



PKP POLSKIE LINIE KOLEJOWE S.A.

System Zarządzania Bezpieczeństwem Informacji w PKP Polskie Linie Kolejowe S.A.		<i>Data wdrożenia SZBI:</i> 2013-01-02
Polityka Bezpieczeństwa Informacji w PKP Polskie Linie Kolejowe S.A. dla Partnerów Biznesowych Spółki	SZBI-lbi-1a	<i>Data wdrożenia:</i> 2014-12-01
	<i>Numer wersji:</i> 7	<i>Data obowiązywania wersji:</i> 2019-06-14

**Polityka
Bezpieczeństwa Informacji
w PKP Polskie Linie Kolejowe S.A.
dla Partnerów Biznesowych Spółki
SZBI-lbi-1a**

Zespół ds. utrzymania SZBI	Irmina Urban	<i>2019-06-14</i> <i>NACZELNIK WYDZIAŁU</i> <i>Irmina Urban</i>	Pełnomocnik ds. SZBI	PEŁNOMOCNIK PKP Polskie Linie Kolejowe S.A. ds. Systemu Zarządzania Bezpieczeństwem Informacji <i>Grzegorz Kuta</i>
<i>Opracowane przez</i>	<i>Uzgadnia</i>	<i>Data i podpis</i>	<i>Zatwierdza</i>	<i>Data i podpis</i> <i>13.06.2019</i>

Właściciel: PKP Polskie Linie Kolejowe S.A.

Wydawca: PKP Polskie Linie Kolejowe S.A. Centrala
Biuro Bezpieczeństwa Informacji i Spraw Obronnych
ul. Targowa 74, 03-734 Warszawa
tel. 22 47 324 00
www.plk-sa.pl, e-mail: ioi@plk-sa.pl

Wszelkie prawa zastrzeżone.

Modyfikacja, wprowadzanie do obrotu, publikacja, kopiowanie i dystrybucja
w celach komercyjnych, całości lub części dokumentu,
bez uprzedniej zgody PKP Polskie Linie Kolejowe S.A. – są zabronione

PKP POLSKIE LINIE KOLEJOWE S.A.	SZBI-lbi-1a	wersja 7
		Data obowiązywania wersji: 2019-06-14

Spis treści

§ 1. Podstawa prawna	5
§ 2. Cel	5
§ 3. Postanowienia ogólne.....	6
§ 4. Cel zarządzania bezpieczeństwem informacji w Spółce	6
§ 5. Aktywa Spółki podlegające ochronie	7
§ 6. Zasada skutecznej ochrony informacji.....	7
§ 7. Zasady klasyfikacji informacji.....	7
§ 8. Bezpieczeństwo osobowe	8
§ 9. Bezpieczeństwo fizyczne	8
§ 10. Bezpieczeństwo teleinformatyczne.....	9
§ 11. Bezpieczeństwo w umowach, porozumieniach, współpracy (także „bezumownej”).	9
§ 12. Odpowiedzialność za przestrzeganie zasad bezpieczeństwa informacji w związku z realizowaną umową, porozumieniem lub współpracą „bezumowną”	9
§ 13. Tabela zmian	10

PKP POLSKIE LINIE KOLEJOWE S.A.	SZBI-Ibi-1a	wersja 7
		Data obowiązywania wersji: 2019-06-14

PKP POLSKIE LINIE KOLEJOWE S.A.	SZBI-Ibi-1a	wersja 7
		Data obowiązywania wersji: 2019-06-14

§ 1.

Podstawa prawna

„Polityka Bezpieczeństwa Informacji w PKP Polskie Linie Kolejowe S.A. dla Partnerów Biznesowych Spółki SZBI-Ibi-1a”, zwana również w skrócie SZBI-Ibi-1a, jest elementem dokumentacji certyfikowanego Systemu Zarządzania Bezpieczeństwem Informacji w PKP Polskie Linie Kolejowe S.A. (SZBI) i jest zgodna z obowiązującym prawem oraz międzynarodowymi standardami w zakresie zarządzania bezpieczeństwem informacji, w szczególności z:

- 1) ustawą z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych;
- 2) przepisami o ochronie danych osobowych, tzn. Rozporządzeniem 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) (Dz. Urz. UE L 119 z 2016 r., str. 1-88), zwanym dalej RODO i przepisami krajowymi wprowadzonymi na mocy RODO;
- 3) ustawą o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości, wdrażająca w życie przepisy dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchyłającą decyzję ramową Rady 2008/977/WSiSW (Dz. Urz. UE L 119 z 04.05.2016, str. 89) na podstawie art. 175 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych, zwana dalej DODO i przepisami krajowymi wprowadzonymi na mocy DODO;
- 4) ustawą z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji;
- 5) ustawą z dnia 6 września 2001 r. o dostępie do informacji publicznej;
- 6) ustawą z dnia 5 lipca 2018 o krajowym systemie cyberbezpieczeństwa;
- 7) przepisami wykonawczymi wydanymi na podstawie w/w ustaw;
- 8) normą ISO/IEC 27001, zwaną dalej Normą.

§ 2.

Cel

1. Celem dokumentu SZBI-Ibi-1a jest zapoznanie Partnerów biznesowych PKP Polskie Linie Kolejowe S.A, zwanej dalej Spółką, z podstawowymi wymaganiami i zasadami Spółki w zakresie bezpieczeństwa informacji oraz w zakresie ogólnego podejścia Spółki do bezpieczeństwa informacji.
2. Jako wskazanych w ust. 1 Partnerów biznesowych Spółki, zwanych dalej Partnerami, rozumie się podmioty:

PKP POLSKIE LINIE KOLEJOWE S.A.	SZBI-Ibi-1a	wersja 7
		Data obowiązywania wersji: 2019-06-14

- 1) ubiegające się bądź zobligowane do zawarcia umowy lub porozumienia ze Spółką,
 - 2) współpracujące ze Spółką, także w ramach współpracy „bezumownej”,
- gdy z realizacją tych umów, porozumień lub współpracy, wiąże się z dostępem Partnera do informacji dotyczących Spółki, będących własnością Spółki, chronionych w Spółce.

§ 3.

Postanowienia ogólne

1. SZBI-Ibi-1a jest dokumentem:
 - 1) przeznaczonym dla Partnerów;
 - 2) opartym o przyjęty przez Zarząd Spółki dokument wewnętrzny „Polityka Bezpieczeństwa Informacji w PKP Polskie Linie Kolejowe S.A. SZBI-Ibi-1”, zwany dalej SZBI-Ibi-1, wyznaczający kierunki i zasady dotyczące zarządzania bezpieczeństwem informacji w Spółce,
 - 3) znanym wszystkim pracownikom Spółki, także w szczególności pracownikom, którzy mają swój udział w procesie przygotowywania umów lub porozumień z Partnerami, organizowania współpracy z nimi oraz nadzorowania ich realizacji z zachowaniem wymagań bezpieczeństwa informacji.
2. Zasady klasyfikacji informacji w Spółce opisuje § 7.
3. Dokument SZBI-Ibi-1a jest regulacją, z którą mają obowiązek zapoznać się Partnerzy, w sposób możliwy do udokumentowania.
4. Dokument SZBI-Ibi-1a jest dokumentem przeznaczonym do publikacji na stronie internetowej Spółki.

§ 4.

Cel zarządzania bezpieczeństwem informacji w Spółce

1. Celem zarządzania bezpieczeństwem informacji w Spółce, jest:
 - 1) zapewnienie ciągłości realizacji zadań statutowych Spółki;
 - 2) zapewnienie odpowiedniego poziomu poufności, integralności, dostępności i rozliczalności informacji;
 - 3) w szczególności zapewnienie odpowiedniego poziomu bezpieczeństwa danych osobowych oraz wypełniania praw i wolności osób, których dane są przetwarzane w Spółce;
 - 4) zapewnienie ciągłości realizacji zadań Spółki, jako operatora usługi kluczowej.
2. Zarząd Spółki deklaruje pełne wsparcie dla realizacji w/w celów oraz wolę zapewnienia niezbędnych ku temu zasobów.

§ 5.**Aktywa Spółki podlegające ochronie**

W Spółce dokonano analizy, na podstawie której dokonano oceny, iż informacje stanowią niezwykle ważny element aktywów podlegających w Spółce ochronie.

§ 6.**Zasada skutecznej ochrony informacji**

Efektywność ochrony informacji zapewnia wyłącznie jednoczesne zastosowanie wybranych odpowiednio rozwiązań w zakresie bezpieczeństwa fizycznego, bezpieczeństwa osobowego, bezpieczeństwa organizacyjnego oraz bezpieczeństwa teleinformatycznego.

§ 7.**Zasady klasyfikacji informacji**

1. W PKP Polskie Linie Kolejowe S.A. obowiązuje klasyfikacja informacji na poniższe grupy:
 - 1) grupa I: informacje niejawne – w rozumieniu przepisów o ochronie informacji niejawnych;
 - 2) grupa II: dane osobowe – w rozumieniu przepisów o ochronie danych osobowych;
 - 3) grupa III: informacje stanowiące tajemnicę przedsiębiorcy PKP Polskie Linie Kolejowe S.A. – w rozumieniu przepisów o zwalczaniu nieuczciwej konkurencji lub o dostępie do informacji publicznej;
 - 4) grupa IV: informacje podmiotów zewnętrznych uzyskane przez Spółkę w związku z realizowanymi umowami, porozumieniami, prowadzoną współpracą z tymi podmiotami zewnętrznymi, itp., których ochrona wynika z zawartych umów, porozumień oraz obowiązujących przepisów prawa;
 - 5) grupa V: informacje wewnętrzne Spółki, wytworzone w Spółce lub na jej rzecz, niewchodzące w zakres informacji zaklasyfikowanych do pozostałych grup;
 - 6) grupa VI: informacje publicznie dostępne (jawne).
2. Przy klasyfikacji informacji przyjęto w Spółce następujące zasady:
 - 1) jeśli informacja jest niejawna w rozumieniu przepisów o ochronie informacji niejawnych, należy zaklasyfikować ją do grupy I i postępować zgodnie z przepisami o ochronie informacji niejawnych, regulującymi wymagania współpracy w sposób szczególny;
 - 2) jeśli informacja stanowi dane osobowe w rozumieniu przepisów o ochronie danych osobowych należy zaklasyfikować ją do grupy II i postępować z nią zgodnie z tymi przepisami i warunkami umowy, porozumienia, w szczególności wymaganiami określonymi przez:
 - a) Spółkę, jako administratora danych, w zakresie zbiorów danych osobowych, obejmujące czynności na danych osobowych, których administratorem jest PKP Polskie Linie Kolejowe S.A. i których rejestr prowadzony jest zgodnie z RODO;

b) Komendanta Głównego Straży Ochrony Kolei, jako administratora danych w zakresie zbiorów danych osobowych przetwarzanych w ramach czynności w związku z zapobieganiem i zwalczaniem przestępczości, ujętych w rejestrze kategorii czynności prowadzonym zgodnie z DODO

w umowie powierzenia przetwarzania danych osobowych, zawartej na podstawie tych przepisów;

- 3) jeśli informacja stanowi tajemnicę przedsiębiorcy (tajemnicę przedsiębiorstwa w rozumieniu przepisów o zwalczaniu nieuczciwej konkurencji lub tajemnicę przedsiębiorcy w rozumieniu przepisów o dostępie do informacji publicznej), należy zaklasyfikować ją do grupy III i postępować z nią (chronić) zgodnie z przepisami o zwalczaniu nieuczciwej konkurencji, przepisami o dostępie do informacji publicznej, warunkami umowy lub porozumienia, w szczególności wymaganiami określonymi przez Spółkę w umowie o zachowaniu poufności;
 - 4) informacje podmiotów zewnętrznych uzyskane przez Spółkę w związku z realizowanymi umowami, porozumieniami, prowadzoną współpracą z tymi podmiotami zewnętrznymi, itp., należy zakwalifikować do grupy IV i postępować zgodnie z zawartymi umowami oraz obowiązującymi przepisami prawa;
 - 5) informacje wewnętrzne Spółki, wytworzone w Spółce lub na jej rzecz, niewchodzące w zakres informacji zaklasyfikowanych do pozostałych grup, należy zakwalifikować do grupy V i postępować zgodnie z zawartymi umowami oraz obowiązującymi przepisami prawa;
 - 6) informacje publicznie dostępne (jawne), których odpowiednia ochrona obowiązuje do momentu publikacji przez Spółkę, należy zakwalifikować do grupy VI.
3. Szczególnym przypadkiem wyłączenia informacji spod stosowania ustawy o dostępie do informacji publicznej, jest przypadek dotyczący informacji o podatnościach, incydentach i zagrożeniach cyberbezpieczeństwa oraz o ryzyku wystąpienia incydentów, do której stosuje się wyłączenie na mocy art. 37 ust. 1 ustawy o krajowym systemie cyberbezpieczeństwa.

§ 8.

Bezpieczeństwo osobowe

Dla każdej grupy informacji wymagania dotyczące bezpieczeństwa osobowego wynikają z odpowiednich przepisów prawa i zapisów w umowach, porozumieniach zawartych z Partnerami.

§ 9.

Bezpieczeństwo fizyczne

1. Bezpieczeństwo fizyczne określają w Spółce wprowadzone uregulowania wewnętrzne.
2. W zakresie niezbędnym z punktu widzenia interesu Spółki, wybrane wymagania w stosunku do Partnera dotyczące bezpieczeństwa fizycznego, są formułowane przed rozpoczęciem współpracy z Partnerem.

PKP POLSKIE LINIE KOLEJOWE S.A.	SZBI-lbi-1a	wersja 7
		Data obowiązywania wersji: 2019-06-14

§ 10.

Bezpieczeństwo teleinformatyczne

1. Bezpieczeństwo informacji przetwarzanej w systemach informacyjnych lub sieciach teleinformatycznych ma na celu utrzymanie podstawowych atrybutów bezpieczeństwa teleinformatycznego, w szczególności: poufności, integralności, autentyczności i dostępności, co przekłada się na jej ochronę: przed nieuprawnionym dostępem, ujawnieniem, przed losowym lub nieuprawnionym zniszczeniem lub modyfikacją, a także przed nieuzasadnioną odmową lub opóźnieniem jej dostarczenia.
2. Zapewnienie utrzymania atrybutów bezpieczeństwa teleinformatycznego należy również do obowiązków Partnerów, na każdym etapie współpracy ze Spółką.

§ 11.

Bezpieczeństwo w umowach, porozumieniach, współpracy (także „bezumownej”)

1. Partner ma obowiązek zapoznać się z dokumentem SZBI-lbi-1a, zgodnie z zapisami w § 3 ust. 3, z zastrzeżeniem zapisów ust. 2.
2. Wymóg zapoznania się z zapisami dokumentu SZBI-lbi-1a przez Partnera, obowiązuje również wszystkie osoby kierowane przez Partnera do realizacji umowy, porozumienia lub współpracy, w takim zakresie tych osób, który zapewni przestrzeganie zapisów SZBI-lbi-1a w trakcie realizacji umowy, porozumienia lub współpracy.
3. Wymóg zapoznania się z zapisami dokumentu SZBI-lbi-1a określa się w zawieranej umowie lub porozumieniu, o których mowa w § 2 ust. 2 pkt 1.
4. W zawieranej umowie lub porozumieniu dookreśla się, stosownie do potrzeb:
 - 1) wymagania, w stosunku do Partnera, dotyczące ochrony informacji Spółki;
 - 2) skutki oraz zakres odpowiedzialności z tytułu nieprzestrzegania wymagań związanych z ochroną informacji Spółki przez Partnera.
5. W przypadku współpracy „bezumownej”, Partner potwierdza Spółce na piśmie fakt zapoznania się z SZBI-lbi-1a, w rozumieniu określonym w ust. 2.

§ 12.

Odpowiedzialność za przestrzeganie zasad bezpieczeństwa informacji w związku z realizowaną umową, porozumieniem lub współpracą „bezumowną”

Za zapewnienie przestrzegania zasad bezpieczeństwa informacji dotyczących Spółki, będących własnością Spółki, chronionych w Spółce przez osoby realizujące umowę, porozumienie lub współpracę z ramienia Partnera, odpowiada przed Spółką bezpośrednio Partner.

§ 13.
Tabela zmian

L.p.	Nr: paragraf/ ust./pkt/lit./tiret	Numer wersji po zmianie / Data zmiany	Opis zmiany
1	2	3	4
1	Nagłówek dokumentu § 1 pkt 2 § 6 ust. 1 pkt 2	2 /2015-03-02	Poprawienie omyłki w dacie wdrożenia dokumentu Uwzględnienie zmiany ustawy o ochronie danych osobowych Doprecyzowanie pojęcia tajemnica przedsiębiorcy
2	Cały dokument Załącznik	3/2016-08-01	Zmiany polegające na doprecyzowaniu zapisów; Wycofano (wzór oświadczenia o zapoznaniu z dokumentem SZBI-Ibi-1a)
3	Cały dokument	4/2018-05-25	Uwzględnienie zmiany przepisów o ochronie danych osobowych
4	Cały dokument	5/2018-11-30	Doprecyzowanie zapisów.
5	Cały dokument	6/2019-03-20	Uwzględnienie wejścia w życie przepisów o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości
6	Cały dokument	7/2019-06-14	Zmiany dotyczące wejścia w przepisów o krajowym systemie cyberbezpieczeństwa,