PKP POLSKIE LINIE KOLEJOWE S.A.

System Zarządzania Bezpieczeństwem Informacji w PKP Polskie Linie Kolejowe S.A.		*Data wdrożenia SZBI:* **2013-01-02**
Polityka Bezpieczeństwa Informacji w PKP Polskie Linie Kolejowe S.A. dla Partnerów Biznesowych Spółki	**SZBI-Ibi-1a**	*Data wdrożenia:* **2014-12-01**
	Numer wersji: **10**	*Data obowiązywania wersji:* **2022-03-22**

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

Zespół ds. utrzymania SZBI	**Paweł Krzyżek**	Elektronicznie podpisany przez Pawel Krzyzek (PLK056235) Data: 2022.03.18 11:39:04 +01'00'	**Pełnomocnik ds. SZBI**	Elektronicznie podpisany przez Grzegorz Jan Kuta Data: 2022.03.18 11:42:09 +01'00'
Opracowane przez	*Uzgadnia*	*Data i podpis*	*Zatwierdza*	*Data i podpis*

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

Spis treści

§ 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 uchylającą 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 11 sierpnia 2021 r. o otwartych danych i ponownym wykorzystywaniu informacji sektora publicznego;
7) ustawą z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa;
8) przepisami wykonawczymi wydanymi na podstawie w/w ustaw;
9) normą ISO/IEC 27001, zwaną dalej Normą.

§ 2.
Cel

1. Celem dokumentu SZBI-Ibi-1a jest:
   1) zapewnienie bezpieczeństwa informacji, w tym tych przetwarzanych w systemach teleinformatycznych PKP Polskie Linie Kolejowe S.A., zwanej dalej Spółką, poprzez

zapoznanie wszystkich podmiotów zewnętrznych wykonujących na rzecz Spółki jakiekolwiek prace bądź z nią współpracujących;

2) zapoznanie podmiotów zewnętrznych, o których mowa w pkt 1 z minimalnymi wymaganiami i zasadami Spółki w zakresie bezpieczeństwa informacji oraz podejściem Spółki do zagadnień związanych z bezpieczeństwem informacji.

2. Jako wskazane w ust. 1 podmioty zewnętrzne, zwane dalej Partnerami, rozumie się podmioty:

1) ubiegające się bądź zobligowane do zawarcia umowy lub porozumienia ze Spółką;

2) współpracujące ze Spółką, także w ramach współpracy „bezumownej".

gdy realizacja 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. Dokument SZBI-Ibi-1a jest regulacją, z którą mają obowiązek zapoznać się Partnerzy, w sposób możliwy do udokumentowania.

3. 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) minimalizacja ryzyka wystąpienia zagrożeń i skuteczna implementacja zabezpieczenia informacji dla zapewnienia ciągłości realizacji zadań statutowych Spółki;

2) zapewnienie odpowiedniego poziomu poufności, integralności, dostępności i rozliczalności informacji w ramach kontaktów biznesowych z osobami trzecimi jak i wewnątrz Spółki, dla stworzenia jak najlepszych warunków do realizacji zadań, o których mowa w pkt 1;

3) zapewnienie odpowiedniego poziomu bezpieczeństwa danych osobowych oraz realizacja praw i wolności osób, których dane są przetwarzane w Spółce;

4) zapewnienie odpowiedniego poziomu bezpieczeństwa informacji, by utrzymać ciągłość 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.
Informacje podlegające ochronie w Spółce

W Spółce dokonano analizy, w wyniku której ustalono, iż informacje stanowią niezwykle ważny element podlegający ochronie. Przetwarzanie informacji w Spółce realizowane jest w ramach wyodrębnionych typów i grup aktywów.

§ 6.
Zasady postępowania z informacjami w Spółce

1. Postępowanie z poszczególnymi rodzajami informacji we współpracy Partnerów z PKP Polskie Linie Kolejowe S.A. przebiega zgodnie z poniższymi zasadami:

   1) jeśli informacja jest niejawna w rozumieniu przepisów o ochronie informacji niejawnych, należy postępować zgodnie z przepisami o ochronie informacji niejawnych, regulującymi wymagania tej współpracy;

   2) jeśli informacja stanowi dane osobowe w rozumieniu przepisów o ochronie danych osobowych należy postępować z nią zgodnie z tymi przepisami i warunkami umowy, porozumienia, w szczególności wymaganiami określonymi:

      a) przez 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) przez 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,

      c) 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 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) jeśli informacja stanowi informacje Partnerów uzyskane przez Spółkę w związku z realizowanymi umowami, porozumieniami, prowadzoną współpracą z Partnerami, itp., należy z nią postępować zgodnie z zawartymi umowami oraz obowiązującymi przepisami prawa;

5) jeśli informacja stanowi informacje wewnętrzne Spółki, wytworzone w Spółce lub na jej rzecz, niewchodzące w zakres informacji zaklasyfikowanych do pozostałych grup, należy postępować z nimi zgodnie z zawartymi umowami oraz obowiązującymi przepisami prawa;

6) jeśli informacja stanowi informacje publicznie dostępne (jawne), to ich odpowiednia ochrona obowiązuje do momentu publikacji przez Spółkę.

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.

§ 7.
Bezpieczeństwo fizyczne i osobowe

1. Partnerzy przed rozpoczęciem przetwarzania informacji należących do Spółki powinni spełnić następujące warunki:

   1) podpisać umowę o zachowaniu poufności, bądź zawrzeć zapisy wynikające z umowy o zachowaniu poufności w Umowie Właściwej, pod warunkiem zawarcia w nich zastrzeżenia, że zapisy dotyczące obowiązku zachowania poufności pozostają w mocy po zakończeniu Umowy Właściwej, przez wskazany w Umowie Właściwej okres;

   2) w przypadku potrzeby przetwarzania przez Partnerów danych osobowych, ze zbiorów, których Administratorem jest PKP Polskie Linie Kolejowe S.A., podpisać umowę powierzenia przetwarzania danych osobowych zgodnie ze wzorem obowiązującym w Spółce;

   3) w przypadku potrzeby przetwarzania przez Partnerów danych osobowych, ze zbiorów, których Administratorem jest Komendant Główny Straży Ochrony Kolei jako Administratora podpisać umowę powierzenia przetwarzania danych osobowych zgodnie ze wzorem zatwierdzonym przez Komendanta Głównego Straży Ochrony Kolei.

2. Pracownicy Partnerów wykonujący na rzecz Spółki prace zgodnie z zawartą umową lub porozumieniem bezumownym mogą przebywać na jej terenie pod nadzorem pracownika Spółki lub pracowników ochrony obiektu (terenu).

3. Partnerzy powinni dopilnować by pomieszczenia, w których znajdą się dokumenty bądź nośniki informatyczne zawierające informacje chronione Spółki, powinny zostać zabezpieczone, odpowiednio do zidentyfikowanych przez Partnerów zagrożeń, ze

szczególnym uwzględnieniem ryzyka przejęcia informacji chronionych przez osoby nieupoważnione oraz ryzyka ich modyfikacji lub usunięcia.

4. W stosunku do wszystkich zasobów teleinformatycznych Spółki udostępnionych Partnerom, stosuje się odpowiednie mechanizmy bezpieczeństwa zapewniające poufność, integralność, dostępność, autentyczność i rozliczalności informacji w nich przetwarzanych.
5. Partner przed uzyskaniem dostępu do systemu informacyjnego Spółki powinien spełnić wymagania zawarte w niniejszym dokumencie.
6. Spółka posiada szereg dokumentów zapewniających bezpieczeństwo informacji uzyskanych w drodze współpracy z Partnerami, a zwłaszcza Politykę Bezpieczeństwa Informacji Partnerów Biznesowych w PKP Polskie Linie Kolejowe S.A. SZBI-Ibi-6.
7. Znajomość SZBI-Ibi-1a, a także Polityki Bezpieczeństwa Informacji Partnerów Biznesowych w PKP Polskie Linie Kolejowe S.A. SZBI-Ibi-6 i przestrzeganie zapisów w niej zawartych, należy do obowiązków wszystkich pracowników Spółki.

§ 8.
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 oraz modyfikacją, a także przed nieuzasadnioną odmową lub opóźnieniem jej dostarczenia.
2. Zapewnienie utrzymania atrybutów bezpieczeństwa teleinformatycznego, wskazanych przez pracowników Spółki bądź zawartych w umowie ze Spółką, należy również do podstawowych obowiązków Partnerów, na każdym etapie współpracy ze Spółką.
3. Do systemu informacyjnego Spółki mogą zostać podłączone wyłącznie komputery i urządzenia zgodne z minimalnymi wymaganiami bezpieczeństwa, w szczególności posiadające:
    1) system operacyjny wspierany przez producenta i zainstalowane wszystkie dostępne aktualizacje zabezpieczeń;
    2) zainstalowany system antywirusowy w systemie operacyjnym, którego sygnatury są aktualne;
    3) uruchomiony w systemie operacyjnym firewall, który posiada właściwą konfigurację;
    4) zainstalowane na komputerze oprogramowanie pochodzące z zaufanych źródeł;
    5) oprogramowanie zainstalowane zgodnie z postanowieniami umowy licencyjnej;
    6) oprogramowanie niełamiące praw autorskich.
4. Partnerzy korzystający z systemów informacyjnych Spółki służących do świadczenia usługi kluczowej, muszą zapewnić ich instalację w obszarach chronionych w sposób

szczególny, przed nieuprawnionym dostępem i szkodami wynikającymi ze zdarzeń losowych.

5. Partnerzy nie powinni uzależniać ochrony udostępnionego przez Spółkę systemu informacyjnego wyłącznie od jednego mechanizmu zabezpieczenia, nawet, gdy zastosowana technologia jest uznawana za wysoce zaawansowaną i niezawodną.
6. System poczty elektronicznej Spółki posiada zainstalowane mechanizmy ochrony przed zagrożeniami (wirusami i spamem), a podejrzane wiadomości przechowywane są w kwarantannie.
7. Partnerzy zobowiązują się do stosowania obowiązujących w Spółce zasad bezpieczeństwa podczas przesyłania wiadomości do Spółki drogą elektroniczną.
8. Pracownicy Partnerów podczas komunikacji z pracownikami Spółki są zobowiązani do:
   1) sprawdzenia czy przesyłane załączniki nie zawierają oprogramowania złośliwego;
   2) nierozsyłania za pośrednictwem poczty elektronicznej do pracowników Spółki informacji mogących stanowić zagrożenie dla systemu informacyjnego (tzw. spamu, łańcuszków szczęścia, itp.);
   3) nieprzesyłania treści zabronionych prawem i informacji niezgodnych z dobrymi obyczajami, np.: dyskryminacja rasowa, itp.
9. Zasady bezpiecznego korzystania pracowników Partnerów z sieci teleinformatycznej Spółki przeznaczonej dla gości są uzgadniane indywidualnie, po uprzednim zgłoszeniu potrzeby takiego dostępu u pracownika Spółki.
10. Dostęp do systemu informacyjnego Spółki jest możliwy wyłącznie poprzez podanie prawidłowego identyfikatora (loginu) i hasła przyznanego użytkownikowi podczas procesu nadawania uprawnień.
11. Polityka haseł dostępu użytkowników Partnerów do systemu informacyjnego Spółki podlega następującym zasadom:
    1) hasło składa się z minimum 8 znaków;
    2) hasło musi spełniać warunek złożoności polegający na występowaniu w nim: wielkiej i małej litery, oraz cyfry lub znaku specjalnego (np. !@#);
    3) hasło musi być zmieniane nie rzadziej niż raz na 30 dni;
    4) kolejne hasła muszą być różne (zapamiętywanych jest minimum 6 ostatnich haseł);
    5) hasła należy przechowywać w sposób gwarantujący ich poufność;
    6) zabrania się udostępniania haseł innym osobom.
12. Zabrania się tworzenia haseł na podstawie:
    1) cech i numerów osobistych (np. dat urodzenia, imion, itp.);
    2) sekwencji klawiszy klawiatury (np. qwerty, 12qwaszx);
    3) identyfikatora (loginu) użytkownika systemu.

13. Zabrania się tworzenia haseł łatwych do odgadnięcia, a logowanie anonimowe przez pracowników Partnera jest zabronione.
14. Uwierzytelnienie następuje wyłącznie po podaniu zgodnego hasła i powiązanego z nim identyfikatora (loginu).
15. W przypadku pierwszego logowania każdy użytkownik ma obowiązek zmiany hasła tymczasowego na właściwe, na znane tylko sobie.
16. W przypadku systemów, które nie wymuszają automatycznie cyklicznej zmiany hasła oraz nie kontrolują jego złożoności, obowiązkiem każdego użytkownika jest zmiana hasła zgodnie z powyższymi zasadami.
17. Użytkownik ponosi pełną odpowiedzialność za utworzenie hasła i jego bezpieczne przechowywanie.
18. Hasła nie mogą być ujawniane w sposób celowy lub przypadkowy oraz powinny być znane wyłącznie użytkownikowi.
19. Hasła nie powinny być przechowywane w formie dostępnej dla osób nieupoważnionych:
    1) w plikach;
    2) na kartkach papieru w miejscach dostępnych dla osób trzecich;
    3) w skryptach;
    4) w innych zapisach elektronicznych i papierowych, które byłyby dostępne dla osób trzecich.
20. W przypadku, gdy Partner podejrzewa ujawnienie haseł osobie nieupoważnionej, hasła muszą być natychmiast zmienione przez użytkownika, a fakt ten zgłoszony pracownikowi Spółki wskazanemu do kontaktu w treści umowy lub porozumienia.
21. Hasło utrzymuje się w tajemnicy również po upływie jego ważności.
22. Zmiany hasła dokonuje pracownik lub pełnomocnik Partnera (w przypadku, gdy zapomniano hasła, Partner zgłasza ten fakt pracownikowi Spółki wskazanemu do kontaktu w treści umowy lub porozumienia, który przekaże zwrotnie ustawione hasło tymczasowe użytkownikowi z wymuszeniem jego zmiany podczas pierwszego logowania).

§ 9.
Przepływ informacji i komunikacja z Partnerami

1. Komunikacja i przepływ informacji z Partnerami odbywa się poprzez kanały komunikacji wyszczególnione w umowach i porozumieniach z Partnerami oraz poprzez inne kanały komunikacji i przepływu informacji dopuszczone do stosowania przez Spółkę.
2. Po analizie ryzyka i uzyskaniu zgody Dyrektora Biura Bezpieczeństwa Informacji i Spraw Obronnych Centrali Spółki jest możliwość odstępstwa od zapisów, o których mowa w ust. 1.

3. Obieg informacji pomiędzy Spółką, a Partnerami musi odbywać się z zachowaniem zasady rozliczalności.
4. Obieg informacji chronionych, o którym mowa w ust. 3, przesyłanych pocztą elektroniczną e-mail, ze szczególnym uwzględnieniem informacji stanowiących tajemnicę przedsiębiorstwa Spółki oraz danych osobowych (z wyłączeniem danych osobowych zaliczanych do szczególnej kategorii), jest możliwy wyłącznie przy zachowaniu poniższych zasad:
   1) informacje należy przesyłać w plikach, wyłącznie w postaci załączników do wiadomości e-mail (obowiązuje zakaz przesyłania danych osobowych lub informacji stanowiących tajemnicę przedsiębiorstwa Spółki, jako niezabezpieczony tekst w treści wiadomości (bez zabezpieczenia) w poczcie elektronicznej;
   2) pliki zawierające informacje chronione, przed wysłaniem pocztą elektroniczną e-mail zabezpiecza się poprzez spakowanie do archiwum i zaszyfrowanie z użyciem „silnego” hasła dostępu;
   3) hasło do rozpakowania pliku przekazuje się adresatowi/adresatom materiału innym środkiem komunikacji, niż poczta elektroniczna (np. telefonicznie, sms);
   4) dla wiadomości, przed jej wysłaniem, włącza się obowiązkowo następujące ustawienia:
      a) charakter – „Poufny”,
      b) opcję żądania potwierdzenia dostarczenia wiadomości,
      c) opcję żądania potwierdzenia przeczytania wiadomości.
   5) temat przesyłanej poczty powinno się poprzedzić się wyraźnym oznaczeniem np. „Informacje w załączeniu” (w ten sposób odbiorca przesyłki otrzyma informację, że załączono plik – spakowany z hasłem – zawierający zabezpieczone informacje chronione).
5. W przypadku braku możliwości zastosowania przez Partnerów rozwiązania, o którym mowa w ust. 4, bądź sposobów komunikacji określonych w szczegółach współpracy ze Spółką, obieg informacji jest możliwy przy zastosowaniu mechanizmów szyfrujących.
6. Mechanizmy szyfrujące, o których mowa w ust. 5, muszą uwzględniać podpisywanie i szyfrowanie wymienianej informacji za pośrednictwem oprogramowania szyfrującego, zaakceptowanych uprzednio przez Biuro Bezpieczeństwa Informacji i Spraw Obronnych Centrali Spółki.
7. Partnerzy powinni dołożyć wszelkich starań, aby zabezpieczenia kryptograficzne stosować również:
   1) na dyskach twardych komputerów, w tym zwłaszcza komputerów przenośnych, na których przetwarzane są informacje chronione Spółki;
   2) na pendrive’ach i innych nośnikach danych używanych do przechowywania informacji;

3) na nośnikach kopii zapasowych;

4) na urządzeniach mobilnych (jeśli posiadają techniczne możliwości przetwarzania informacji chronionych Spółki);

5) w tunelach VPN.

8. W przypadku planowanego przetwarzania przez Partnerów informacji chronionych w chmurze, Partner zgłasza uprzednio ten fakt pracownikowi Spółki wskazanemu do kontaktu w treści umowy lub porozumienia w celu uprzedniej oceny stosowanych przez Partnera zabezpieczeń przez Biuro Bezpieczeństwa Informacji i Spraw Obronnych Centrali Spółki.

§ 10.
Zasady bezpieczeństwa przy dostępie zdalnym do zasobów systemów informacyjnych Spółki

1. Zdalny dostęp do zasobów systemów informacyjnych Spółki, możliwy jest tylko po spełnieniu warunków wymienionych w niniejszym dokumencie.
2. Zdalny dostęp Partnerów realizowany jest za pomocą systemu do zarządzania kontami uprzywilejowanymi (oprogramowanie klasy PIM/PAM), a sesje związane ze zdalnym dostępem są nagrywane.
3. Zdalnego dostępu udziela się na zasadach i na czas określony zapisami umowy.
4. Pracownik Spółki wskazany do kontaktu w treści umowy lub porozumienia wnioskuje o dostęp zdalny dla pracowników i przedstawicieli Partnera zgodnie z wewnętrznymi regulacjami Spółki.
5. Zakres zdalnego dostępu może zostać ograniczony lub zwiększony po przeanalizowaniu potrzeb określonych zapisami umowy lub porozumienia z Partnerem.
6. W ramach zdalnego dostępu do zasobów systemu informacyjnego Spółki zabrania się Partnerom:

   1) trwale usuwać danych;

   2) przeprowadzać jakichkolwiek operacji na dyskach mogących prowadzić do ich uszkodzenia lub utraty zawartych na nich danych, w tym ich formatowania,

   chyba, że zapisy umowy lub porozumienia z Partnerem stanowią inaczej.
7. Dla środowisk produkcyjnych (oddanych do eksploatacji) Partner poinformowany o fakcie wykonywania prac zdalnych w krytycznych systemach informacyjnych Spółki, przed przystąpieniem do prac, przedstawia przyczynę konieczności uzyskania dostępu wraz z oceną ryzyka podejmowanych czynności.
8. Pracownik lub przedstawiciel Partnera wykonujący zdalne prace, przystępując do czynności, co do których istnieje wysokie ryzyko utraty informacji Spółki, informuje o istniejącym ryzyku pracownika Spółki wskazanego w umowie z Partnerem jako osoba do kontaktu lub jako osoba odpowiedzialna za jej realizację z ramienia Spółki i oczekuje na formalną akceptację istniejącego poziomu ryzyka.

9. Po formalnej, pisemnej akceptacji przez Spółkę ryzyka, o którym mowa powyżej, pracownik Partnera może rozpocząć realizację czynności objętych wskazanym ryzykiem.
10. Wykonywanie prac polegających na standardowej obsłudze serwisowej lub prac nad rozwojem systemu informacyjnego będącego w fazie wdrażania nie wymaga każdorazowego ustalenia ze Spółką warunków realizacji czynności, będącej ich częścią.
11. Po analizie ryzyka i uzyskaniu zgody Dyrektora Biura Bezpieczeństwa Informacji i Spraw Obronnych Centrali Spółki jest możliwość odstępstwa od zapisów ust. 7-10.
12. W ramach wykonywania standardowej obsługi serwisowej lub prac nad rozwojem systemu informacyjnego obowiązują uzgodnione i opisane wcześniej warunki.
13. Zabrania się Partnerowi podejmowania jakichkolwiek czynności zmierzających do penetrowania zasobów teleinformatycznych Spółki, chyba, że czynności te dotyczą realizacji umowy na testy bezpieczeństwa, testy penetracyjne, itp.
14. Każdorazowe przeprowadzanie przez Partnera testów bezpieczeństwa lub testów penetracyjnych musi być realizowane za uprzednią formalną zgodą Spółki.
15. Partner zobowiązuje się do wykorzystywania tylko i wyłącznie uzgodnionych zasobów informacyjnych, nawet, jeśli dostępne są inne niż wymagane do realizacji zlecenia.
16. Na potrzeby realizacji umowy Spółka może udzielić zdalnego dostępu do następujących środowisk:
    1) testowych;
    2) produkcyjnych;
    3) szkoleniowych.
17. Zabrania się wykonywania dostępu zdalnego z komputerów oraz sieci teleinformatycznych dostępnych publicznie np. kafejki internetowe, dworce, restauracje, bezprzewodowe sieci miejskie, itp.

§ 11.
Reagowanie na incydenty

1. Każde zdarzenie naruszające bezpieczeństwo informacji, a zwłaszcza w zakresie:
    1) cyberbezpieczeństwa;
    2) ochrony powierzonych do przetwarzania danych osobowych;

    należy każdorazowo zgłaszać w formie e-mail za potwierdzeniem odbioru na adres: [manager.bpm@plk-sa.pl] z tematem wiadomości „*Naruszenie bezpieczeństwa informacji”*.
2. Jeśli zdarzenie jest ewidentnym naruszeniem bezpieczeństwa informacji natychmiastowo zawiesza się / odbiera uprawnienia użytkownikom Partnera i informuje o tym fakcie osobę wskazaną ze strony Partnera w zawartej umowie lub porozumieniu.

3. W przypadku naruszenia bezpieczeństwa informacji pracownicy Spółki oraz pracownicy lub przedstawiciele Partnera zabezpieczają ślady tego naruszenia (np. ślady włamania, logi systemowe).
4. W szczególnych przypadkach naruszenia bezpieczeństwa informacji zwłaszcza naruszenia bezpieczeństwa danych osobowych Spółka informuje organy ścigania oraz inne uprawnione podmioty o zaistniałej sytuacji.
5. Pracownicy Spółki oraz uprawniony pracownik Partnera usuwają skutki naruszenia bezpieczeństwa oraz wprowadzają dodatkowe zabezpieczenia (np. zmieniają konfigurację, itp.).
6. Pracownicy Spółki wraz z pracownikami Partnera podejmują wszelkie właściwe działania korygujące i zapobiegawcze w odniesieniu do stwierdzonego incydentu.

§ 12.
Audyty bezpieczeństwa informacji

1. Partner zobowiązuje się udostępniać Spółce wszelkie informacje niezbędne do wykazania spełnienia zapisów obligatoryjnej umowy o zachowaniu poufności oraz obowiązków określonych w aktualnych przepisach dotyczących ochrony danych osobowych, w szczególności w:
   1) art. 28 RODO;
   2) art. 34 DODO;

   a także umożliwiać Spółce, Komendantowi Głównemu Straży Ochrony Kolei lub audytorom przez nich upoważnionych przeprowadzanie audytów, w tym inspekcji.
2. Partner niezwłocznie poinformuje Spółkę, jeżeli jego zdaniem wydane mu polecenie w ramach działań, o którym mowa w ust. 1 stanowić będzie naruszenie aktualnych przepisów, a w szczególności przepisów o ochronie danych osobowych.

§ 13.
Bezpieczeństwo w umowach, porozumieniach, współpracy (także „bezumownej")

1. Partner ma obowiązek zapoznać się z dokumentem SZBI-Ibi-1a, zgodnie z zapisami w § 3 ust. 2, z zastrzeżeniem zapisów ust. 2 niniejszego §.
2. Wymóg zapoznania się z zapisami dokumentu SZBI-Ibi-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-Ibi-1a w trakcie realizacji umowy, porozumienia lub współpracy.
3. Wymóg zapoznania się z zapisami dokumentu SZBI-Ibi-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-Ibi-1a, w rozumieniu określonym w ust. 2.

§ 14.
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.

§ 15.
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,

l.p.	Nr: paragraf/ ust./pkt/lit./tiret	Numer wersji po zmianie / Data zmiany	Opis zmiany
1	*2*	*3*	*4*
7	Cały dokument	8/2020-07-01	Zmiany polegające na uszczegółowieniu zapisów.
8	§ 4 §1	9/2021-10-15	Zmiana polegająca na doprecyzowaniu celów zarządzania bezpieczeństwem informacji w Spółce. Uzupełniono podstawę prawną
9	§ 5	10/2022-03-22	Zmiana polegająca na doprecyzowaniu istoty informacji w Spółce