SELENA GLOBAL EXPERIENCE	ORYGINAŁ/KOPIA	Nr Dokumentu: P/G/IT/001/01	Wersja 1.0
	Typ: POLITYKA		
Tytuł: POLITYKA BEZPIECZEŃSTWA INFORMACJI W GRUPIE SELENA			Strona Strona 1 z **31**

	Imię i Nazwisko	Stanowisko	Data i podpis
Opracował:	Szostek_Bar i Partnerzy Kancelaria Prawna	Radcy Prawni	23.08.2019
Zatwierdził:	Wojciech Knapik	CIO	
Zatwierdził:	Michał Westerlich	Legal and Audit Department Director	

Jacek Michalak
Członek Zarządu

POLITYKA BEZPIECZEŃSTWA INFORMACJI W GRUPIE SELENA

	Imię i Nazwisko	Stanowisko	Data i podpis
Opracował:	Szostek_Bar i Partnerzy Kancelaria Prawna	Radcy Prawni	
Zatwierdził:	Wojciech Knapik	CIO	
Zatwierdził:	Michał Westerlich	Legal and Audit Department Director	

Spis treści

	Imię i Nazwisko	Stanowisko	Data i podpis
Opracował:	Szostek_Bar i Partnerzy Kancelaria Prawna	Radcy Prawni	
Zatwierdził:	Wojciech Knapik	CIO	
Zatwierdził:	Michał Westerlich	Legal and Audit Department Director	

PREAMBUŁA

W celu zapewnienia zgodności z prawem, regulacjami wewnętrznymi i dobrymi praktykami, zachowania ciągłości i efektywności procesów, zminimalizowania ryzyka ujawnienia lub utraty Informacji oraz budowy wizerunku Spółek z Grupy Selena jako dbających o bezpieczeństwo zasobów informacyjnych, wprowadza się niniejszą Politykę Bezpieczeństwa Informacji (PBI).

I. WPROWADZENIE

1. Niniejsza PBI jest ogólnym i nadrzędnym dokumentem dotyczącym zarządzania systemem Bezpieczeństwa Informacji w Grupie Selena oraz zawiera odniesienia do innych dokumentów: polityk, procedur, instrukcji, których komplementarne stosowanie gwarantuje wysoki poziom Bezpieczeństwa Informacji w Grupie Selena.
2. Na System Bezpieczeństwa Informacji w Grupie Selena składa się zbiór zasad umożliwiających zarządzanie Bezpieczeństwem Informacji, obejmujący w szczególności: organizację Bezpieczeństwa Informacji, zarządzanie aktywami, kontrolę dostępu, utrzymanie i rozwój Systemów Przetwarzania, w tym systemów teleinformatycznych, bezpieczeństwo zasobów ludzkich, środki bezpieczeństwa fizyczne, organizacyjne i techniczne, zarządzanie incydentami, zarządzanie ciągłością działania, zapewnienie zgodności z prawem i regulacjami wewnętrznymi. System ten opisany jest w niniejszej PBI oraz dokumentach z nią powiązanych.
3. Grupa Selena odpowiada za zapewnienie poufności i kontrolowanie dostępu do wszelkich Informacji Chronionych oraz Informacji Wewnętrznych, dotyczących zarówno Grupy Selena jak i informacji dotyczących jej klientów, dostawców, partnerów biznesowych, którzy powierzając Grupie Selena lub Spółkom z Grupy określone Informacje, oczekują, że będą one przetwarzane w sposób rzetelny, zgodny z prawem i bezpieczny.
4. Kluczowe dla prawidłowego wdrożenia niniejszej PBI jest, aby każdy Współpracownik Grupy Selena lub Spółek z Grupy znał postanowienia PBI oraz aktów z nią powiązanych, był świadomy odpowiedzialności związanej z Bezpieczeństwem

Informacji, rozumiał charakter i sposób ochrony Informacji poszczególnych kategorii oraz wiedział, jak postępować w razie naruszeń Bezpieczeństwa Informacji.

5. Niniejsza PBI opisuje ogólne zasady Bezpieczeństwa Informacji obowiązujące w Grupie Selena, role i zadania osób uczestniczących w procesie Przetwarzania Informacji i zarządzania Bezpieczeństwem Informacji oraz podstawowe wymogi, jakie muszą spełniać Systemy Przetwarzania.

II. CELE PBI

1. Do celów niniejszej PBI należą:
   1) zapewnienie, że Informacje przetwarzane przez Grupę Selena są odpowiednio zabezpieczone przed możliwymi konsekwencjami naruszenia poufności, braku integralności lub przerw w dostępie do tych Informacji;
   2) zagwarantowanie właściwej ochrony Informacji bez względu na jakim nośniku jest zapisana;
   3) zapewnienie ciągłości procesów Przetwarzania Informacji;
   4) zapewnienie, że wszyscy Użytkownicy znają i stosują zasady Bezpieczeństwa Informacji, w tym wszystkie aktualne regulacje wewnętrzne w Grupie Selena i mające zastosowanie przepisy prawa polskiego i unijnego;
   5) zapewnienie bezpiecznego środowiska Systemów Przetwarzania dla wszystkich Użytkowników;
   6) zapewnienie ochrony Spółek z Grupy Selena przed odpowiedzialnością lub szkodami wynikającymi z niewłaściwego zabezpieczenia lub wykorzystania Informacji;
   7) zapewnienie, że Informacje są usuwane lub niszczone w odpowiedni sposób, gdy nie są już istotne, wymagane lub potrzebne;
   8) zapewnienie właściwego reagowania na naruszenia Bezpieczeństwa Informacji.
2. Realizacja przyjętych celów powinna być zrealizowana poprzez:

	Imię i Nazwisko	Stanowisko	Data i podpis
Opracował:	Szostek_Bar i Partnerzy Kancelaria Prawna	Radcy Prawni	
Zatwierdził:	Wojciech Knapik	CIO	
Zatwierdził:	Michał Westerlich	Legal and Audit Department Director	

autentyczności (prawdziwości), integralności (ochrona dokładności i kompletności informacji), dostępności (zapewnienie, że informacje są dostępne dla upoważnionych Użytkowników, gdy jest to wymagane) oraz rozliczalności (zapewnienie, że określone działanie dowolnego podmiotu będzie jednoznacznie przypisane temu podmiotowi);

3) **Grupa Selena** – spółka Selena FM S.A. z siedzibą we Wrocławiu Selena FM S.A. z siedzibą we Wrocławiu, ul. Strzegomska 2-4, wpisana do rejestru przedsiębiorców Krajowego Rejestru Sądowego pod numerem 0000292032 w Sądzie Rejonowym dla Wrocławia-Fabrycznej we Wrocławiu, VI Wydział Gospodarczy KRS, NIP 884-00-30-013 oraz jej spółki powiązane (tj. spółki zależne; spółki, w których Selena FM S.A. posiada udziały lub akcje; spółki współpracujące na podstawie umów typu joint venture i podobnych);

4) **Informacja** - dane, które zostały uporządkowane i usystematyzowane w określony sposób, niezależnie od faktu i sposobu ich utrwalenia na materialnych nośnikach analogowych lub cyfrowych, w szczególności wszelkiego rodzaju dokumenty i pliki elektroniczne zawierające dane osobowe, organizacyjne, techniczne, ekonomiczne, planistyczne, jakościowe, prognostyczne, w tym plany, schematy, rysunki i fotografie;

5) **Podmioty Nieupoważnione** - osoby, które nie są uprawnione do posługiwania się daną Informacją, w szczególności Współpracownicy, którym Informacja nie jest potrzebna do wykonywania obowiązków zgodnie z rodzajem czynności wykonywanych na zajmowanym stanowisku lub w ramach wykonywania zobowiązań wobec Spółek z Grupy Selena (w tym nieposiadający kodów dostępu, kluczy, kart dostępu) oraz osoby trzecie, którym Spółka nie ujawniła danej Informacji, a Informacja ta nie jest niezbędna do prowadzenia współpracy handlowej lub innej współpracy w ramach prowadzonej działalności gospodarczej (klienci, dostawcy, inne osoby trzecie);

6) **Przetwarzanie Informacji** – działania lub operacje wykonywane w odniesieniu do Informacji, takie jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez

1) wyznaczenie zadań i odpowiedzialności związanych z zapewnieniem Bezpieczeństwa Informacji;
2) wyznaczenie Właścicieli Informacji, którzy odpowiadają za odpowiednią kwalifikację Informacji oraz zapewnienie adekwatnego poziomu Bezpieczeństwa Informacji;
3) wdrożenie i utrzymanie niezbędnych zabezpieczeń fizycznych, organizacyjnych i technicznych;
4) zapoznanie się przez wszystkich Współpracowników z właściwymi politykami i procedurami z zakresu Bezpieczeństwa Informacji obowiązującymi w Grupie Selena;
5) ciągłe podnoszenie świadomości Współpracowników w obszarze Bezpieczeństwa Informacji
6) przeglądy i aktualizowanie polityk, procedur, regulaminów i instrukcji dotyczących Bezpieczeństwa Informacji w Grupie Selena;
7) reagowanie na zagrożenia i naruszenia Bezpieczeństwa Informacji w sposób zgodny z przyjętymi zasadami w sposób umożliwiający szybkie podjęcie działań naprawczych i zapobiegawczych na przyszłość.

III. DEFINICJE I TERMINOLOGIA

1. Terminy użyte w niniejszym dokumencie lub w którymkolwiek załączniku do niniejszej PBI oznaczają:
   1) **Administrator Systemu Przetwarzania** – osoba odpowiedzialna za nadzorowanie pracy powierzonych jej Systemów Przetwarzania w Grupie Selena, zarządzanie kontami i uprawnieniami Użytkowników, aktualizacje i konfigurowanie tych systemów oraz dbanie o bezpieczeństwo systemów; do każdego Systemu Przetwarzania w Grupie Selena przypisany jest Administrator Systemu – zgodnie z **Załącznikiem nr 3** do niniejszej PBI– *Administratorzy Systemów Przetwarzania*;
   2) **Bezpieczeństwo Informacji** - zapewnienie poufności informacji (ochrona informacji przed nieuprawnionym dostępem i ujawnieniem),

	Imię i Nazwisko	Stanowisko	Data i podpis
Opracował:	Szostek_Bar i Partnerzy Kancelaria Prawna	Radcy Prawni	
Zatwierdził:	Wojciech Knapik	CIO	
Zatwierdził:	Michał Westerlich	Legal and Audit Department Director	

Spółek z Grupy Selena, osoby zajmujące stanowiska kierownicze w tych Spółkach, a także stażyści i praktykanci odbywający staż lub praktykę na podstawie umowy ze Spółką z Grupy Selena.

2. W ramach **Załącznika nr 1** do niniejszej PBI dla oznaczenia Właścicieli grup i podgrup Informacji oraz Użytkowników z dostępem stosuje się ujednolicone nazwy stanowisk dla całej Grupy Selena.

3. Jeżeli w danej Spółce z Grupy Selena stanowisko wskazane w kategoriach podmiotów, o których mowa w ust. 2 powyżej, nie istnieje, wtedy odpowiadająca mu część **Załącznika nr 1** nie znajdzie zastosowania do danej Spółki z Grupy Selena. Jednakże jeżeli w danej Spółce z Grupy Selena istnieje odmiennie nazwane stanowisko, które odpowiada zakresem uprawnień i obowiązków stanowisku wskazanemu w **Załączniku nr 1,** odpowiadająca mu część **Załącznika nr 1** znajdzie zastosowanie do danej Spółki z Grupy Selena.

4. Nazwy działów pisane dużą literą oznaczają jednostki organizacyjne w Selena FM S.A. Stanowiska pisane dużą literą oznaczają stanowiska w Selena FM S.A.

IV. PRZEDMIOTOWY ZAKRES OBOWIĄZYWANIA PBI

1. Niniejsza PBI odnosi się do każdego rodzaju Informacji, niezależnie od jej treści, wartości oraz sposobu utrwalenia i przesyłu.
2. Informacje przetwarzane w Grupie Selena należą do jednej z trzech grup (klasyfikacja Informacji):
   1) **Informacje Chronione;**
   2) **Informacje Wewnętrzne;**
   3) **Informacje Publiczne.**
3. Kategoria „Informacje Chronione" obejmuje podkategorie:
   1) „Informacje Poufne", których zasady klasyfikacji, obiegu i bezpieczeństwa określa *Polityka Obiegu Informacji Poufnych w Grupie Selena;*

przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie;

7) **Spółka** – Selena FM S.A. oraz każda spółka należąca do Grupy Selena, w której wprowadzono niniejszą PBI;

8) **System Przetwarzania** – dowolny system, w tym system teleinformatyczny, w którym Informacja jest przetwarzana (zbierana, utrwalana, organizowana, porządkowana, przechowywana, modyfikowana, pobierana, przeglądana, udostępniana, przesyłana, łączona, ograniczana, usuwana lub niszczona) w sposób zautomatyzowany lub niezautomatyzowany, dowolnej postaci analogowej lub elektronicznej; szczegółowa lista Systemów Przetwarzania znajduje się w zakładce „Systemy Przetwarzania" w **Załączniku nr 1** do niniejszej PBI - *Zasoby informacyjne w Grupie Selena*.

9) **Twórca Informacji** – Użytkownik, który stworzył Informację, samodzielnie lub wraz z innymi osobami, w oparciu o posiadaną wiedzę, umiejętności i zasób innych Informacji;

10) **Właściciel Informacji** – Użytkownik, który jest odpowiedzialny za Informację (także grupy lub podgrupy Informacji) w swoim obszarze działania, zarządzający delegacją odpowiedzialności w przetwarzaniu Informacji; decyduje o sposobie postępowania z Informacjami (oznaczanie Informacji, dostęp, udostępnianie, usuwanie lub niszczenie);

11) **Właściciel PBI** – Członek Zarządu Selena FM S.A. wskazany w uchwale Zarządu Selena FM S.A., odpowiedzialny za zaimplementowanie niniejszej PBI, dokonywanie modyfikacji PBI wynikających ze zmian w Systemach Przetwarzania, procesach biznesowych lub ze zmian w organizacji Grupy Selena oraz monitorowanie przestrzegania PBI w Grupie Selena;

12) **Współpracownik** lub **Użytkownik** - każdy pracownik lub współpracownik Spółek z Grupy Selena, zatrudniony w ramach stosunku pracy lub na podstawie innej umowy, w tym cywilnoprawnej, bez względu na rodzaj pracy, wymiar czasu pracy oraz zajmowane stanowisko, przedsiębiorcy świadczący usługi na rzecz Spółek z Grupy Selena na podstawie umowy o współpracy lub innego kontraktu, Członkowie Zarządu

	Imię i Nazwisko	Stanowisko	Data i podpis
Opracował:	Szostek_Bar i Partnerzy Kancelaria Prawna	Radcy Prawni	
Zatwierdził:	Wojciech Knapik	CIO	
Zatwierdził:	Michał Westerlich	Legal and Audit Department Director	

2) „dane osobowe", których zasady przetwarzania i bezpieczeństwa określa *Polityka bezpieczeństwa danych osobowych w Selena FM Spółka Akcyjna*.

4. Klasyfikacji Informacji w Spółce dokonuje się zgodnie z poniższą tabelą, z uwzględnieniem szczegółowych regulacji, wskazanych w ust. 3 powyżej.

Klasyfikacja Informacji	**Dostęp do Informacji**	**Skutki naruszenia Bezpieczeństwa Informacji**	**Rodzaje Informacji należących do danej klasy**
Informacje Chronione	Dostępne tylko dla niektórych Współpracowników w zakresie, w jakim są one potrzebne do realizacji zadań poszczególnych Współpracowników. Mogą być częściowo dostępne także dla podmiotów zewnętrznych, które współpracują z Grupą Selena (dostawcy, partnerzy biznesowi) na warunkach uregulowanych w umowach zawartych z tymi podmiotami. Mogą być dostępne także dla organów publicznych, na podstawie	Naruszenie bezpieczeństwa tych Informacji wpłynie na działalność biznesową lub reputację Grupy Selena lub Spółek z Grupy, będzie stanowić naruszenie zobowiązań umownych lub przepisów prawa i spowoduje szkodę w majątku Grupy Selena lub Spółek z Grupy.	– dane osobowe; – dane objęte tajemnicą zawodową; – dane stanowiące tajemnicę przedsiębiorstwa; – dane chronione na podstawie umów cywilnoprawnych (umowy o zachowaniu poufności); – dane stanowiące własność intelektualną lub przemysłową; – inne Informacje, chronione na mocy przepisów prawa; – Informacje związane z procesem produkcyjnym oraz badawczo - rozwojowym (R&D), m.in. receptury, wynalazki (również przed uzyskaniem ochrony patentowej); – Informacje związane z funkcjonowaniem Grupy Selena, tj.: dotyczące planowanych transakcji, zmian w strukturze Grupy i poszczególnych Spółek, zmian struktury właścicielskiej, formy prowadzonej działalności (np.

	obowiązujących przepisów prawa.		przekształcenia, połączenia, podział Spółek); planowanej emisji lub sprzedaży akcji lub udziałów; – dane dostępowe do Systemów Przetwarzania, tj.: hasła do logowania, kody dostępu, hasła do elektronicznej obsługi kont bankowych.
Informacje Wewnętrzne	Dostępne tylko dla Współpracowników Grupy Selena zgodnie z zasadą przywilejów koniecznych. Mogą być częściowo dostępne także dla podmiotów zewnętrznych, które współpracują z Grupą Selena (dostawcy, partnerzy biznesowi) na warunkach uregulowanych w umowach zawartych z tymi podmiotami. Mogą być dostępne także dla organów publicznych, na podstawie obowiązujących przepisów prawa.	Naruszenie bezpieczeństwa tych Informacji może wpłynąć na działalność biznesową lub reputację Grupy Selena, może stanowić naruszenie zobowiązań umownych lub spowodować szkodę w majątku Grupy Selena lub Spółek z Grupy.	– polityki, procedury wewnętrzne, regulaminy i instrukcje; – plany biznesowe, marketingowe, Informacje finansowe, m. in. raporty, zestawienia, prognozy, udziały Grupy Selena w rynku, opisy produktów; – dane związane z dystrybucją produktów, w tym warunki współpracy, m.in. treść umów handlowych, zamówień, ofert handlowych, prowadzonych procesów negocjacyjnych, stosowanych cen, marż na poszczególnych produktach; – dane dotyczące stosowanych rozwiązań w Systemach Przetwarzania; – Informacje o urządzeniach i infrastrukturze technicznej Grupy Selena; – Informacje o stosowanym w Grupie Selena oprogramowaniu do obsługi procesów biznesowych;

	Imię i Nazwisko	Stanowisko	Data i podpis
Opracował:	Szostek_Bar i Partnerzy Kancelaria Prawna	Radcy Prawni	
Zatwierdził:	Wojciech Knapik	CIO	
Zatwierdził:	Michał Westerlich	Legal and Audit Department Director	

Informacje Publiczne	Dostępne bez ograniczeń.	Ta kategoria obejmuje Informacje przeznaczone do użytku publicznego; mogą być podawane do wiadomości publicznej bez żadnych negatywnych skutków dla działalności biznesowej lub reputacji Grupy Selena.	– Informacje ujawnione przez Zarządy Spółek w Grupie Selena; – Informacje dostępne na stronach internetowych Grupy Selena; – broszury marketingowe; – opublikowane raporty; – udostępniane publicznie wyniki finansowe; – Informacje prasowe na temat Grupy Selena; – Informacje na temat klientów, dostawców i innych podmiotów współpracujących z Grupą Selena znajdujące się w ogólnie dostępnych źródłach (prasa, publiczne bazy danych, Internet).

5. Klasyfikacji Informacji jako Chronionej, Wewnętrznej lub Publicznej dokonuje Twórca Informacji z chwilą jej stworzenia. Właściciel Informacji ma prawo zmiany tej kwalifikacji. W wypadku, gdy Twórcą Informacji jest więcej niż jedna osoba, klasyfikacji dokonuje Właściciel Informacji.
6. W odniesieniu do zasobów informacyjnych istniejących w Grupie Selena w dniu wejścia w życie niniejszej PBI, klasyfikacji Informacji lub grup i podgrup Informacji, zgodnie z ust. 2 powyżej, dokonuje Właściciel Informacji.
7. Wszystkie Informacje w Grupie Selena zostały ujęte w grupy, a w ramach poszczególnych grup w podgrupy do poziomu n-2. Grupy i podgrupy informacji, Właściciele Informacji (ich grup i podgrup), środki bezpieczeństwa, Systemy Przetwarzania oraz terminy retencji dla poszczególnych grup lub podgrup Informacji określone zostały w **Załączniku nr 1** do niniejszej PBI.
8. Wszystkie grupy i podgrupy Informacji mają przypisanych Właścicieli Informacji, którzy są odpowiedzialni za odpowiednią klasyfikację Informacji oraz utrzymanie

zabezpieczeń tych Informacji. Wdrożenie określonych zabezpieczeń jest delegowane przez Właściciela Informacji, jednak pozostaje on odpowiedzialny za właściwą ochronę przypisanych mu grup lub podgrup Informacji.

9. Sposób postepowania z Informacjami sklasyfikowanymi według powyższych kategorii przedstawia **Załącznik nr 2** do niniejszej PBI: *Poziomy ochrony i sposób postępowania z Informacjami.*

V. PODMIOTOWY ZAKRES OBOWIĄZYWANIA PBI

1. Niniejsza PBI obowiązuje w całej Grupie Selena. Obowiązek stosowania się do jej postanowień obejmuje wszystkich Współpracowników. Niniejsza PBI dotyczy wszelkich działań Współpracowników mających związek zarówno z działalnością którejkolwiek Spółek z Grupy Selena, jak i całej Grupy Selena.
2. Niniejsza PBI reguluje uniwersalny standard postępowania dla wszystkich Współpracowników Grupy Selena we wszystkich jej lokalizacjach. W przypadku, gdy indywidualnie uzgodnienia w umowie ze Współpracownikiem regulują daną materię bardziej szczegółowo lub restrykcyjnie, mają one pierwszeństwo zastosowania przed postanowieniem PBI pozostającymi z nimi w sprzeczności.
3. W odniesieniu do członków organów Spółek pierwszeństwo zastosowania mają dokumenty regulujące tzw. ład korporacyjny, tj. statut lub umowa Spółki, regulaminy organów Spółki oraz umowy zawierane z członkami organów danej Spółki, o ile regulują one kwestie objęte niniejszą PBI.
4. Obowiązki w zakresie odpowiedzialności za Bezpieczeństwo Informacji w Grupie Selena podzielone są w następujący sposób:
   1) **Zarząd** określa cele i strategie w zakresie Bezpieczeństwa Informacji oraz zapewnia odpowiednie zasoby do realizacji działań w tej dziedzinie.
   2) **Właściciel PBI:**
      a) jest odpowiedzialny za opracowanie i aktualizację PBI,
      b) nadzoruje przestrzegania zasad określonych w PBI;

implementowaniem nowych rozwiązań informatycznych mających na celu zwiększenie Bezpieczeństwa Informacji.

5) Administratorzy Systemów Przetwarzania:

a) zarządzają przypisanymi im Systemami Przetwarzania w sposób zapewniający ochronę Informacji w nich przetwarzanych;

b) kontrolują przepływ Informacji pomiędzy Systemami Przetwarzania w Grupie Selena a Systemami Zewnętrznymi;

c) zarządzają stosowanymi w Systemach Przetwarzania środkami nadawania i odbierania uprawnień oraz uwierzytelniania Użytkowników tych systemów, zgodnie z obowiązującymi w tym zakresie procedurami wewnętrznymi.

6) Dyrektorzy obszarów/kierownicy jednostek organizacyjnych:

a) nadzorują i zapewniają przestrzeganie przepisów prawa i regulacji wewnętrznych w Grupie Selena dotyczących Bezpieczeństwa Informacji w odniesieniu do zarządzanych przez siebie aktywów Grupy Selena;

b) zapewniają przestrzeganie przez podlegających im Współpracowników przestrzegania przepisów prawa i zasad Bezpieczeństwa Informacji obowiązujących w Grupie Selena, w szczególności odpowiadają za ich należyte przeszkolenie przed przystąpieniem do realizacji zadań wynikających z umowy z danym Współpracownikiem.

7) wszyscy Współpracownicy:

a) przestrzegają przepisów prawa i regulacji wewnętrznych w Grupie Selena dotyczących Bezpieczeństwa Informacji w odniesieniu do przetwarzanych przez siebie Informacji;

b) chronią Informacje podlegające ochronie przed dostępem do nich Podmiotów Nieuprawnionych, a także przed

c) nadzoruje zastosowanie środków Bezpieczeństwa Informacji;

d) planuje, nadzoruje i koordynuje kontrole w zakresie Bezpieczeństwa Informacji;

e) zapewnia rejestrowanie naruszeń Bezpieczeństwa Informacji;

f) opracowuje roczne raporty dotyczące zgłoszonych naruszeń Bezpieczeństwa Informacji i na ich podstawie rekomenduje działania zmierzające do poprawy Bezpieczeństwa Informacji;

g) organizuje szkolenia dla Współpracowników z zakresu Bezpieczeństwa Informacji.

3) Właściciel Informacji:

a) jest odpowiedzialny za prawidłową klasyfikację Informacji;

b) decyduje o zastosowaniu określonych zabezpieczeń Informacji oraz odpowiada za ich utrzymanie przez cały cykl życia Informacji;

c) decyduje o sposobach postępowania z Informacją (prawo odczytu, modyfikacji lub usuwania);

d) zarządza delegowaniem odpowiedzialności w Systemach Przetwarzania;

e) wspiera Właściciela PBI w zakresie organizacji i przeprowadzania kontroli Bezpieczeństwa Informacji.

4) Osoba odpowiedzialna za obszar zarządzania systemami teleinformatycznymi:

a) planuje, koordynuje i nadzoruje działania mające na celu zapewnienie bezpieczeństwa systemów informatycznych oraz Informacji przetwarzanych w tych systemach;

b) zarządza procesami związanymi z utrzymaniem i rozwojem systemów informatycznych w Grupie Selena oraz z

przypadkowym lub umyślnym zniszczeniem, utratą lub modyfikacją;

c) zgłaszają niezwłocznie wszelkie podejrzenia naruszenia przepisów prawa i regulacji wewnętrznych, w szczególności PBI, niezależnie od tego, czy dane naruszenie może być związane bezpośrednio z obszarem zadań danego Współpracownika.

VI. POLITYKI, PROCEDURY, REGULAMINY I INSTRUKCJE POWIĄZANE

1. Niniejszą PBI uzupełniają szczegółowe regulacje wewnętrzne obowiązujące w Grupie Selena dotyczące poszczególnych Informacji, zarządzania nimi i sposobów ich ochrony. Do tych regulacji należą w szczególności:

   1) *Polityka obiegu informacji poufnych w Grupie Selena* – w zakresie spełnienia wymogów prawa związanych z obrotem instrumentami finansowymi;

   2) *Polityka bezpieczeństwa danych osobowych* - w zakresie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych;

   3) *Polityka zgłaszania incydentów w zakresie ochrony danych osobowych w Selena FM S.A.* – w zakresie zgłaszania i dokumentowania naruszeń danych osobowych;

   4) *Procedura zgłaszania naruszeń i postępowania w sprawach związanych ze stosowaniem polityk bezpieczeństwa w Grupie Selena* – w zakresie obowiązków dotyczących zgłaszania naruszeń zasad bezpieczeństwa;

   5) *Polityka Grupy Selena dotycząca zakazu konkurencji oraz konfliktu interesów* – w zakresie zasad postępowania Współpracowników pozwalających na uniknięcie konfliktu interesów oraz ryzyka naruszenia interesów Spółek z Grupy Selena;

   6) *Polityka Grupy Selena dotycząca przeciwdziałaniu korupcji* – w zakresie zasad i sposobów eliminowania działań noszących znamiona korupcji oraz zapewnienia postępowania zgodnego z najwyższymi standardami etycznymi;

7) *Regulamin IT w Grupie Selena* – w zakresie zasad i warunków korzystania z systemów teleinformatycznych oraz usług IT w Grupie Selena oraz nadawania uprawnień do Systemów Przetwarzania w Grupie Selena;

8) *Procedura Zarządzania Zmianą w Systemie AX – w zakresie* procesu przeprowadzenia zmiany w Systemie AX;

9) *Instrukcja Wykonywania Testów Akceptacyjnych Modyfikacji* – w zakresie procesu przeprowadzania testów akceptacyjnych modyfikacji w Systemie AX.

2. Regulacje, o których mowa w ust. 2 powyżej stanowią przepisy szczególne wobec PBI, a zatem maja pierwszeństwo w zastosowaniu, jeśli regulują daną kwestię bardziej szczegółowo niż niniejsza PBI.

VII. ZASADY BEZPIECZEŃSTWA INFORMACJI

1. Grupa Selena przetwarza Informacje zgodnie z następującymi zasadami:

1) **zasadą uprawnionego dostępu**, zgodnie z którą każdy Współpracownik spełnia kryteria dopuszczenia do Informacji, odbył właściwe szkolenie lub instruktaż i podpisał stosowne oświadczenia o zachowaniu poufności;

2) **zasadą przywilejów koniecznych**, zgodnie z którą każdy Współpracownik posiada prawa dostępu do Informacji, ograniczone wyłącznie do tych, które są konieczne do wykonywania powierzonych mu zadań;

3) **zasadą wiedzy koniecznej**, zgodnie z którą każdy Współpracownik posiada wiedzę o systemie, do którego ma dostęp, ograniczoną wyłącznie do zagadnień, które są konieczne do realizacji powierzonych mu zadań;

4) **zasadą usług koniecznych**, zgodnie z którą zakres dostępnych dla Użytkownika usług w ramach systemów teleinformatycznych jest ograniczony tylko do tych, które są konieczne do prawidłowej realizacji zadań na zajmowanym stanowisku;

5) **zasadą indywidualnej odpowiedzialności**, zgodnie z którą każda z Informacji ma ustanowionego Właściciela Informacji, który za odpowiada za daną Informację, grupy lub podgrupy Informacji oraz, że każdy z

	Imię i Nazwisko	Stanowisko	Data i podpis
Opracował:	Szostek_Bar i Partnerzy Kancelaria Prawna	Radcy Prawni	
Zatwierdził:	Wojciech Knapik	CIO	
Zatwierdził:	Michał Westerlich	Legal and Audit Department Director	

VIII. OBOWIĄZKI W ZAKRESIE OCHRONY INFORMACJI

1. Obowiązki określone w niniejszej PBI są nieograniczone w czasie.
2. Informację należy traktować jako Chronioną lub Wewnętrzną dopóki nie stała się Informacją Publiczną z przyczyn innych niż jej bezprawnej ujawnienie.
3. Obowiązki w zakresie zachowania poufności nie dotyczą Informacji Chronionych lub Wewnętrznych, jeśli ich ujawnienia wymaga właściwy organ władzy publicznej działający na podstawie i w granicach przepisów prawa.
4. W razie wątpliwości co do charakteru danej Informacji przyjmuje się, że jest ona Informacji Chronioną.
5. Współpracownik uprawniony jest do korzystania z Informacji Chronionych i Wewnętrznych wyłącznie w zakresie, w jakim jest to niezbędne do prawidłowego wykonywania przez niego obowiązków umownych na rzecz Grupy Selena lub którejkolwiek ze Spółek z Grupy.
6. Każdy Współpracownik zobowiązany jest do ochrony Informacji Chronionych oraz Informacji Wewnętrznych przed ich bezprawnym ujawnieniem lub innym naruszeniem Bezpieczeństwa Informacji, w szczególności powinien:
    1) używać Informacji wyłącznie w celach, do jakich są przeznaczone;
    2) nie przekazywać ani nie ujawniać jakichkolwiek Informacji Chronionych lub Wewnętrznych osobom, w celach i zakresie innym niż przewidziane dla tej Informacji przez Właściciela Informacji;
    3) podjąć wszelkie niezbędne czynności uniemożliwiające dostęp do Informacji Chronionych lub Informacji Wewnętrznych Podmiotom Nieupoważnionym.
7. Współpracownik zobowiązany jest ponadto:
    1) w żaden sposób, bezpośrednio lub pośrednio nie wykorzystywać Informacji Chronionych lub Informacji Wewnętrznych dla celów prywatnych lub w interesie Podmiotów Nieupoważnionych lub innej osoby trzeciej;
    2) w żaden sposób nie kopiować, nie zwielokrotniać lub nie zatrzymywać otrzymanych w związku z realizacją powierzonych mu obowiązków dokumentów lub nośników danych zawierających Informacje Chronione bez

Użytkowników odpowiada indywidualnie za naruszenie obowiązujących przepisów prawa i regulacji wewnętrznych w Grupie Selena;

6) **zasadą obecności koniecznej**, zgodnie z którą prawo przebywania w określonych miejscach, w których przetwarzane są Informacje, mają tylko osoby upoważnione;

7) **zasadą stałej gotowości**, zgodnie z którą systemy teleinformatyczne Grupy Selena są przygotowane na zagrożenia; niedopuszczalne jest tymczasowe wyłączanie mechanizmów zabezpieczających;

8) **zasadą adekwatności**, zgodnie z którą używane zabezpieczenia - środki techniczne i organizacyjne – są optymalizowane na podstawie analizy i szacowania ryzyka, z wykorzystaniem kryteriów skuteczności, efektywności oraz spełnienia obowiązków wynikających z przepisów prawa, regulacji wewnętrznych i przyjętych zobowiązań umownych;

9) **zasadą autoryzacji**, zgodnie z którą każdy System Przetwarzania, urządzenie, program komputerowy lub inny składnik aktywów Grupy Selena jest autoryzowany przed jego wykorzystaniem w procesie Przetwarzania Informacji;

10) **zasadą uwierzytelniania**, zgodnie z którą przed każdym rozpoczęciem pracy w systemie teleinformatycznym, Użytkownik powinien zalogować się z wykorzystaniem indywidualnego identyfikatora i hasła spełniającego kryteria określone w odrębnych przepisach wewnętrznych;

11) **zasadą czystego ekranu i czystego biurka,** zgodnie z którą każdy Współpracownik zobowiązany jest do uniemożliwienia odczytu danych z ekranu swojego komputera lub z dokumentów Podmiotowi Nieupoważnionemu, w szczególności poprzez stosowanie odpowiednich środków Bezpieczeństwa Informacji.

2. Dokumentacja wewnętrzna dotycząca systemu Bezpieczeństwa Informacji w Grupie Selena musi być zgodna z powyższymi zasadami.

uprzedniej zgody Spółki, której Informacje dotyczą, wyrażonej w formie pisemnej lub elektronicznej;

3) nie poruszać kwestii objętych zakresem Informacji Chronionych lub Informacji Wewnętrznych w prywatnych rozmowach lub prywatnej korespondencji, a także w korespondencji z Podmiotami Nieupoważnionymi.

8. Obowiązek ochrony Informacji w Grupie Selena wiąże Współpracownika niezależnie od tego, czy dane Informacje zostały formalnie oznaczone jako Chronione lub Wewnętrzne.

9. Współpracownik zobowiązuje się niezwłocznie zwrócić lub zniszczyć, na żądanie Spółki i zgodnie z wyborem Spółki, wszelkie dokumenty oraz nośniki danych zawierające Informacje Chronione lub Informacje Wewnętrzne uzyskane przez niego lub jemu udostępnione w związku z realizacją umowy wiążącej go z Grupą Selena lub Spółką z Grupy Selena.

10. W wypadku konieczności przesłania lub przewiezienia nośników zawierających Informacje Chronione, Współpracownik zobowiązany jest do bezpiecznego ich opakowania lub zapieczętowania uniemożliwiającego dostęp do ich treści przez Podmioty Nieupoważnione..

11. Do każdego zasobu informacyjnego przypisany jest okres retencji – zgodnie z **Załącznikiem nr 1** do niniejszej PBI. Po upływie terminu retencji wszelkie nośniki zawierające Informacje Chronione i Informacje Wewnętrzne są bezpiecznie i trwale usuwane lub niszczone.

12. Decyzja o trwałym usunięciu lub zniszczeniu Informacji Chronionych lub Informacji Wewnętrznych podejmowana jest przez Właściciela Informacji. Zniszczenie lub usunięcie następuje w sposób uniemożliwiający odtworzenie Informacji.

13. Współpracownicy korzystający z infrastruktury teleinformatycznej Grupy Selena dbają o bezpieczeństwo systemów, urządzeń i oprogramowania zgodnie z *Regulaminem IT w Grupie Selena*.

	Imię i Nazwisko	Stanowisko	Data i podpis
Opracował:	Szostek_Bar i Partnerzy Kancelaria Prawna	Radcy Prawni	
Zatwierdził:	Wojciech Knapik	CIO	
Zatwierdził:	Michał Westerlich	Legal and Audit Department Director	

IX. ODPOWIEDZIALNOŚĆ ZA BEZPIECZEŃSTWO INFORMACJI

1. Nieprzestrzeganie zasad zawartych w niniejszej PBI oraz powiązanych z nią regulacjach wewnętrznych obowiązujących w Grupie Selena, może stanowić naruszenie obowiązków pracowniczych wynikających w szczególności z ustawy – Kodeks pracy i może pociągnąć za sobą skutki dyscyplinarne oraz spowodować pociągnięcie sprawcy do odpowiedzialności wynikającej z przepisów prawa pracy.
2. W wypadku Współpracowników współpracujących ze Grupą Selena na innej podstawie niż umowa o pracę, nieprzestrzeganie zasad zawartych w niniejszej PBI oraz powiązanych z nią regulacjach wewnętrznych, obowiązujących w Grupie Selena, może stanowić naruszenie zobowiązań umownych i rodzić odpowiedzialność z tytułu nienależytego wykonania zobowiązania lub czynów niedozwolonych.
3. Niezależnie od powyższego, w zależności od okoliczności danej sprawy, Współpracownik, który narusza niniejszą PBI, może ponosić odpowiedzialność odszkodowawczą wobec Spółek z Grupy Selena. W przypadku zaś, gdy naruszenie niniejszej PBI jest jednocześnie czynem zabronionym – także odpowiedzialność karną.

X. ŚRODKI OCHRONY INFORMACJI

1. Grupa Selena zapewnia odpowiednie zabezpieczenia mające na celu ochronę Informacji Chronionych i Informacji Wewnętrznych.
2. Stosowane środki ochrony są dobierane na podstawie:
    1) przepisów obowiązujących aktów prawnych;
    2) wyników przeprowadzonej analizy ryzyka w Bezpieczeństwie Informacji;
    3) dobrych praktyk uznanych w obrocie profesjonalnym.
3. Wyróżnia się standardowe oraz niestandardowe środki ochrony.
4. Na standardowe środki ochrony składają się:

8) stosowanie zasad polityki czystego biurka i czystego ekranu.

2. Szczegółowe zasady stosowania środków bezpieczeństwa fizycznego w Grupie Selena lub w poszczególnych Spółkach mogą być opisane w regulaminach lub procedurach szczegółowych i mogą się różnić w poszczególnych Spółkach w Grupie Selena.

XII. ZARZĄDZANIE ORGANIZACYJNYMI ŚRODKAMI BEZPIECZEŃSTWA

1. Każdy Współpracownik przed przystąpieniem do wykonywania zadań wynikających z umowy wiążącej go z Grupą Selena lub Spółką z Grupy zapoznaje się z obowiązującymi regulacjami wewnętrznymi, a w szczególności dokumentami wymienionymi w części VI. niniejszej PBI.
2. Każdy Współpracownik przed przystąpieniem do wykonywania zadań wynikających z umowy wiążącej go z Grupą Selena lub Spółką z Grupy składa oświadczenie o zapoznaniu się i przestrzeganiu polityk, procedur i instrukcji, o których mowa w części VI. niniejszej PBI.
3. Każdemu Współpracownikowi nadawane są przez Administratorów Systemów Przetwarzania indywidualne uprawnienia dostępowe do Informacji przetwarzanych w systemach teleinformatycznych.
4. Każdy Współpracownik, przed rozpoczęciem wykonywania zadań wynikających z umowy wiążącej go z Grupą Selena lub Spółką z Grupy zostaje pouczony o zasadach Bezpieczeństwa Informacji obowiązujących w Grupie Selena oraz przechodzi instruktaż stanowiskowy obejmujący szczegółowe zasady Bezpieczeństwa Informacji, w tym bezpieczeństwa systemów teleinformatycznych, obowiązujące na danym stanowisku.
5. Z każdym Współpracownikiem, a także z podmiotem zewnętrznym, któremu zamierza się udostępnić Informację Chronioną lub Informację Wewnętrzną, zawierana jest umowa o zachowaniu poufności.
6. Proces nadawania nowych uprawnień, modyfikacji lub odbierania uprawnień dostępowych realizowany jest na podstawie procedury nadawania uprawnień stanowiącej integralną część *Regulaminu IT w Grupie Selena.*

1) zabezpieczenia fizyczne takie jak: nadzór nad dostępem do budynków i pomieszczeń, kontrola dostępu fizycznego (karty dostępu), ochrona osób i mienia;
2) zabezpieczenia organizacyjne: procedura nadawania uprawnień do Systemów Przetwarzania, szkolenia, informowanie o wszelkich zmianach w zakresie systemu Bezpieczeństwa Informacji;
3) zabezpieczenia techniczne: zabezpieczenie sprzętu infrastruktury informatycznej i telekomunikacyjnej oraz stosowanie oprogramowania zapewniającego bezpieczeństwo korzystania z Informacji i ich przesyłu, zgodnie z *Regulaminem IT w Grupie Selena.*

5. Zabezpieczenia fizyczne, organizacyjne i techniczne uzupełniają się wzajemnie, zapewniając łącznie wymagany poziom Bezpieczeństwa Informacji.
6. Zastosowanie niestandardowych środków ochrony odbywa się w odniesieniu do poszczególnych podgrup Informacji zgodnie ze wskazaniami zawartymi w **Załączniku nr 1** do niniejszej PBI.

XI. ZARZĄDZANIE BEZPIECZEŃSTWEM FIZYCZNYM

1. Zarządzanie bezpieczeństwem fizycznym w Grupie Selena i kontrolą dostępu realizowane jest poprzez:
   1) nadzór nad dostępem do budynków i pomieszczeń;
   2) zatrudnianie personelu bezpieczeństwa;
   3) stosowanie systemów sygnalizacji włamania i napadu;
   4) stosowanie szaf zamykanych na klucz w odniesieniu do Informacji Chronionych;
   5) stosowanie systemów kontroli dostępu (karty dostępu);
   6) kontrolę dostępu do obszarów przechowywania Informacji Chronionych i Informacji Wewnętrznych;
   7) kontrolę dostępu do sprzętu, sieci i systemów informatycznych;

XIII. ZARZĄDZANIE TECHNICZNYMI ŚRODKAMI BEZPIECZEŃSTWA = SYSTEMAMI TELEINFORMATYCZNYMI I SIECIAMI

1. Wdrożenia, eksploatacja oraz utrzymanie systemów informatycznych są realizowane przez kompetentnych i świadomych zagadnień Bezpieczeństwa Informacji specjalistów.
2. Usługi dostarczane przez osoby trzecie są weryfikowane pod kątem spełniania wymogów w zakresie Bezpieczeństwa Informacji.
3. Systemy informatyczne są monitorowane w celu wykrycia naruszeń Bezpieczeństwa Informacji oraz zapobieganiu im.
4. Szczegółowe zasady zarządzania systemami i sieciami teleinformatycznymi opisane zostały w *Regulaminie IT Grupy Selena* lub w innych dokumentach wewnętrznych.

XIV. KONTROLE BEZPIECZEŃSTWA INFORMACJI

1. Grupa Selena przeprowadza wewnętrzne kontrole w zakresie Bezpieczeństwa Informacji w zaplanowanych odstępach czasu, aby określić, czy cele stosowania zabezpieczeń, środki ochrony, procesy i procedury wewnętrzne są:
    1) zgodne z przepisami prawa i aktualnym stanem wiedzy technicznej;
    2) zgodne ze zidentyfikowanymi o wymaganiami Bezpieczeństwa Informacji;
    3) skutecznie wdrożone i stosowane.
2. Za przygotowanie i organizację czynności kontrolnych odpowiedzialny jest Właściciel PBI.

XV. ZARZĄDZANIE ZMIANĄ W ZASOBACH INFORMACYJNYCH

1. Zmiany w zasobach informacyjnych są wprowadzane zgodnie z formalnym procesem kontroli zmian. Proces ten gwarantuje, że proponowane zmiany zostaną przetestowane, autoryzowane i wdrożone w kontrolowany sposób przez uprawnione do tego osoby oraz że status każdej proponowanej zmiany jest monitorowany.

	Imię i Nazwisko	Stanowisko	Data i podpis
Opracował:	Szostek_Bar i Partnerzy Kancelaria Prawna	Radcy Prawni	
Zatwierdził:	Wojciech Knapik	CIO	
Zatwierdził:	Michał Westerlich	Legal and Audit Department Director	

2. Proces kontroli zmian dotyczy wszystkich istotnych Systemów Przetwarzania Informacji w Grupie Selena (systemy teleinformatyczne, dokumentacja systemów, procesy biznesowe i procedury operacyjne).
3. Wszystkie żądania zmian powinny być rejestrowane, niezależnie od tego, czy zostały zatwierdzone, czy odrzucone - w centralnym systemie zarządzania zmianą. Zatwierdzenie każdego wniosku o zmianę i konsekwencje wprowadzenia zmiany muszą być należycie udokumentowane (dokumentacja żądania zmiany, decyzja co do zmiany oraz wynik zmiany).
4. Przed zaakceptowaniem zmiany należy przeprowadzić ocenę ryzyka związanego z wprowadzeniem zmiany. W wypadku, gdy w wyniku oceny ryzyka okaże się, że wprowadzenie zmiany powoduje ryzyko dla Bezpieczeństwa Informacji należy zastosować środki eliminujące to ryzyko lub minimalizujące je do poziomu akceptowalnego w Grupie Selena..
5. Każda zmiana, przed jej wdrożeniem do środowiska produkcyjnego (do korzystania przez Użytkowników) powinna zostać przetestowana w odizolowanym, kontrolowanym i reprezentatywnym środowisku, aby zminimalizować ewentualny negatywny wpływ na odpowiedni proces biznesowy oraz ocenić wpływ zmiany na Bezpieczeństwo Informacji w Grupie Selena.
6. Implementacja każdej zmiany powinna być zatwierdzona przed wdrożeniem przez upoważnioną osobę.
7. Wszyscy Użytkownicy, których zmiana dotyczy, zostaną powiadomieni o zmianie.
8. Szczegółowe zasady dotyczące zarządzania zmianą w poszczególnych Systemach Przetwarzania mogą zostać opisane w odrębnych procedurach i instrukcjach.

XVI. ZASADY REAGOWANIA NA NARUSZENIA BEZPIECZEŃSTWA INFORMACJI

1. Naruszenie Bezpieczeństwa Informacji to incydent prowadzący do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do Informacji przesyłanych, przechowywanych lub w inny sposób przetwarzanych.

6. Szczegółowy tryb postępowania w sprawach naruszeń Bezpieczeństwa Informacji reguluje odrębna *Procedura zgłaszania naruszeń i postępowania w sprawach związanych ze stosowaniem polityk bezpieczeństwa w Grupie Selena,* do której przestrzegania zobowiązani są wszyscy Współpracownicy.
7. Odrębne procedury obowiązujące w Grupie Selena regulują obowiązek raportowania incydentów bezpieczeństwa do odpowiednich organów wynikający z przepisów prawa powszechnie obowiązującego.

XVII. ZARZĄDZANIE CIĄGŁOŚCIĄ DZIAŁANIA

1. Grupa Selena zapewnia ciągłość działania usług związanych z Przetwarzaniem Informacji.
2. W celu skutecznego zarządzania ciągłością działania stosowane są zasady:
    1) opracowanie i wdrożenie planów ciągłości działania dla krytycznych Systemów Przetwarzania w Grupie Selena;
    2) wskazanie osób odpowiedzialnych za utrzymanie ciągłości działania Systemów Przetwarzania w Grupie Selena;
    3) podział odpowiedzialności za zarządzanie ciągłością działania.
3. Szczegółowe regulacje mogą zostać wprowadzone odrębnym dokumentem dotyczącym zachowania ciągłości działania w Grupie Selena lub w poszczególnych Spółkach z Grupy Selena opracowanym na podstawie procedur podstawowych.

XVIII. POSTANOWIENIA KOŃCOWE

1. Właściciel PBI powinien zapewnić zapoznanie się z niniejszą PBI przez wszystkie osoby, których ona dotyczy.
2. PBI może być udostępniona także:
    1) podmiotom, które powierzają Grupie Selena Informacje o charakterze poufnym;

	Imię i Nazwisko	Stanowisko	Data i podpis
Opracował:	Szostek_Bar i Partnerzy Kancelaria Prawna	Radcy Prawni	
Zatwierdził:	Wojciech Knapik	CIO	
Zatwierdził:	Michał Westerlich	Legal and Audit Department Director	

2. Naruszenia Bezpieczeństwa Informacji obejmują zarówno incydenty, których źródłem są czynniki pochodzące z zewnątrz jak i związane z przetwarzaniem danych wewnątrz Grupy Selena w sposób naruszający zasady Bezpieczeństwa Informacji.
3. Naruszenie Bezpieczeństwa Informacji może polegać na:
    1) naruszeniu poufności Informacji – w rezultacie którego dochodzi do nieuprawnionego lub przypadkowego ujawnienia lub nieuprawnionego dostępu do Informacji;
    2) naruszeniu integralności Informacji – w rezultacie którego dochodzi do nieuprawnionego lub przypadkowego zmodyfikowania Informacji;
    3) naruszenie dostępności Informacji - w rezultacie którego dochodzi do przypadkowego lub nieuprawnionego dostępu do Informacji lub zniszczenia Informacji.
4. Każdy Współpracownik jest zobowiązany do niezwłocznego zgłaszania wszelkich przypadków, w których istnieje ryzyko naruszenia Bezpieczeństwa Informacji Chronionych lub Informacji Wewnętrznych, w szczególności:
    1) zgubienia, kradzieży, pozostawienia bez nadzoru nośników danych (m in. pendrive, dyski zewnętrzne, karty pamięci) lub dokumentów w postaci papierowej w miejscach dostępnych dla Podmiotów Nieupoważnionych;
    2) awarii wewnętrznego serwera, sprzętu komputerowego lub nośników danych, które mogą spowodować utratę Informacji;
    3) zgubienia lub kradzieży kart dostępu, kluczy i innych podobnych, umożliwiających dostęp Podmiotów Nieupoważnionych do miejsc przechowywanie Informacji Chronionych lub Informacji Wewnętrznych, w szczególności do siedziby Spółek z Grupy Selena;
    4) ujawnienia haseł dostępu do urządzeń i nośników danych (m.in. komputerów i telefonów służbowych).
5. Współpracownik, który posiada wiedzę o jakimkolwiek naruszeniu Bezpieczeństwa Informacji przez Podmiot Nieupoważniony, w tym innego Współpracownika, jest zobowiązany do niezwłocznego zgłoszenia tego faktu zgodnie z *Procedurą zgłaszania naruszeń i postępowania w sprawach związanych ze stosowaniem polityk bezpieczeństwa w Grupie Selena.*

2) publicznym organom nadzoru (np. Prezes Urzędu Ochrony Danych Osobowych, Komisja Nadzoru Finansowego);

3) sądom powszechnym w sprawach związanych z Bezpieczeństwem Informacji, w których Spółka z Grupy Selena jest stroną;

4) organom władzy publicznej działającym w granicach swoich prerogatyw, na podstawie obowiązujących przepisów prawa;

5) organizacjom branżowym, w których Spółka z Grupy Selena uzyskała członkostwo.

3. Co najmniej raz w każdym roku kalendarzowym Właściciel PBI dokonuje przeglądu niniejszej PBI pod kątem aktualności oraz zgodności deklarowanego w niej stanu z prawem, warunkami zawartych umów, innymi wewnętrznymi regulacjami w Grupie Selena oraz dobrymi praktykami w zakresie Bezpieczeństwa Informacji.
4. Właściciel PBI jest uprawniony do wyznaczenia pełnomocnika ds. bezpieczeństwa informacji oraz powierzenia mu wykonywania części lub całości obowiązków i uprawnień przypisanych w niniejszej PBI do Właściciela PBI.
5. Odstępstwa od reguł Bezpieczeństwa Informacji opisanych w PBI i dokumentacji z nią powiązanej możliwe są wyłącznie po łącznym spełnieniu następujących warunków:

   1) złożenie pisemnego wniosku do Właściciela PBI o odstąpienie od reguł Bezpieczeństwa Informacji wraz z uzasadnieniem powodu odstąpienia od tych zasad;

   2) otrzymanie decyzji Właściciela PBI w formie pisemnej, elektronicznej lub dokumentowej;

   3) postępowania zgodnie z przepisami prawa.

6. Integralną część niniejszej PBI stanowią załączniki:

   1) Załącznik 1: Zasoby informacyjne w Grupie Selena;

   2) Załącznik 2: Poziomy ochrony i sposób postępowania z informacjami;

   3) Załącznik 3: Administratorzy Systemów Przetwarzania;

7. Wszelkie zmiany w PBI mogą być wprowadzane wyłącznie w drodze uchwały Zarządu Spółki, z zastrzeżeniem ust. 8 poniżej.

	Imię i Nazwisko	Stanowisko	Data i podpis
Opracował:	Szostek_Bar i Partnerzy Kancelaria Prawna	Radcy Prawni	
Zatwierdził:	Wojciech Knapik	CIO	
Zatwierdził:	Michał Westerlich	Legal and Audit Department Director	

8. Zmiany załączników do niniejszej PBI, o których mowa w ust. 5 powyżej, mogą być dokonywane przez Właściciela PBI i nie wymagają dla swojej ważności uchwały Zarządu Spółki.
9. Wszelkie zmiany niniejszej PBI oraz załączników do niej są skuteczne wobec wszystkich osób, których PBI dotyczy, z chwilą ich opublikowania w Selnecie (selnet.selena.com).
10. Niniejsza PBI wejdzie w życie po upływie dwóch tygodni od daty podania jej do wiadomości Współpracowników poprzez Selnet (selnet.selena.com).

Załącznik nr 1 – *Zasoby informacyjne w Grupie Selena*

[Plik Excel]

Załącznik nr 2 - *Poziomy ochrony i sposób postępowania z Informacjami*

Informacje Chronione	
Oznaczanie	Oznaczane jako „CHRONIONE", od momentu rozpoczęcia tworzenia Informacji przez Twórcę Informacji.
Przechowywanie	W meblach biurowych zamykanych na klucz, w szafach metalowych lub w sejfach - w zamykanych pomieszczeniach; na serwerach Grupy Selena. Informacje przechowywane na nośnikach informatycznych powinny mieć kopie zapasowe i być zabezpieczone hasłem dostępu, zaszyfrowane lub zamknięte.
Modyfikacje (edycja, kopiowanie, niszczenie)	Za zgodą Właściciela Informacji.

	Imię i Nazwisko	Stanowisko	Data i podpis
Opracował:	Szostek_Bar i Partnerzy Kancelaria Prawna	Radcy Prawni	
Zatwierdził:	Wojciech Knapik	CIO	
Zatwierdził:	Michał Westerlich	Legal and Audit Department Director	

Odczyt	Właściciel Informacji, upoważnieni Współpracownicy.
Przekazywanie wewnątrz	Za zgodą Właściciela Informacji w sposób zapewniający nieujawnienie Informacji Podmiotom Nieupoważnionym, z jednoznacznym wskazaniem odbiorcy Informacji – wyłącznie do tego odbiorcy. W obrębie sieci wewnętrznej Grupy Selena szyfrowanie nie jest wymagane.
Przekazywanie na zewnątrz	Za zgodą Właściciela Informacji oraz jego bezpośredniego przełożonego w sposób zapewniający nieujawnienie Informacji Podmiotom Nieupoważnionym. Oznaczone klauzulą „CHRONIONE". W wypadku korzystania z Internetu wymagane jest szyfrowanie połączenia lub zabezpieczenie Informacji hasłem, przekazywanym osobno innym sposobem komunikacji.
Korzystanie z Informacji poza siedzibą Spółki	Za zgodą Właściciela Informacji. Wyłącznie na bezpiecznych nośnikach, zabezpieczonych fizycznie lub kryptograficznie. Informacje w postaci elektronicznej mogą być wynoszone wyłącznie na służbowych bezpiecznych urządzeniach (komputerach, laptopach, smartfonach, tabletach) lub nośnikach (dyski zewnętrzne, pamięci przenośne).

Informacje Wewnętrzne

Oznaczanie	Oznaczane jako „WEWNĘTRZNE", od momentu rozpoczęcia tworzenia Informacji przez Twórcę Informacji.
Przechowywanie	W zamykanych pomieszczeniach i zamykanych meblach biurowych. Informacje w postaci elektronicznej powinny być przechowywane wyłącznie na serwerach Grupy Selena oraz na służbowych urządzeniach (komputerach, laptopach,

	Imię i Nazwisko	Stanowisko	Data i podpis
Opracował:	Szostek_Bar i Partnerzy Kancelaria Prawna	Radcy Prawni	
Zatwierdził:	Wojciech Knapik	CIO	
Zatwierdził:	Michał Westerlich	Legal and Audit Department Director	

	smartfonach, tabletach) lub nośnikach (dyski zewnętrzne, pamięci przenośne).
Modyfikacje (edycja, kopiowanie, niszczenie)	Za zgodą Właściciela Informacji.
Odczyt	Współpracownicy, którzy potrzebują Informacji do wykonywania swoich zobowiązań wobec Spółek z Grupy Selena.
Przekazywanie wewnątrz	Z jednoznacznym wskazaniem odbiorcy Informacji – wyłącznie do tego odbiorcy. W obrębie sieci Grupy Selena szyfrowanie nie jest wymagane.
Przekazywanie na zewnątrz	Za zgodą Właściciela Informacji, w sposób zapewniający nieujawnienie Informacji Podmiotom Nieupoważnionym.
Korzystanie z Informacji poza siedzibą Spółki	Za zgodą przełożonego. Informacje w postaci elektronicznej mogą być wynoszone wyłącznie na bezpiecznych służbowych urządzeniach (komputerach, laptopach, smartfonach, tabletach) lub nośnikach (dyski zewnętrzne, pamięci przenośne).
Informacje Publiczne	
Oznaczanie	Nie określa się zasad oznaczania.
Przechowywanie	Nie określa się zasad przechowywania.
Modyfikacje (edycja, kopiowanie, niszczenie)	Nie określa się zasad modyfikacji.

	Imię i Nazwisko	Stanowisko	Data i podpis
Opracował:	Szostek_Bar i Partnerzy Kancelaria Prawna	Radcy Prawni	
Zatwierdził:	Wojciech Knapik	CIO	
Zatwierdził:	Michał Westerlich	Legal and Audit Department Director	

Odczyt	Bez ograniczeń.
Przekazywanie wewnątrz	Bez ograniczeń.
Przekazywanie na zewnątrz	Bez ograniczeń
Korzystanie z Informacji poza siedzibą Spółki	Bez ograniczeń.

Załącznik nr 3 – *Administratorzy Systemów Przetwarzania*

[Plik Excel]

Rejestr zmian PBI

Lp.	Data	Opis	Dotyczy stron(y)	Wprowadzający zmianę

Jacek Michalak
Członek Zarządu