

ZASADY ZARZĄDZANIA BEZPIECZEŃSTWEM INFORMACJI JAKO PODSTAWA REALIZACJI POLITYKI BEZPIECZEŃSTWA INFORMACJI

**W CELU ZMINIMALIZOWANIA RYZYKA UTRATY DANYCH BEZPOŚREDNIO NALEŻY
ZASTOSOWAĆ ZASADY, KTÓRYCH SPEŁNIENIE MA BYĆ KLUCZEM DO
ZAPEWNIENIA KOMPLEKSOWEJ POLITYKI BEZPIECZEŃSTWA INFORMACJI**

Celem zapewnienia bezpieczeństwa informacji jest w szczególności:

1. Ochrona zasobów informacji.
2. Zapewnienie ciągłości działania Banku i sprawnej obsługi jego klientów i partnerów.
3. Zgodność procesu przetwarzania informacji z przepisami prawa.
4. Ochrona wizerunku Banku.

Spełnienie powyższych celów poprzez zachowanie poufności, integralności, dostępności, rozliczalności, autentyczności, niezaprzeczalności danych umożliwia współużytkowanie informacji.

Każdy, kto przetwarza dane Banku zobowiązany jest do stosowania niżej opisanych zasad bezpieczeństwa. Dodatkowo wszyscy pracownicy powinni przejść szkolenia i muszą zapoznać się z funkcjonującymi podstawowymi zasadami realizacji bezpieczeństwa informacji:

- 1) **ZASADA WIEDZY KONIECZNEJ**
w myśl której dostęp do informacji ograniczony jest do tych, które są niezbędne do prawidłowego wykonywania obowiązków na danym stanowisku. Za przestrzeganie tej zasady odpowiedzialni są kierownicy.
- 2) **ZASADA ŚWIADOMOŚCI ZBIOROWEJ**
wszyscy są świadomi konieczności ochrony zasobów, zapewnienia ich dostępności, poufności, integralności i aktywnie w tym procesie uczestniczą.
- 3) **ZASADA ŚWIADOMEJ KONWERSACJI**
polega na tym, że nie zawsze i wszędzie trzeba mówić co się wie, ale zawsze i wszędzie trzeba wiedzieć co, gdzie i do kogo się mówi.
- 4) **ZASADA ODPOWIEDZIALNOŚCI ZA ZASOBY**
każdy, kto przetwarza informacje jest odpowiedzialny za zapewnienie ich dostępności, poufności i integralności poprzez przestrzeganie procedur ich bezpiecznego przetwarzania oraz ochronę przyznaných zasobów, w tym za szkody wyrządzone w systemie informatycznym

przez nieautoryzowane oprogramowanie lub niewłaściwe korzystanie z urządzeń systemu informatycznego.

5) **ZASADA CHRONIONEGO POMIESZCZENIA**

wyraża się tym, że pod nieobecność osoby uprawnionej w pomieszczeniach (poza ogólnodostępnymi typu korytarze) nie mogą przebywać osoby postronne, po opuszczeniu pomieszczenia osoba odpowiedzialna zamyka je na klucz (bez pozostawiania kluczy w zamkach – wyjątek stanowi ewakuacja).

6) **ZASADA NADZOROWANIA KLUCZY I KART MAGNETYCZNYCH**

pobrane klucze i karty magnetyczne do pomieszczeń powinny być zawsze pod kontrolą.



Pracownicy odpowiedzialni są za należyte zabezpieczenie kluczy do ich biurek stanowiskowych i szaf biurowych, w których przechowywane są dokumenty; ostatni pracownik opuszczający dane pomieszczenie po zakończeniu pracy zamyka szafy i chowa klucze w bezpieczne, ustalone z pozostałymi współpracownikami miejsce.

Ta sama zasada dotyczy dystrybucji kart magnetycznych, którymi otwierane są dostępy do stref specjalnych np. serwerowni. Po zakończeniu prac w serwerowni przez upoważnionych pracowników karta powinna być zdeponowana w dystrybutorze kart magnetycznych i kluczy. Nadzór nad dystrybutorem powinna sprawować osoba

odpowiedzialna za nadzór dostępu do pomieszczeń

7) **ZASADA CZYSTEGO BIURKA**

wyraża się tym, że zarówno dokumentów papierowych, jak i jakichkolwiek innych nośników informacji (płyty CD, DVD, pamięci flash, USB itp.) nie pozostawia się bez nadzoru.

8) **ZASADA CZYSTEGO EKRANU**

każdorazowe opuszczenie pomieszczenia w godzinach pracy powinno zostać poprzedzone zablokowaniem komputera, każdorazowe opuszczenie stanowiska pracy w celu załatwienia czynności musi być poprzedzone zablokowaniem ekranu komputera; na wszystkich stacjach aktywny jest wygaszacz ekranu zabezpieczony hasłem, który aktywizuje się automatycznie po przekroczeniu max. 5 – 10 lub 15 minut braku aktywności. Każdy użytkownik systemu zobowiązany jest zadbać, aby po zakończeniu pracy sprzęt został poprawnie wyłączony.

9) **ZASADA CZYTEJ DRUKARKI**

wszyscy pracownicy, praktykanci i stażyści zobowiązani są do zabierania dokumentów z drukarek zaraz po ich wydrukowaniu. W przypadku nieudanej próby wydrukowania użytkownik

powinien skontaktować się z osobą odpowiedzialną za dane urządzenie lub zgłosić incydent bezpieczeństwa.

10) **ZASADA CZYSTEGO KOSZA**

nieprzydatne dokumenty, brudnopisy, zbędne kopie muszą zostać trwale zniszczone w sposób uniemożliwiający odtworzenie zawartych w nich informacji. Zasada ta dotyczy również informacji zapisanych w innej niż papierowa formie – na nośnikach elektronicznych. Do kosza na śmieci nie wyrzuca się płyt CD/DVD oraz innych nośników, powinny one zostać zniszczone w specjalistycznych niszczarkach. W przypadku, gdy będzie to niemożliwe nośniki te należy przekazać do Wydziału Informatyki celem ich utylizacji.

11) **ZASADA CZYSTEJ TABLICY**

w przypadku korzystania z tablic w salach ogólnodostępnych osoba organizująca spotkanie musi uprzątnąć wszystkie pozostałe tam materiały i wyczyścić tablice; pracownicy korzystający z tablic w biurach zobowiązani są do nie zamieszczania na tablicach informacji podlegających ochronie.

12) **ZASADA LEGALNOŚCI OPROGRAMOWANIA**

zabrania się samodzielnego instalowania oprogramowania, a także przechowywania na komputerach treści naruszających prawo.

13) **ZASADA WERYFIKACJI PRZENOŚNYCH NOŚNIKÓW DANYCH** (np. pendrive, CD, DVD)

każdy komputer wymaga przeprowadzenia skanowania przez system antywirusowy zewnętrznych nośników danych przed ich uruchomieniem.

14) **ZASADA ZGŁASZANIA ZDARZEŃ, INCYDENTÓW, NIEPRAWIDŁOWEJ PRACY SPRZĘTU**

każdy użytkownik systemu zobowiązany jest do zgłaszania do Działu Informatyki wszelkich zauważonych nietypowych zdarzeń, incydentów oraz nieprawidłowej pracy sprzętu).

15) **ZASADA MONITORINGU STANOWISKA KOMPUTEROWEGO**

każde stanowisko komputerowe jest objęte monitorowaniem działania użytkowników i oprogramowania.

16) **ZASADA ASEKURACJI – REDUNDANCJI**

polega na tym, że każdy mechanizm zabezpieczający system jest ubezpieczony drugim; w szczególnych przypadkach może zostać zastosowana większa liczba mechanizmów zabezpieczających; możliwe jest stosowanie zabezpieczeń technicznych i organizacyjnych.

17) **ZASADA KOMPLETNOŚCI**

skuteczne zabezpieczenie jest tylko wtedy, gdy stosuje się podejście kompleksowe, uwzględniające wszystkie stopnie i ogniwa ogólnie pojętego procesu przetwarzania informacji.



18) **ZASADA EWOLUCJI**

każdy system musi ciągle dostosowywać mechanizmy wewnętrzne do zmieniających się warunków zewnętrznych.

19) **ZASADA ODPOWIEDZIALNOŚCI**

używane mechanizmy muszą być adekwatne do sytuacji.

20) **ZASADA AKCEPTOWALNEJ RÓWNOWAGI**

podejmowane środki zaradcze nie mogą przekraczać poziomu akceptacji.

21) **ZASADA INDYWIDUALNEJ ODPOWIEDZIALNOŚCI**

za bezpieczeństwo poszczególnych elementów odpowiadają konkretne osoby.

22) **ZASADA OBECNOŚCI KONIECZNEJ**

prawo przebywania w określonych miejscach mają tylko osoby upoważnione.

23) **ZASADA STAŁEJ GOTOWOŚCI**

system jest przygotowany na wszelkie zagrożenia. Niedopuszczalne jest tymczasowe wyłączanie mechanizmów zabezpieczających.

24) **ZASADA NAJSŁABSZEGO OGNIWA**

poziom bezpieczeństwa wyznacza najsłabszy (najmniej zabezpieczony) element.

25) **ZASADA UPRAWNIONEGO DOSTĘPU DO INFORMACJI**

pracownik przechodzi szkolenie z zasad ochrony informacji, spełnia kryteria dopuszczenia do informacji i podpisuje stosowne oświadczenie o zachowaniu poufności.

26) **ZASADA ŚWIADOMOŚCI ZBIOROWEJ**

wszyscy pracownicy są świadomi konieczności ochrony zasobów informacyjnych Banku i aktywnie uczestniczą w tym procesie.

W celu uzyskania pełnej informacji w omawianych zakresach zapraszamy do kontaktu:

Andrzej Popiołek

Audytor Wiodący SZBI, Członek IIA Polska

+48 602 220 749 andrzej.popiolek@servus-comp.pl

Ewa Niesiołowska

Audytor Wiodący SZBI, Członek IIA Polska

+48 531 364 287 ewa.niesiolowska@servus-comp.pl

Anna Stręk

Audytor Wiodący SZBI, Członek IIA Polska

+48 781 555 025 anna.strek@servus-comp.pl





servus comp
data security



Anna Kramarczyk

Kierownik ds. projektów IT

+48 794 671 787 anna.kramarczyk@servus-comp.pl

Servus Comp Sp. z o.o. Sp.k.

ul. Mazowiecka 25/502, 30-019 Kraków

Sąd Rejonowy dla Krakowa – Śródmieście,

XI Wydział Gospodarczy Krajowego Rejestru Sądowego

NIP: 6772394344 | Regon: 362815411 | KRS: 0000582481

<https://zadbajobezpieczenstwo.pl>

<https://premiumbank.zadbajobezpieczenstwo.pl>

Nota prawna:

1. Zaprezentowany materiał jest autorskim opracowaniem i jest objęty prawem autorskim.
2. Niniejszy materiał, ani żaden jego fragment nie może być reprodukowany, przetwarzany i rozpowszechniany w jakikolwiek sposób za pomocą urządzeń elektronicznych, mechanicznych, kopiujących, nagrywających i in. do celów innych niż realizacja przedmiotowej umowy u Klienta.



Servus Comp Sp. z o.o. Sp. K.

30-019 Kraków ul. Mazowiecka 25/502

tel. 12 631-91-22

biuro@servus-comp.pl

www.premiumbank.zadbajobezpieczenstwo.pl