WYCIĄG

POLITYKA BEZPIECZEŃSTWA INFORMACJI INSTYTUTU KOLEJNICTWA

Zatwierdzam do stosowania.
Dyrektor
Instytutu Kolejnictwa
dr inż. Andrzej Żurkowski

01.09.2014

podpis, data

Warszawa, 12 sierpnia 2014 rok

Spis treści

1. CEL PROCEDURY 3
2. PRZEDMOT PROCEDURY 3
3. ZAKRES STOSOWANIA PROCEDURY 3
4. ODPOWIEDZIALNOŚĆ 4
5. DEFINICJE I OZNACZENIA 4
6. OPIS POSTĘPOWANIA 8
   6.1. Zgodność z przepisami prawa i standardami 8
   6.2. Budowa systemu bezpieczeństwa informacji 9
   6.3. Organizacja bezpieczeństwa informacji 9
   6.4. Klasyfikacja informacji 10
   6.5. Zasoby podlegające ochronie 11
   6.6. Bezpieczeństwo osobowe 12
   6.7. Bezpieczeństwo fizyczne i środowiskowe 12
   6.8. Bezpieczeństwo teleinformatyczne 12
   6.9. Bezpieczeństwo w umowach ze stronami zewnętrznymi (trzecimi) 13
   6.10. Rozwiązywanie problemów związanych z bezpieczeństwem informacji 14
7. DOKUMENTY I ZAPISY 14
8. INFORMACJE DODATKOWE 15
9. Załącznik nr 1. Oświadczenie o zapoznaniu się przedstawicieli podmiotu zewnętrznego z zapisami „Polityki Bezpieczeństwa Informacji Instytutu Kolejnictwa” 16

1. CEL PROCEDURY

Celem niniejszego dokumentu jest określenie działań dotyczących zarządzania bezpieczeństwem informacji w Instytucie Kolejnictwa.

Zarządzanie bezpieczeństwem informacji ma za zadanie zapewnić:

1) ciągłość realizacji zadań statutowych,
2) właściwy poziom poufności, integralności, dostępności informacji, w tym w szczególności prawnie chronionych.

Niniejszy dokument jest dokumentem ramowym, wyznaczającym kierunki i zasady dotyczące zarządzania bezpieczeństwem informacji i uwzględniającym cele statutowe Instytutu Kolejnictwa oraz uregulowania prawne z tego zakresu.

2. PRZEDMIOT PROCEDURY

Przedmiotem niniejszego dokumentu jest określenie ramowych zasad ochrony informacji Instytutu Kolejnictwa, poprzez:

1) klasyfikację informacji,
2) określenie zasad postępowania z informacją,
3) wdrożenie zabezpieczeń w obszarze bezpieczeństwa informacji wynikających z wymagań prawnych,
4) wdrożenie zabezpieczeń wynikających z analizy ryzyka w obszarze bezpieczeństwa informacji,
5) politykę Kierownictwa Instytutu w zakresie zapewnienia bezpieczeństwa zasobom informacyjnym.

3. ZAKRES STOSOWANIA PROCEDURY

1. Zakres obowiązywania niniejszego dokumentu dotyczy:
   1) wszystkich pracowników Instytutu Kolejnictwa, w tym nowo zatrudnionych,
   2) stażystów i praktykantów,
   3) przedstawicieli podmiotów zewnętrznych, realizujący pracę lub wykonujący zadania na rzecz Instytutu Kolejnictwa, lub z nim współpracujących, na podstawie zawartych umów cywilno - prawnych.
2. Wymóg przestrzegania zapisów niniejszego dokumentu jest obowiązkowym zapisem w umowach, o których mowa w ust. 1 pkt 3.
3. System Zarządzania Bezpieczeństwem Informacji w Instytucie Kolejnictwa stanowi część całościowego systemu zarządzania, opartego na podejściu wynikającym z oceny ryzyka prowadzonej działalności statutowej.
4. System Zarządzania Bezpieczeństwem Informacji w Instytucie Kolejnictwa został opracowany, wdrożony i jest utrzymywany dla procesów prowadzonej działalności statutowej w dziedzinie prowadzenia badań naukowych i prac badawczo-rozwojowych w obszarze transportu kolejowego.

4. ODPOWIEDZIALNOŚĆ

1. Odpowiedzialnymi za stosowanie zapisów niniejszego dokumentu są:
   1) wszyscy pracownicy Instytutu Kolejnictwa,
   2) stażyści i praktykanci,
   3) przedstawiciele podmiotów zewnętrznych, realizujący pracę lub wykonujący zadania na rzecz Instytutu Kolejnictwa.
2. Odpowiedzialność za przestrzeganie zapisów niniejszego dokumentu ponoszą kierownicy komórek organizacyjnych Instytutu.
3. Odpowiedzialność za naruszenie zasad ochrony informacji określają obowiązujące przepisy i regulacje wewnętrzne, w tym „Regulamin Pracy Instytutu Kolejnictwa".
4. Każdy pracownik Instytutu Kolejnictwa ma obowiązek zapoznania się z treścią niniejszego dokumentu.
5. Odpowiedzialność cywilną i karną regulują:
   1) kodeks pracy,
   2) kodeks cywilny,
   3) kodeks karny,
   4) ustawa o ochronie danych osobowych,
   5) ustawa o zwalczaniu nieuczciwej konkurencji.

5. DEFINICJE I OZNACZENIA

1. **Administrator Systemów Informatycznych (ASI)** – osoba (lub zespół osób) wyznaczona przez Kierownictwo Instytutu, odpowiedzialna za bezpieczeństwo sieci i systemów informatycznych w Instytucie, odpowiedzialna za przestrzeganie zasad i wymagań przyjętej „Polityki Bezpieczeństwa Informacji Instytutu Kolejnictwa", w szczególności „Polityki Bezpieczeństwa Teleinformatycznego Instytutu Kolejnictwa".
2. **Administrator zabezpieczeń** – osoba odpowiedzialna za wdrożenie, utrzymanie i eksploatację zabezpieczeń.
3. **Aktywa** – wszystko co ma wartość dla Instytutu Kolejnictwa.
4. **Analiza ryzyka** – systematyczne zbieranie i przetwarzanie informacji w celu identyfikacji ryzyka bezpieczeństwa informacji, określania jego wartości i identyfikacji niezbędnych zabezpieczeń.
5. **Analiza zagrożeń** – określenie poziomu zagrożeń z uwzględnieniem wszystkich istotnych czynników mogących mieć wpływ na bezpieczeństwo informacji niejawnych.
6. **Bezpieczeństwo fizyczne i środowiskowe** – zespół odpowiednio dobranych środków organizacyjnych, technicznych (mechanicznych, elektronicznych i budowlanych) oraz ludzkich zapewniających skuteczną ochronę informacji, na poziomie kontroli dostępu fizycznego.

7. **Bezpieczeństwo osobowe** – zespół odpowiednio dobranych środków organizacyjnych i proceduralnych uwzględniających aspekt bezpieczeństwa informacji, stosowanych w zarządzaniu zasobami ludzkimi, w szczególności w przydzielaniu obowiązków i uprawnień pracowników.
8. **Bezpieczeństwo teleinformatyczne** – szeroko pojęta ochrona informacji, w tym w szczególności informacji prawnie chronionych: wytwarzanych, przetwarzanych, przechowywanych i przekazywanych w systemach i sieciach teleinformatycznych.
9. **Ciągłość działania** – strategiczna i taktyczna zdolność organizacji do zaplanowania i reakcji na incydent oraz zakłócenia działania, tak by móc kontynuować działania biznesowe i/lub statutowe na możliwym do przyjęcia wcześniej określonym poziomie.
10. **Dane osobowe** – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej.
11. **Dokument** – każda utrwalona informacja, w szczególności na piśmie, mikrofilmach, negatywach i fotografiach, nośnikach do zapisów informacji w postaci cyfrowej i na taśmach elekromagnetycznych, także w formie mapy, wykresu, rysunku, obrazu, grafiki, fotografii, broszury, książki, kopii, odpisu, wypisu, wyciągu i tłumaczenia dokumentu, zbędnego lub wadliwego wydruku, odbitki, kliszy, matrycy i dysku optycznego, kalki, taśmy atramentowej, jak również informacja utrwalona na elektronicznych nośnikach danych.
12. **Dokumentacja bezpieczeństwa systemu teleinformatycznego** – dokument szczególnych wymagań bezpieczeństwa oraz dokument procedur bezpiecznej eksploatacji danego systemu lub sieci teleinformatycznej, sporządzone zgodnie z zasadami określonymi w ustawie o ochronie informacji niejawnych.
13. **Dokumentacja Polityki Bezpieczeństwa Danych Osobowych** – kompletny zbiór dokumentów zawierający aktualizowane i uzupełniane na bieżąco zasady przetwarzania danych osobowych w Instytucie Kolejnictwa.
14. **Dostępność** – funkcja bezpieczeństwa zapewniająca, że informacja jest osiągalna i możliwa do wykorzystania na żądanie, w założonym czasie, przez autoryzowany podmiot.
15. **Działania korygujące** – działanie podjęte w celu wyeliminowania przyczyn wykrytej niezgodności.
16. **Działania zapobiegawcze** – działania podjęte w celu wyeliminowania przyczyn potencjalnej niezgodności lub innej niepożądanej sytuacji.
17. **Gestor aktywu** – osoba, z grona kadry zarządzającej, która ze względu na zajmowane stanowisko, przydział zadań i odpowiedzialności, zarządza bezpieczeństwem głównych elementów składowych danej grupy aktywów. Gestorem aktywu może zostać właściciel aktywów lub administrator zabezpieczeń tych aktywów.
18. **Gestor systemu** – osoba z kadry kierowniczej Instytutu Kolejnictwa, decydująca o zakresie przetwarzania danych w systemie, przy czym ten zakres nie może „wychodzić” poza zakres przetwarzania danych w zbiorze.

19. **Gestor zbioru (części zbioru)** – osoba z kadry kierowniczej Instytutu Kolejnictwa, decydująca o celach i zakresie przetwarzania danych w zbiorze (w części zbioru).
20. **Grupa aktywów** – zbiór aktywów podobnych pod kątem zawartości informacyjnej i jej wartości dla organizacji, które są podatne na podobne ryzyko wystąpienia zagrożeń i w podobny sposób mogą być przed tym ryzykiem zabezpieczane. Każda grupa aktywów ma swojego opiekuna odpowiedzialnego za koordynację bezpieczeństwa aktywów wchodzących w zakres danej grupy.
21. **Identyfikacja zagrożeń** – proces polegający na określeniu, co może się zdarzyć, powodując utratę bezpieczeństwa informacji, a także na sporządzeniu i aktualizacji katalogu zagrożeń.
22. **Incydent bezpieczeństwa informacji** – pojedyncze zdarzenie lub seria niepożądanych lub niespodziewanych zdarzeń związanych z bezpieczeństwem informacji, które stwarzają znaczne prawdopodobieństwo zakłócenia działań biznesowych i/lub statutowych i zagrażają bezpieczeństwu informacji.
23. **Informacja niejawna** – informacja, której nieuprawnione ujawnienie spowodowałoby lub mogłoby spowodować szkody dla Rzeczypospolitej Polskiej albo byłoby z punktu widzenia jej interesów niekorzystne, także w trakcie ich opracowywania oraz niezależnie od formy i sposobu ich wyrażania.
24. **Informacje publicznie** – informacje podane do publicznej wiadomości na mocy zapisów zawartych w dokumentach, zapisów zawartych w innych uregulowaniach wewnętrznych Instytutu Kolejnictwa, obowiązującej ustawy o dostępie do informacji publicznej lub innych przepisów prawa.
25. **Informacje wewnętrzne** – informacje dotyczące działalności Instytutu Kolejnictwa przeznaczone wyłącznie do użytku wewnętrznego.
26. **Integralność** – funkcja bezpieczeństwa polegająca na tym, że dane nie zostały zmienione, dodane lub usunięte w nieautoryzowany sposób.
27. **Inspektor Ochrony Danych (IOD)** – pracownik Instytutu Kolejnictwa wyznaczony przez administratora danych (Kierownictwo Instytutu), odpowiedzialny za nadzór i kontrolę ochrony informacji oraz danych osobowych przetwarzanych w Instytucie, podległy bezpośrednio administratorowi danych.
28. **Nośnik informatyczny** – urządzenie służące do zapisu i przechowywania informacji w postaci cyfrowej (np. dysk twardy, dyskietka, dysk optyczny, taśma magnetyczna, pendrive, karta pamięci itp.).
29. **Ochrona fizyczna** – system mający na celu uniemożliwienie osobom nieupoważnionym dostępu do informacji.
30. **Pełnomocnik ds. ochrony informacji niejawnych** – pracownik, podległy bezpośrednio Dyrektorowi Instytutu Kolejnictwa, spełniający wymagania określone w art. 14 ust. 3 ustawy o ochronie informacji niejawnych, który odpowiada za zapewnienie przestrzegania przepisów o ochronie informacji niejawnych.

31. **Poufność** – funkcja bezpieczeństwa wskazująca obszar, w którym dane nie powinny być udostępniane lub ujawniane nieuprawnionym osobom, procesom lub innym podmiotom.
32. **Ryzyko** – wartościowe ujęcie prawdopodobnego wykorzystania podatności aktywu lub grupy aktywów przez określone zagrożenie, aby spowodować utratę tych aktywów lub stratę wpływającą na zdolność organizacji do osiągnięcia zakładanych celów biznesowych i /lub statutowych.
33. **Sieć teleinformatyczna** – organizacyjne i techniczne połączenie systemów teleinformatycznych wraz z łączącymi je urządzeniami i liniami telekomunikacyjnymi.
34. **System informatyczny** – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych (zwany zamiennie systemem teleinformatycznym).
35. **System Zarządzania Bezpieczeństwem Informacji** – część całościowego systemu zarządzania, oparta na podejściu wynikającym z analizy ryzyka biznesowego i/lub statutowego w obszarze bezpieczeństwa informacji.
36. **Umowa o zachowaniu poufności** – pisemne porozumienie się dwóch lub więcej stron w celu ustalenia wzajemnych praw i obowiązków związanych z zachowaniem poufności informacji przekazywanych w związku z nawiązanymi rozmowami, negocjacjami oraz z realizacją umowy właściwej, zawierane w interesie jednego lub więcej podmiotów.
37. **Umowa właściwa** – pisemne (lub ustne) porozumienie się dwóch lub więcej stron w celu ustalenia wzajemnych praw i obowiązków (np. wykonanie określonej usługi, realizacja danego projektu lub przedsięwzięcia, sprzedaż produktu, towaru itp.).
38. **Zabezpieczenie** – rozwiązanie techniczne i/lub organizacyjne minimalizujące ryzyko.
39. **Zabezpieczenie danych w systemie informatycznym** – wdrożenie i eksploatacja stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem.
40. **Zagrożenie** – niepożądana sytuacja, która może niekorzystnie wpłynąć na prawidłowość przetwarzania lub bezpieczeństwo informacji, powodując negatywne skutki dla Instytutu Kolejnictwa. Zagrożenie może odnosić się bezpośrednio do informacji lub wpływać na bezpieczeństwo informacji poprzez inne aktywa uczestniczące w procesie przetwarzania tej informacji.
41. **Zespół ds. Bezpieczeństwa** – organ doradczy kierownictwa Instytutu Kolejnictwa w sprawach związanych z bezpieczeństwem informacji.
42. **Zobowiązanie do zachowania poufności** – część umowy lub jej załącznik zawierający zobowiązania dotyczące ochrony informacji, przeznaczony do podpisania przez pracowników realizujących umowę.

6. OPIS POSTĘPOWANIA

6.1. Zgodność z przepisami prawa i standardami

Niniejszy dokument oraz wynikające z niego uregulowania regulujące obszar bezpieczeństwa informacji są zgodne z obowiązującym prawem, międzynarodowymi standardami w zakresie zarządzania bezpieczeństwem informacji oraz tzw. „dobrymi praktykami" z tego zakresu, tj.:

1) ustawą z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (t.j. Dz. U. z 2019 r.., poz. 742),
2) 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. U. UE L z 4 maja 2016 r., Nr 119),
3) ustawą z dnia 10 maja 2018 r. o ochronie danych osobowych (t.j. Dz. U. z 2019 r., poz. 1781),
4) ustawą z dnia 16 kwietnia 1993 r. o zwalczaniu nieuczciwej konkurencji (t.j. Dz. U. z 2019 r., poz. 1010 z późn. zm.),
5) ustawą z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (t.j. Dz. U. z 2019 r., poz. 1231 z późn. zm.),
6) ustawą z dnia 30 czerwca 2000 r. Prawo własności przemysłowej (t.j. Dz. U. z 2020 r., poz. 286 z późn. zm.),
7) ustawą z dnia 27 lipca 2001 r. o ochronie baz danych (t.j. Dz. U. z 2019 r., poz. 2134 z późn. zm.),
8) ustawą z dnia 29 września 1994 r. o rachunkowości (t.j. Dz. U. z 2019 r., poz. 351 z późn. zm.),
9) ustawą z dnia 6 września 2001 r. o dostępie do informacji publicznej (t.j. Dz. U. z 2019 r., poz. 1429 z późn. zm.),
10) ustawą z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów (t.j. Dz. U. z 2020 r., poz. 1076 z późn. zm.),
11) ustawą z dnia 29 stycznia 2004 r. Prawo zamówień publicznych (t.j. Dz. U. z 2019 r., poz. 1843 z późn. zm.),
12) ustawą z dnia 29 czerwca 1995 r. o statystyce publicznej (t.j. Dz. U. z 2020 r., poz.443 z późn. zm.),
13) ustawą z dnia 23 kwietnia 1964 r. Kodeks cywilny (t.j. Dz. U. z 2020 r., poz. 1740),
14) ustawą z dnia 26 czerwca 1974 r. Kodeks pracy (t.j. Dz. U. z 2020 r., poz. 1320),
15) ustawą z dnia 6 czerwca 1997 r. Kodeks karny (t.j. Dz. U. z 2020 r., poz. 1444 z późn. zm.),

16) ustawą z dnia 6 czerwca 1997 r. Kodeks postępowania karnego (t.j. Dz. U. z 2020 r., poz. 30 z późn. zm.),
17) przepisami wykonawczymi wydanymi na podstawie w/w ustaw,
18) normą PN-ISO/IEC 27001:2007 – „Technika informatyczna – Techniki bezpieczeństwa - Systemy zarządzania bezpieczeństwem informacji – Wymagania".

6.2. Budowa systemu bezpieczeństwa informacji

1. Efektywność systemu ochrony informacji w Instytucie Kolejnictwa zapewnia jednoczesne stosowanie odpowiednio dobranych środków:
   1) bezpieczeństwa fizycznego i środowiskowego,
   2) bezpieczeństwa osobowego,
   3) bezpieczeństwa organizacyjnego,
   4) bezpieczeństwa teleinformatycznego.
2. Zarządzanie bezpieczeństwem informacji w Instytucie Kolejnictwa jest procesem ciągłym, wymagającym podejścia systemowego, co jest spowodowane szybkim tempem rozwoju w dziedzinie technologii przetwarzania informacji oraz pojawiania się nowych zagrożeń.
3. Dokumentacja obszaru zarządzania bezpieczeństwem informacji podlega regularnym przeglądom oraz aktualizacji w miarę pojawiania się istotnych zmian dotyczących chronionych zasobów, zmiany obowiązującego prawa, powstania nowych zagrożeń, istotnych zmian związanych z informatyzacją Instytutu Kolejnictwa lub zmianą warunków i potrzeb przetwarzania informacji.

6.3. Organizacja bezpieczeństwa informacji

1. Odpowiedzialność za bezpieczeństwo informacji w Instytucie Kolejnictwa ponoszą wszyscy pracownicy zgodnie z posiadanym zakresem obowiązków służbowych.
2. Kierownictwo Instytutu Kolejnictwa odpowiedzialne jest za zapewnienie zasobów niezbędnych dla opracowania, wdrożenia, funkcjonowania, utrzymania i doskonalenia systemu zarządzania bezpieczeństwem informacji oraz poszczególnych zabezpieczeń.
3. Kierownictwo Instytutu Kolejnictwa wydaje zgodę na użytkowanie urządzeń służących do przetwarzania informacji i zabezpieczeń rekomendowanych przez Zespół ds. Bezpieczeństwa.
4. Kierownictwo Instytutu Kolejnictwa decyduje o współpracy w zakresie bezpieczeństwa z innymi podmiotami i organizacjami.
5. Kierownictwo Instytutu Kolejnictwa wyraża zgodę na udostępnienie podmiotom (stronom) trzecim informacji stanowiących tajemnicę Instytutu Kolejnictwa.

6. Inspektor Ochrony Danych odpowiedzialny jest za wdrożenie i koordynację działań zapewniających bezpieczeństwo informacji oraz związanych z nim polityk i procedur.
7. Zespół ds. Bezpieczeństwa jest organem doradczym w zakresie zagadnień związanych z bezpieczeństwem informacji.
8. Zespół ds. Bezpieczeństwa tworzą:
   1) Inspektor Ochrony Danych,
   2) Pełnomocnik ds. ochrony informacji niejawnych,
   3) Administrator Systemów Informatycznych,
   4) Gestor aktywu podlegającego ochronie.
9. Gestor aktywu odpowiada za bieżące nadzorowanie oraz zarządzanie aktywem.
10. Administrator zabezpieczeń odpowiada za realizację i nadzór nad technicznymi aspektami aktywu w ścisłej kooperacji z Gestorem aktywu.

6.4. Klasyfikacja informacji

1. Niniejszy dokument wprowadza podział informacji przetwarzanych w Instytucie Kolejnictwa na grupy informacji.
2. Podstawą podziału, o którym mowa w ust. 1 jest:
   1) obowiązujące prawo,
   2) wartość i ważność informacji,
   3) wymagania wewnętrzne i statutowe Instytutu Kolejnictwa.
3. W Instytucie Kolejnictwa obowiązuje następująca klasyfikacja informacji:
   1) informacje niejawne – w rozumieniu ustawy o ochronie informacji niejawnych,
   2) dane osobowe – w rozumieniu ustawy o ochronie danych osobowych,
   3) „tajemnica Instytutu Kolejnictwa” – w rozumieniu ustawy o zwalczaniu nieuczciwej konkurencji,
   4) informacje wewnętrzne (jawne) – nie wchodzące w zakres informacji, o których mowa w pkt 1 – 3 powyżej,
   5) informacje publiczne – w rozumieniu ustawy o dostępie do informacji publicznej.
4. Za właściwe sklasyfikowanie informacji odpowiada jej twórca (referent) oraz jego bezpośredni zwierzchnik służbowy.
5. Przy klasyfikacji informacji przyjmuje i stosuje się następujące zasady i procedury:
   1) ***informacja niejawna*** – w rozumieniu ustawy o ochronie informacji niejawnych – należy postępować zgodnie z:
      a) „Polityką Bezpieczeństwa Informacji Niejawnych w Instytucie Kolejnictwa” – SZBI_PBIN,
      b) „Planem ochrony informacji niejawnych Instytutu Kolejnictwa” – SZBI_PBIN_PO,

c) „Instrukcją dotyczącą sposobu i trybu przetwarzania informacji niejawnych o klauzuli „zastrzeżone" w Instytucie Kolejnictwa oraz zakres i warunki stosowania środków bezpieczeństwa fizycznego w celu ich ochrony" – SZBI_PBIN_IZ,

d) Dokumentacją bezpieczeństwa systemu teleinformatycznego akredytowanego do przetwarzania informacji niejawnych – w przypadku przetwarzania informacji niejawnych w systemie informatycznym,

2) ***dane osobowe*** – w rozumieniu ustawy o ochronie danych osobowych – należy postępować zgodnie z:
   a) „Polityką Bezpieczeństwa Danych Osobowych Instytutu Kolejnictwa" – SZBI_PBDO,
   b) „Instrukcją zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Instytucie Kolejnictwa" – SZBI_IZDO – w przypadku przetwarzania tych danych w systemach informatycznych,
3) ***„Tajemnica Instytutu Kolejnictwa"*** – w rozumieniu ustawy o zwalczaniu nieuczciwej konkurencji – należy postępować zgodnie z „Polityką Bezpieczeństwa Tajemnicy Instytutu Kolejnictwa" – SZBI_PBTI, uwzględniając „Wykaz rodzajów informacji stanowiących tajemnicę Instytutu Kolejnictwa",
4) jeśli informacja nie wchodzi w zakres, o którym mowa w pkt 1 – 3 powyżej, należy postępować z nią zgodnie z zapisami „Instrukcji Kancelaryjnej Instytutu Kolejnictwa".
5) jeśli informacja jest przeznaczona do podania do publicznej wiadomości na mocy zapisów zawartych w dokumencie, wewnętrznych uregulowaniach Instytutu Kolejnictwa, ustawy o dostępie do informacji publicznej, innych przepisów prawa (np. ustawy o rachunkowości, ustawy o statystyce publicznej, itp.), należy postępować z nią zgodnie z „Polityką Bezpieczeństwa Informacji Publicznych Instytutu Kolejnictwa" – SZBI_PBIP, z uwzględnieniem zapisów „Instrukcji Kancelaryjnej Instytutu Kolejnictwa".

6.5. Zasoby podlegające ochronie

Podział aktywów na grupy podlegające ochronie w Instytucie Kolejnictwa:

1) Ludzie,
2) Lokalizacje,
3) Systemy teleinformatyczne,
4) Sieci teleinformatyczne,
5) Infrastruktura,
6) Nośniki danych,
7) Urządzenia mobilne,
8) Urządzenia stacjonarne,
9) Informacje.

6.6. Bezpieczeństwo osobowe

1. Celem postępowania jest ograniczenie ryzyka błędu ludzkiego, kradzieży, nadużycia lub niewłaściwego użytkowania zasobów.
2. Skuteczna realizacja postawionego celu możliwa jest dzięki ustanowionym praktykom i podziałowi odpowiedzialności związanemu z weryfikacją kandydatów do pracy podczas naboru, zasadom zatrudniania pracowników, zawieraniem umów o zakazie konkurencji, zasadą rozliczania pracowników oraz ustalonym procedurom rozwiązywania umów o pracę.
3. Szczegółowe wymagania dotyczące bezpieczeństwa osobowego określone są w dokumentach, o których mowa w punkcie 6.4. powyżej.
4. Wymagania dotyczące bezpieczeństwa osobowego w zakresie dostępu do systemów i sieci teleinformatycznych zdefiniowane są w „Polityce Bezpieczeństwa Teleinformatycznego Instytutu Kolejnictwa" – SZBI_PBIT oraz dokumentach szczegółowych właściwych dla danego systemu lub sieci teleinformatycznej.

6.7. Bezpieczeństwo fizyczne i środowiskowe

1. Celem postępowania jest zapewnienie bezpieczeństwa informacji przed dostępem osób niepowołanych, uszkodzeniem i utratą zasobów lub innymi zakłóceniami w obiektach Instytutu Kolejnictwa.
2. W przypadku informacji i danych od Klientów najważniejsze jest zapewnienie podstawowych atrybutów bezpieczeństwa tj. poufności, dostępności i integralności informacji.
3. Skuteczna realizacja postawionego celu możliwa jest dzięki ustanowionym praktykom i podziałowi odpowiedzialności związanemu z wyznaczeniem stref ochronnych, zasadami pracy oraz administrowaniem prawami dostępu.
4. Krytyczne systemy techniczne i teleinformatyczne wyposażone są w systemy podtrzymujące zasilanie.
5. Wymagania bezpieczeństwa fizycznego i środowiskowego określają odrębne uregulowania, w tym w szczególności:
   1) instrukcje ochrony fizycznej,
   2) instrukcje ruchu osobowego i materiałowego,
   3) plan ochrony informacji niejawnych.

6.8. Bezpieczeństwo teleinformatyczne

1. Bezpieczeństwo informacji przetwarzanej w systemach lub sieciach teleinformatycznych ma na celu zapewnienie jej ochrony przed nieuprawnionym dostępem, ujawnieniem, losowym lub nieuprawnionym zniszczeniem lub modyfikacją, a także przed nieuzasadnioną odmową lub opóźnieniem jej dostarczenia.

2. Celem postępowania jest zapewnienie poufności, integralności i dostępności przetwarzanej przez systemy teleinformatyczne informacji.
3. Skuteczna realizacja postawionego celu, o którym mowa w ust. 2, możliwa jest dzięki:
   1) kompetencjom i świadomości pracowników,
   2) umowom podpisanym z firmami administrującymi zasobami teleinformatycznymi i wspomagającymi pracę Instytutu,
   3) opracowanym zasadom konserwacji urządzeń w celu zapewnienia ich ciągłości działania,
   4) kontrolowaniu wprowadzania wszelkich zmian do infrastruktury teleinformatycznej,
   5) testowaniu na oddzielnych urządzeniach lub w oddzielnych środowiskach bezpieczeństwa systemów teleinformatycznych,
   6) nadzorowaniu usług dostarczanych przez strony trzecie,
   7) wdrożeniu zabezpieczeń chroniących przed oprogramowaniem szkodliwym (złośliwym),
   8) systematycznemu tworzeniu i testowaniu kopii bezpieczeństwa,
   9) przestrzeganiu opracowanych zasad postępowania z nośnikami,
   10) bieżącemu monitorowaniu aktywów informacyjnych, w tym informatycznych, pod kątem wcześniejszego wykrycia wszelkich niebezpieczeństw mogących zagrozić bezpieczeństwu systemów.
4. Bezpieczeństwo teleinformatyczne zapewnia się poprzez wdrożenie systemu zarządzania bezpieczeństwem teleinformatycznym wynikającym z „Polityki Bezpieczeństwa Teleinformatycznego Instytutu Kolejnictwa” – SZBI_PBIT i szczegółowych procedur w tym zakresie.
5. Instytut Kolejnictwa monitoruje poziom incydentów w systemach teleinformatycznych i posiada mechanizmy reagowania w przypadkach ich wystąpienia.

6.9. Bezpieczeństwo w umowach ze stronami zewnętrznymi (trzecimi)

1. Współpraca Instytutu Kolejnictwa z innymi podmiotami oparta jest na umowach cywilno – prawnych.
2. Zawierając umowy należy mieć na uwadze, żeby obejmowały one deklarację o zachowaniu poufności: zobowiązanie lub umowę o zachowaniu poufności.
3. Podmiot zewnętrzny ubiegający się o zawarcie umowy związanej z dostępem do informacji będących w gestii Instytutu Kolejnictwa ma obowiązek zapoznania się z niniejszym dokumentem i potwierdzeniem tego faktu, poprzez złożenie oświadczenia, zgodnie ze wzorem stanowiącym załącznik do niniejszego dokumentu.

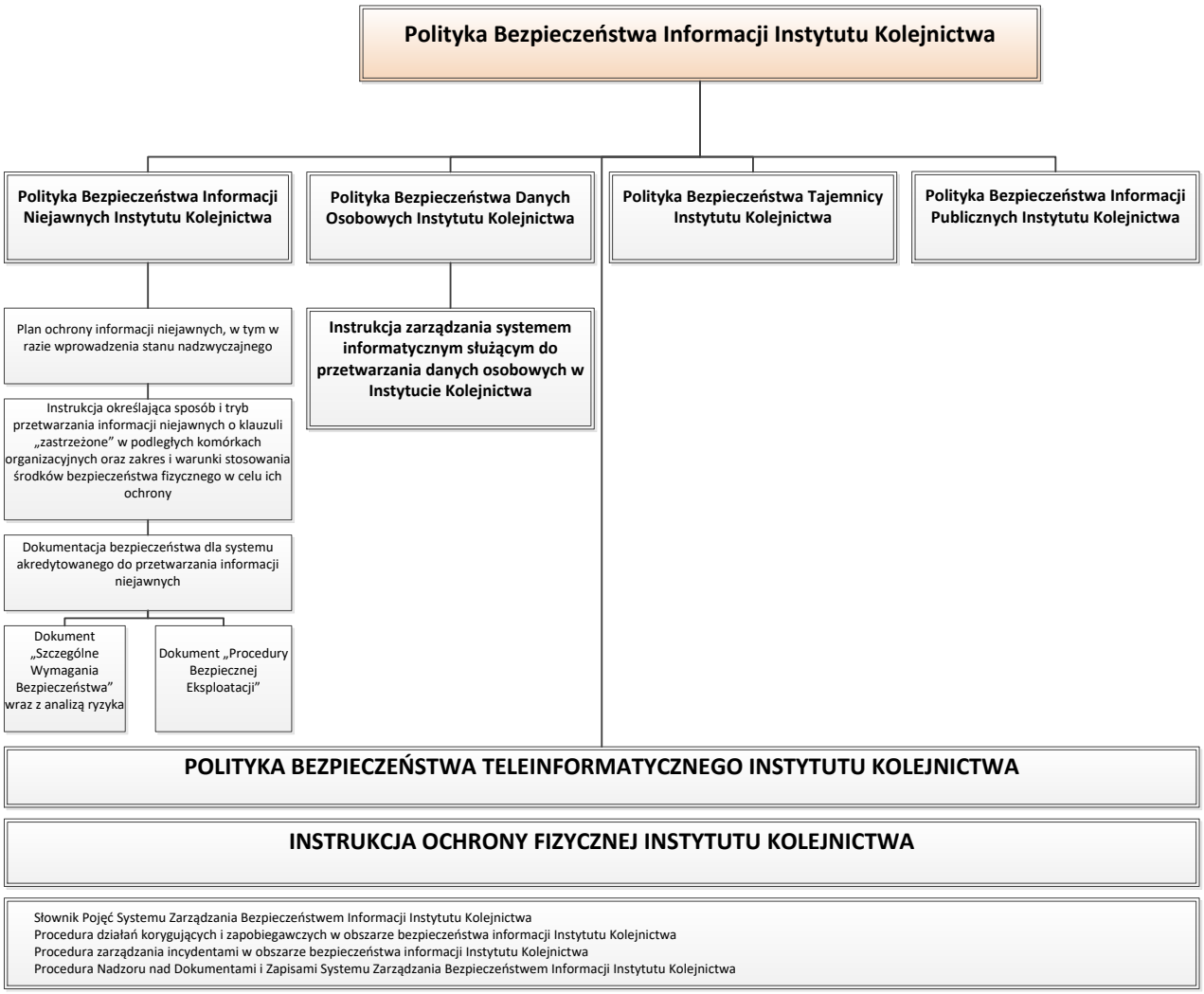
4. W zawieranej umowie ze stroną trzecią należy określić:
   1) wymagania dotyczące ochrony informacji, które zostaną przekazane stronie trzeciej w związku z realizacją umowy,
   2) skutki oraz zakres odpowiedzialności strony trzeciej z tytułu nieprzestrzegania wymagań związanych z ochroną informacji.
5. Każda informacja udostępniana stronom trzecim (zewnętrznym) podlega ochronie. Przed udostępnieniem/wymianą informacji każdy pracownik Instytutu Kolejnictwa jest odpowiedzialny za upewnienie się, że może informacje przekazać. W przypadku wątpliwości o przekazaniu informacji decyduje bezpośredni zwierzchnik służbowy.
6. Zapisy, o których mowa w ust. 4 powyżej muszą uwzględniać wymagania określone w dokumentach, o których mowa punkcie 6.4. niniejszej procedury.

6.10. Rozwiązywanie problemów związanych z bezpieczeństwem informacji

1. Za rozwiązywanie sytuacji związanej z bezpieczeństwem informacji w Instytucie Kolejnictwa odpowiada Zespól ds. bezpieczeństwa.
2. Zespół, o którym mowa w ust. 1, ma obowiązek:
   1) przeprowadzenia analizy zagrożeń oraz metod zarządzania elementami ochrony przed tymi zagrożeniami,
   2) opracowania podstawowych procedur awaryjnych, w których określa się zasady postępowania na wypadek wystąpienia sytuacji mającej związek z bezpieczeństwem informacji, w celu:
      a) zachowania ciągłości działania,
      b) zapewnienia bezpieczeństwa informacji,
      c) przywrócenia w możliwie najkrótszym czasie stanu sprzed wystąpienia problemu.
3. Procedury awaryjne muszą zawierać instrukcje postępowania, z wyszczególnieniem zakresu obowiązków i ponoszonej odpowiedzialności przez pracowników Instytutu Kolejnictwa.

7. DOKUMENTY I ZAPISY

1. Z niniejszego dokumentu wynikają dokumenty szczegółowe tj.
   1) polityki bezpieczeństwa poszczególnych grup informacji,
   2) polityka bezpieczeństwa teleinformatycznego,
   3) instrukcje, procedury i zasady postępowania.
2. Mapa dokumentów i uregulowań w zakresie ochrony zasobów informacyjnych Instytutu Kolejnictwa została przedstawiona poniżej.



8. INFORMACJE DODATKOWE

W zakresie wszelkich spraw związanych z bezpieczeństwem informacji, nieuregulowanych w niniejszym dokumencie oraz innych uregulowaniach wewnętrznych Instytutu Kolejnictwa, obowiązują przepisy prawne.

Załącznik nr 1. Oświadczenie o zapoznaniu się przedstawicieli podmiotu zewnętrznego z zapisami „Polityki Bezpieczeństwa Informacji Instytutu Kolejnictwa"

IK INSTYTUT KOLEJNICTWA

…… ……

(imię i nazwisko) *(miejscowość i data)*

……

(nazwa firmy, instytucji)

……

(adres siedziby)

O Ś W I A D C Z E N I E

1. Niniejszym oświadczam, że zapoznałem (-łam)* się z dokumentem **„Polityka Bezpieczeństwa Informacji Instytutu Kolejnictwa" – SZBI_PBI**, w związku z realizacją umowy*/zlecenia*/kontraktu* Nr …… z dnia ….-….-20…. r.
2. Oświadczenie stanowi integralną część umowy*/zlecenia*/kontraktu* określonego w punkcie 1 powyżej.

……..…..

podpis składającego oświadczenie

** niewłaściwe skreślić*