

Polityka

bezpieczeństwa informacji

Czego dotyczy Polityka

Polityka wprowadza system zarządzania bezpieczeństwem informacji (SZBI) w RFG i określa cele bezpieczeństwa informacji RFG, strukturę zarządzania bezpieczeństwem oraz ogólne ramy ochrony informacji, pozwalające osiągnąć niezbędny, adekwatny do zagrożeń poziom bezpieczeństwa informacji, w szczególności danych osobowych klientów, pracowników i partnerów biznesowych.

System zarządzania bezpieczeństwem informacji w RFG, jest zgodny z wymaganiami międzynarodowej normy ISO/IEC 27001:2022. Szczegółowy zakres procesów, w ramach których stosujemy SZBI, znajduje się w załączniku nr 1.

Kogo dotyczy polityka

Polityka dotyczy wszystkich pracowników/współpracowników RFG (niezależnie od formy zatrudnienia lub współpracy), a także przedstawicieli stron trzecich współpracujących z RFG, którzy zostali dopuszczeni do przetwarzania informacji lub środków służących do przetwarzania informacji.

Odpowiedzialność

dział/stanowisko	czynności w procesie
ISO (Information security officer)	Nadzór nad aktualnością i zgodnością dokumentu z wymaganiami normy ISO/IEC 27001 i przepisami prawa oraz nadzór nad realizacją określonych w polityce celów bezpieczeństwa i zasad.
IOD (Inspektor ochrony danych osobowych)	Nadzór nad aktualnością i zgodnością dokumentu z regulacjami w zakresie ochrony danych osobowych
Role oraz ich zakres odpowiedzialności zostały określone w rozdziale Role i odpowiedzialność.	

Spis treści

Definicje i skróty 2

Treść 3

Nasza Polityka	3
Jak stosować Politykę	4
Role i odpowiedzialności	5
Klasyfikacja informacji	8
Zarządzanie ryzykiem	8
Podstawowe zasady ochrony	9
Monitorowanie działań	9
Zobowiązanie do zachowania poufności	9
Reagowanie na incydenty	10
Odstępstwa	10
Egzekwowanie zasad bezpieczeństwa	10
Doskonalenie	10
Załączniki	11
Dokumenty powiązane	11
Miejsca udostępnienia	11
Metryka dokumentu	11

Definicje i skróty

W dokumencie używamy pojęć:

- **Bezpieczeństwo informacji** - zachowanie poufności, integralności i dostępności informacji.
- **ISO** - Information Security Officer.
- **IOD** - Inspektor ochrony danych osobowych.
- **RFG** – Regionalny Fundusz Gospodarczy S.A. z siedzibą w Częstochowie, Aleja Pokoju 44, 42-202 Częstochowa, KRS 0000100887, REGON 000025483, NIP 573-020-60-30.
- **My, Zarząd** - Zarząd RFG.

Treść

Nasza Polityka

1. Wprowadzamy Politykę bezpieczeństwa informacji, aby osiągnąć i utrzymać niezbędny, adekwatny do zagrożeń poziom bezpieczeństwa informacji, w szczególności danych osobowych klientów, pracowników i naszych partnerów biznesowych. Zasady ujęte w tym dokumencie muszą być stosowane niezależnie od postaci i sposobu przetwarzania informacji (danych).
2. Naszymi głównymi celami bezpieczeństwa informacji są:
 - ochrona informacji przed udostępnieniem lub ujawnieniem ich nieupoważnionym osobom, podmiotom lub procesom (poufność) oraz przed nieuprawnionymi zmianami i manipulacjami (integralność),
 - zapewnienie dostępu uprawnionym osobom, podmiotom i procesom do wszelkich informacji i usług, kiedy jest to wymagane (dostępność), w szczególności zapewnienie, że będziemy w stanie kontynuować świadczenie usług nawet w przypadku wystąpienia sytuacji awaryjnych,
 - przypisanie odpowiedzialności za ochronę sprzętu i kluczowych informacji w całym cyklu ich życia odpowiednim osobom,
 - utrzymanie zgodności z prawem i regulacjami bezpieczeństwa informacji, w tym ochrony danych osobowych (ochrona prywatności),
 - zapewnienie, że działania osoby, podmiotu mogą być przypisane w sposób jednoznaczny tylko tej osobie, podmiotowi (rozliczalność),
 - zapewnienie przestrzegania wymagań międzynarodowych standardów bezpieczeństwa informacji, m.in. ISO/IEC 27001,
 - zapewnienie przestrzegania przepisów wynikających z Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych),
 - zwiększenie poziomu ochrony w zakresie cyberbezpieczeństwa i przestrzeganie wymagań wynikających z Dyrektywy Parlamentu Europejskiego i Rady (UE) 2022/2555 w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 oraz przepisów wdrażających Dyrektywę do polskiego porządku prawnego.
3. Cele bezpieczeństwa informacji osiągamy m.in. przez:

- zapewnienie integracji bezpieczeństwa informacji z działalnością operacyjną,
 - określenie ról organizacyjnych i przypisanie odpowiedzialności za bezpieczeństwo informacji,
 - promowanie i motywowanie do odpowiedzialnego postępowania w zakresie bezpieczeństwa informacji wśród pracowników i współpracowników,
 - podejmowanie efektywnych działań w oparciu o analizę ryzyka, w szczególności stosowanie adekwatnych do poziomu ryzyka zabezpieczeń technicznych i organizacyjnych,
 - monitorowanie zmian w prawie i regulacjach oraz adekwatne dostosowywanie procedur, procesów i zabezpieczeń,
 - skuteczne zarządzanie incydentami bezpieczeństwa informacji oraz wyciąganie wniosków z ich przebiegu.
4. Niniejsza Polityka jest dokumentem nadrzędnym względem wszystkich wewnętrznych regulacji dotyczących bezpieczeństwa informacji. Szczegółowe zasady bezpieczeństwa opisujemy w Standardach bezpieczeństwa oraz przewodnikach, które mają charakter operacyjny lub techniczny.
5. Polityka, standardy oraz inne dokumenty zależne tworzą wspólnie system zarządzania bezpieczeństwem informacji, który ustanowiliśmy, wdrożyliśmy, utrzymujemy i ciągle doskonalimy zgodnie z wymaganiami normy ISO/IEC 27001. Zakres Systemu zarządzania bezpieczeństwem informacji przedstawia Załącznik nr 1. Schemat powiązanych z Polityką standardów, składających się na system zarządzania bezpieczeństwem informacji przedstawia Załącznik nr 2.
6. Deklarujemy zapewnienie niezbędnych zasobów oraz wsparcie, aby osiągać cele bezpieczeństwa informacji oraz utrzymywać i ciągle doskonalić system zarządzania bezpieczeństwem informacji.

Jak stosować Politykę

7. Polityka i zasady przez nią wprowadzone obowiązują:
- wszystkich pracowników i współpracowników RFG niezależnie od formy zatrudniania oraz inne osoby uzyskujące dostęp do danych należących do RFG,
 - podmioty zewnętrzne realizujące działania lub współpracujące z RFG na podstawie umów i porozumień.
8. Politykę i zasady należy stosować względem wszystkich zasobów informacyjnych, w szczególności w stosunku do:
- istniejących, wdrażanych obecnie lub w przyszłości systemów informatycznych,
 - zbiorów danych oraz nośników, na których te zbiory są zapisywane i przetwarzane niezależnie od typu nośnika,

- budynków i pomieszczeń, w których są lub będą przetwarzane informacje podlegające ochronie.
9. Politykę i zasady należy stosować łącznie ze standardami oraz podręcznikami bezpieczeństwa.
10. Polityka jest dokumentem jawnym. Naszą intencją jest zaznajomienie i stosowanie Polityki przez wszystkich pracowników, współpracowników oraz podmioty zewnętrzne współpracujące z RFG. Z jawności wyłączone są dokumenty zależne od niej, tj. standardy, podręczniki oraz dokumentacja operacyjna.

Role i odpowiedzialności

11. Bezpieczeństwo informacji organizujemy w oparciu o następujące role organizacyjne oraz wskazanie konkretnych odpowiedzialności:

Rola	Odpowiedzialność w zakresie bezpieczeństwa informacji
ISO - Information Security Officer	• inicjuje i koordynuje wdrażanie zabezpieczeń technicznych oraz organizacyjnych, a także przeglądy ryzyka • konsultuje projekty i zmiany biznesowe • monitoruje zmiany regulacyjne • monitoruje działania dostawców • koordynuje zarządzanie ciągłością działania • zapewnia nadzór i uczestniczy w procesie zarządzania ryzykiem • realizuje obsługę incydentów • realizuje przeglądy i audyty bezpieczeństwa • raportuje w zakresie bezpieczeństwa informacji do Zarządu • odpowiada za projektowanie i utrzymanie zabezpieczeń RFG
Inspektor ochrony danych osobowych	• informuje administratora, podmioty przetwarzające oraz pracowników o obowiązkach spoczywających na nich, wynikających z RODO

	• monitoruje przestrzeganie przepisów w zakresie ochrony danych osobowych • konsultuje zabezpieczenia • udziela na żądanie zaleceń, co do oceny skutków dla ochrony danych oraz monitoruje ich wykonanie • współpracuje i pełni rolę punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem danych osobowych • uczestniczy w procesie analizy ryzyka • konsultuje projekty i zmiany biznesowe • monitoruje zmiany regulacyjne w zakresie danych osobowych
Właściciel biznesowy (zasobu informacyjnego)	• określa zasady dostępu i postępowania z informacjami, których jest właścicielem • identyfikuje i ocenia ryzyka oraz opracowuje plany postępowania z ryzykiem • realizuje zadania z zakresu ciągłości działania
Administrator IT	• wdraża i utrzymuje zabezpieczenia techniczne • stosuje zasady zarządzania bezpieczeństwem IT • identyfikuje i podejmuje reakcję na incydenty • realizuje zadania z zakresu ciągłości działania • stosują zasady bezpieczeństwa w rozwoju i wdrażaniu systemów
Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego (CSIRT)	• ocenia pojawiające luki, podatności i ich wpływ na systemy IT • ocenia i obsługuje incydenty związane z bezpieczeństwem IT • doradza w zakresie bezpieczeństwa IT, oceny ryzyka i strategii rozwoju bezpieczeństwa IT

Zarząd	• akceptuje i jest sponsorem inicjatyw w zakresie bezpieczeństwa informacji • wyznacza Właścicieli biznesowych • uczestniczy w procesie zarządzania ryzykiem, zapewnia adekwatne aktywa oraz zatwierdza stosowane zabezpieczenia w obszarze cyberbezpieczeństwa • określa poziom akceptowalnego ryzyka • zatwierdza Politykę i Standardy
Centrum Usług Finansowo-Kadrowych	• odpowiada za realizację działań szkoleniowych oraz uświadamiających • zapewnia bezpieczeństwo w relacjach z pracownikami oraz współpracownikami
Biuro Zarządu	• sprawuje nadzór nad obiegiem i zabezpieczeniem dokumentacji
Wszyscy pracownicy	• stosują regulacje w zakresie akceptowanego użycia zasobów informacyjnych • postępują z informacjami zgodnie z przypisaną klasyfikacją

Klasyfikacja informacji

12. Wprowadzamy zasadę klasyfikowania informacji przetwarzanych w RFG wprowadzając następujący podział:

- **Informacje niewymagające ochrony** – to takie informacje, które są ogólnodostępne lub których ujawnienie nie ma żadnego wpływu na bezpieczeństwo informacji i na działalność RFG. W niektórych przypadkach (np. umieszczenie na stronie WWW) informacje mogą wymagać ochrony przed utratą integralności i/lub dostępności.

- **Informacje wymagające ochrony** – to takie informacje, których ujawnienie lub utrata integralności i dostępności ma niepożądany wpływ na bezpieczeństwo lub interes RFG, klientów, dostawców usług i innych stron trzecich. Naruszenie ochrony informacji prowadzi do naruszenia wewnętrznych regulacji, braku zgodności z umowami lub przepisami prawa. Może narazić RFG na roszczenia stron trzecich, kary przewidziane w przepisach i negatywnie wpłynąć na wizerunek RFG.
- **Informacje wymagające szczególnej ochrony** – są to informacje wymagające szczególnej ochrony ze względu na ich krytyczne znaczenie dla RFG lub wymagania umowne i prawne. Utrata bezpieczeństwa może prowadzić do znaczących konsekwencji zarządczych, finansowych, wizerunkowych lub prawnych.

13. Tworząc informacje (pliki, dokumenty, zbiory danych) lub będąc Właścicielem biznesowym zasobu informacyjnego, jesteś odpowiedzialny za sklasyfikowanie tej informacji.
14. Wszyscy pracownicy są odpowiedzialni za postępowanie z informacjami zgodnie z przyjętym schematem klasyfikacji informacji.
15. Szczegółowe wytyczne w zakresie klasyfikacji i postępowania z informacjami znajdziesz w Standardzie klasyfikacji informacji.

Zarządzanie ryzykiem

16. Nasze działania w zakresie bezpieczeństwa informacji realizujemy w oparciu o ustanowiony proces zarządzania ryzykiem. Wynikiem tego procesu jest wdrożenie zabezpieczeń, które redukują ryzyko do akceptowalnego dla nas poziomu.
17. Ocenę ryzyka możemy podjąć w każdej sytuacji, gdy zmieniają się procesy lub otoczenie biznesowe RFG na skutek uruchomienia nowych projektów, wdrożenia istotnych zmian w systemach, zmiany otoczenia biznesowego lub zmian regulacyjnych.
18. Proces zarządzania ryzykiem opisaliśmy szczegółowo w Standardzie zarządzania ryzykiem bezpieczeństwa informacji.

Podstawowe zasady ochrony

19. Planując i wdrażając ochronę informacji, stosujemy następujące zasady:
 - **zasada minimalizacji uprawnień** - otrzymasz tylko takie niezbędne uprawnienia, abyś mógł/mogła wykonywać swoje zadania i obowiązki; uprawnienia te będą ograniczać dostęp do systemów, usług oraz danych,

- **zasada wiedzy koniecznej** - przekazujemy informacje ograniczone wyłącznie do tych, które są konieczne do realizacji powierzonych zadań,
- **zasada ubezpieczania zabezpieczeń** - tam, gdzie to możliwe i efektywne, stosujemy i będziemy stosować zabezpieczenia wielowarstwowe, które wzajemnie się ubezpieczają,
- **zasada indywidualnej odpowiedzialności** - odpowiedzialność za bezpieczeństwo informacji przypisujemy każdej osobie dopuszczonej do przetwarzania.

Monitorowanie działań

20. Informujemy Was, że wszelkie działania wykonywane w systemach teleinformatycznych należących do RFG mogą być monitorowane. Zastrzegamy sobie prawo do ich wglądu i monitorowania z zachowaniem pełnej dbałości o ich poufność i integralność. Monitoring pozwoli nam tworzyć raporty, poprawiać bezpieczeństwo i unikać problemów technicznych. Dane z monitoringu mogą być dowodem w sprawie o naruszenie bezpieczeństwa informacji.

Zobowiązanie do zachowania poufności

21. Zobowiązujemy wszystkich pracowników i współpracowników RFG do zachowania poufności. Obowiązek zachowania poufności trwa również po ustaniu stosunku pracy lub innego stosunku prawnego, na podstawie którego była wykonywana praca na rzecz RFG.
22. Wprowadzamy zasadę potwierdzenia stosowania się do zachowania poufności przez podpisanie "Oświadczenia o zapoznaniu się z Polityką bezpieczeństwa informacji oraz zachowaniu poufności" - Załącznik nr 3 do naszej Polityki.
23. Zasada zachowania poufności obowiązuje też podmioty zewnętrzne, co jest każdorazowo regulowane w ramach zawieranych umów.

Reagowanie na incydenty

24. Wprowadzamy zasadę zgłaszania wszelkich zidentyfikowanych przez Was słabości lub zdarzeń, które mogą mieć wpływ na bezpieczeństwo informacji. W Intranecie dostępne są informacje pomocne w ocenie, czy dana sytuacja nosi znamiona incydentu i czy i do jakiego podmiotu powinna zostać zgłoszona.
25. Zapewniamy skuteczny model zarządzania incydentami, który opiera się na zasadach współpracy zespołowej. Zasady zarządzania incydentami zostały określone w Standardzie zarządzania incydentami.

Odstępstwa

26. Odstępstwa od stosowania zasad Polityki oraz dokumentów powiązanych muszą zostać zgłoszone i zaakceptowane przez ISO. Istotne odstępstwa akceptowane są przez Zarząd. Za ocenę istotności odstępstwa odpowiada ISO.

Egzekwowanie zasad bezpieczeństwa

27. Będziemy dążyć do egzekwowania zasad bezpieczeństwa określonych niniejszą Polityką. Zastrzegamy, że nieprzestrzeganie zasad wynikających z Polityki oraz dokumentów powiązanych może prowadzić do podjęcia właściwych sankcji dyscyplinarnych lub umownych na podstawie stosownych przepisów prawa.

Doskonalenie

28. Przyjmujemy zasadę okresowego analizowania skuteczności systemu zarządzania bezpieczeństwem informacji, w tym aktualności, adekwatności i skuteczności Polityki bezpieczeństwa oraz innych dokumentów związanych z bezpieczeństwem.

29. Efektem przeglądu może być zaplanowanie i wdrożenie działań, które poprawią skuteczność zarządzania bezpieczeństwem informacji.

30. Niezależnie od wyników przeglądu Politykę oraz dokumenty zależne możemy zmienić, zawsze, gdy:

- zidentyfikujemy nowe ryzyka,
- zmieniają się przepisy prawa lub regulacje wewnętrzne,
- nastąpią zmiany organizacyjne lub procesowe w RFG,
- będzie to wymagane w związku z wynikami przeglądów i/lub audytów bezpieczeństwa.

31. Wdrożyliśmy Standard nadzoru, który szczegółowo opisuje zasady monitorowania, przeglądów i doskonalenia naszego systemu zarządzania bezpieczeństwem informacji.

Załączniki

- Załącznik nr 1 – Zakres systemu zarządzania bezpieczeństwem informacji
- Załącznik nr 2 – Schemat dokumentacji składającej się na system zarządzania bezpieczeństwem informacji
- Załącznik nr 3 - Oświadczenie o zapoznaniu się z Polityką bezpieczeństwa informacji oraz zachowaniu poufności

Dokumenty powiązane

- Wszystkie standardy składające się na system zarządzania bezpieczeństwem informacji oraz wszelkie podręczniki i dokumenty operacyjne dotyczące bezpieczeństwa informacji.

Miejsca udostępnienia

lp.	lokalizacja
1.	Baza procedur na dysku sieciowym

Metryka dokumentu

wersja	data	opis zmiany	sporządził	zatwierdził
wer.1.0	26.05.2025 r.	Utworzenie dokumentu	Piotr Błaszczek - ISO	Piotr Grzybowski - Prezes Zarządu