwoju, wdrożenia i wsparcia systemów IT,
 - bezpieczeństwo w procesach eksploatacji systemów IT.
 - 100% ujawnienie ryzyka zmian systemów pod względem ciągłości i integralności ich funkcjonowania.
- Przyjęta przez Bank systemowość podejścia do zarządzania bezpieczeństwem informacji przewiduje zapewnienie spójności procesów i działań realizowanych w zakresie bezpieczeństwa:
- z uwarunkowaniami otoczenia, w jakim funkcjonuje Bank,
 - ze strategią i celami biznesowymi Banku,
 - z wynikami oceny ryzyka i możliwości,
 - z wynikami oceny efektywności systemu zarządzania i wdrożonych środków ochrony,
 - ze wszystkimi aspektami zarządzania działalnością operacyjną i technologiami informatycznymi Banku.

6. Oprogramowanie Banku powinno odpowiadać wymaganiom dotyczącym bezpieczeństwa informacji ustawodawstwa Ukrainy, dokumentów i standardów NBU, a także międzynarodowych standardów ISO 2700X i spełniać następujące wymagania:

- występowanie wbudowanego systemu ochrony informacji, którego nie można wyłączyć i nie można przetwarzać informacji bez jego wykorzystania;
- występowanie wbudowanych mechanizmów właściwej ochrony informacji podczas jej przesyłania między różnymi podsystemami, w których przetwarzane są informacje;
- dla zautomatyzowanych systemów funkcjonujących w trybie „klient-serwer”, dostęp użytkowników do bazy danych powinien odbywać się tylko poprzez dodatkowe oprogramowanie, za pomocą którego przeprowadza się uwierzytelnienie i autoryzacja osób, które mają zezwolenie na korzystanie z tej bazy danych;
- zastosowanie wzmożonego uwierzytelnienia użytkowników usługi płatniczej;
- występowanie wbudowanych mechanizmów zapewniających jednoznaczną i niepodważalną identyfikację użytkownika na każdym sprzęcie dostępu do systemu, w każdym module lub elemencie, do którego użytkownik ma dostęp, a także podczas przeprowadzenia jakichkolwiek operacji w systemie;
- zapewnienie możliwości automatycznego blokowania konta w systemie po przekroczeniu zdefiniowanej liczby nieudanych prób wprowadzenia nieprawidłowego hasła – na dowolnym urządzeniu dostępowym do systemu; zapewnienie nieprzerwanej kontroli technologicznej całości informacji, a także składanie/sprawdzanie cyfrowego podpisu na wszystkich płatniczych dokumentach bankowych, na każdym etapie cyklu technologicznego ich opracowywania;
- zapewnienie szyfrowania elektronicznych dokumentów bankowych, które zawierają poufną informację, podczas przekazywania ich na nośnikach zewnętrznych albo w trybie online poprzez kanały telekomunikacyjne, z odpowiednim potwierdzeniem ich otrzymania; zapewnienie obowiązkowego rejestrowania wszystkich prób dostępu, wszystkich operacji i innych działań w systemie oraz zapisywanie ich w zautomatyzowanym systemie w zabezpieczonym przed modyfikacją elektronicznym rejestrze, ze stałą kontrolą jego kompletności i integralności.

7. Wymagania, o których mowa powyżej mają zastosowanie zarówno do oprogramowania nabytego przez Bank jako gotowe oprogramowanie (COTS – Commercial Off-The-Shelf), jak również do oprogramowania opracowanego przez Bank samodzielnie lub przez dostawców zewnętrznych na zlecenie Banku.

8. Bank stosuje standardy, dokumenty oraz wytyczne otwartego projektu ochrony aplikacji "Open web application security project" (OWASP) w celu opracowania bezpiecznych aplikacji

9. Bank utrzymuje wysoki poziom bezpieczeństwa informacji, opracowywanych, przechowywanych i przekazywanych za pomocą technologii chmurowych przechowywania danych.

10. W Banku działa zasada udzielenia minimalnego poziomu uprawnień podczas udzielenia dostępu do systemów informatycznych banku (w tym dostęp do uprzywilejowanych użytkowników).

11. W Banku opracowano, obowiązuje, testuje się i aktualizuje plan zapewnienia ciągłości działalności uwzględniający ciągłość funkcjonowania środków bezpieczeństwa informacji w ramach procesu zarządzania ciągłością działalności Banku, działania skierowane na wznowienie systemów informatycznych po awariach.

12. W celu zmniejszenia ryzyka powstania incydentów bezpieczeństwa informacji, w Banku podejmowane są systematyczne działania mające na celu podnoszenie poziomu świadomości personelu w zakresie bezpieczeństwa informacji, w szczególności:

- poinformowanie pracowników Banku o wprowadzanych (nowych lub zmienianych) regulacjach wewnętrznych określających zasady zapewnienia bezpieczeństwa (m.in. niniejszej Polityki) i zobowiązania pracowników do zapoznawania się z nimi oraz przestrzegania wymagań zawartych w tych dokumentach;
- przeprowadzanie dla pracowników treningów i szkoleń z zakresu bezpieczeństwa informacji;
- przeprowadzanie wewnętrznych kampanii i działań (aktywności), szczególnie po wystąpieniu poważnego incydentu bezpieczeństwa oraz w przypadku pojawienia się informacji o nowych metodach ataków na Banki i ich Klientów;
- przeprowadzanie testów i audytów bezpieczeństwa (w tym testów socjotechnicznych) oraz testów planów ciągłości działalności Banku i omawianie ich wyników z odpowiedzialnymi osobami odpowiednich komórek organizacyjnych.

13. Każdy pracownik Banku ma obowiązek informowania o wystąpieniu incydentu bezpieczeństwa informacji. Zasady i tryb powiadamiania oraz dane kontaktowe osób, które mają być powiadamiane, zostały określone w odrębnym dokumencie, szczegółowo określającym procedurę reagowania na incydenty bezpieczeństwa informacji.

14. Każdy pracownik i osoba współpracująca z Bankiem są zobowiązani do wspierania działań na rzecz osiągnięcia i utrzymywania odpowiedniego poziomu bezpieczeństwa informacji w Banku, w zakresie adekwatnym do powierzonych mu obowiązków i udzielonych uprawnień.

15. Podejmując zatrudnienie, wszyscy pracownicy Banku podpisują zobowiązanie o nieujawnianiu informacji o ograniczonym dostępie, w tym tajemnicy bankowej i danych osobowych. Pracownicy Banku zobowiązani są do nieujawniania i nieużywania dla siebie lub osób trzecich informacji o ograniczonym dostępie, o których dowiedzieli się przy wykonywaniu swoich obowiązków.