Załącznik nr 2 do zarządzenia nr 26/2018
Dyrektora Narodowy Instytut Geriatrii, Reumatologii i Rehabilitacji
im. prof. dr hab. Eleonory Reicher
z dnia 7 listopada 2018 r.

ZATWIERDZIŁ:
Dyrektor Narodowego Instytutu Geriatrii,
Reumatologii i Rehabilitacji im. prof. dr hab. med. Eleonory Reicher
Dr n. med. Marek Tombarkiewicz

POLITYKA
BEZPIECZEŃSTWA INFORMACJI

w

Narodowym Instytucie Geriatrii, Reumatologii i Rehabilitacji im. prof. dr hab. Eleonory Reicher

DOKUMENT DO UŻYTKU WEWNĘTRZNEGO

Warszawa, listopad 2018 r.

I. Spis treści

II. Definicje

Pojęcie	Znaczenie
akceptowalny poziom ryzyka	poziom ryzyka, powyżej którego Instytut bez wdrożenia środków zaradczych (zabezpieczeń) nie jest skłonny do ponoszenia kosztów negatywnych skutków z tytułu wystąpienia zagrożenia lub nie jest w stanie tych kosztów ponieść;
analiza ryzyka	proces identyfikacji ryzyka, określania jego wartości i identyfikowanie niezbędnych zabezpieczeń;
ASI	wyznaczona przez administratora informacji osoba, pełniąca funkcję administratora systemu informatycznego, odpowiedzialna za sprawność, konserwację oraz wdrażanie technicznych zabezpieczeń systemu informatycznego;
audyt bezpieczeństwa informacji	czynności mające na celu monitorowanie przestrzegania Polityki bezpieczeństwa informacji;
informacje (dane)	Wszystko co posiada logiczne znaczenie jako przekaz treści i może być praktycznie wykorzystane w procesach, skutkując osiągnięciem celu. Informacja może być przetwarzana na różnych typach nośników (m.in. papierowych, magnetycznych, optycznych) w szczególności w systemach informatycznych;
docelowy poziom ryzyka	docelowy poziom pojedynczego ryzyka, jaki administrator informacji zamierza osiągnąć w odniesieniu do konkretnego ryzyka;
dostępność	właściwość bycia dostępnym i użytecznym na żądanie upoważnionego podmiotu;
działania zaradcze	środki zastosowane lub proponowane przez administratora informacji w celu zaradzenia naruszeniu ochrony danych, w tym środki w celu zminimalizowania ewentualnych negatywnych skutków naruszenia;
hasło	ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym;
identyfikator	ciąg znaków literowych, cyfrowych lub innych znaków identyfikujący osobę upoważnioną do przetwarzania danych w systemie informatycznym;
incydent	naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych przesyłanych, przechowywanych lub w inny sposób przetwarzanych;
Instytut	Narodowy Instytut Geriatrii, Reumatologii i Rehabilitacji im. prof. dr hab. Eleonory Reicher, adres: ul. Spartańska 1, 02-637 Warszawa;
integralność	zasada dotycząca przetwarzania danych zapewniająca, że dane nie zostały zmienione, dodane lub usunięte w nieautoryzowany sposób;
istotność ryzyka	iloczyn prawdopodobieństwa i wpływu ryzyka określający potencjalny skumulowany poziom wpływu ryzyka na osiąganie przez administratora informacji zamierzonych celów;
mapa ryzyka	graficzne zestawienie ryzyka z punktu widzenia ich istotności, lub innych kryteriów;
ocena ryzyka	proces porównywania ryzyka z założonymi kryteriami ryzyka w celu wyznaczenia wagi ryzyka;

osoba uprawniona	osoba upoważniona przez administratora informacji do przetwarzania informacji, nad którą administrator informacji sprawuje bezpośrednią kontrolę w procesie przetwarzania danych realizowanym przez tę osobę;
Polityka	niniejszy dokument, tj. Polityka bezpieczeństwa informacji;
poufność	właściwość zapewniająca, że dane nie są udostępniane nieupoważnionym podmiotom;
pracownik lub współpracownik	osoba zatrudniona przez Instytut na podstawie umowy o pracę oraz osoba świadcząca na rzecz Instytut usługi na podstawie umów cywilnoprawnych, a także praktykanci, wolontariusze, stażyści i studenci;
prawdopodobieństwo	oczekiwana częstość materializacji danego ryzyka;
przetwarzanie	operacja lub zestaw operacji wykonywanych na danych lub zestawach danych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie;
raport zgodności	dokument opracowywany przez ASI po dokonaniu audytu bezpieczeństwa informacji zawierający ogólną ocenę poziomu bezpieczeństwa informacji;
rola	grupa uprawnień przypisanych do stanowiska pracy: np. administracja, lekarz, pielęgniarka, ratownik medyczny, rehabilitant, technik obrazowy, rozliczenia, kadry, płace, księgowość.
rozliczalność	właściwość zapewniająca, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi;
ryzyko	kombinacja prawdopodobieństwa zdarzenia i jego konsekwencji. Ryzyko związane z bezpieczeństwem danych to prawdopodobieństwo, że określone zagrożenie wykorzysta podatność zasobu lub grupy zasobów, aby spowodować straty lub zniszczenie zasobów;
rzetelność	zasada dotycząca przetwarzania informacji zapewniająca merytoryczną poprawność danych poprzez ich zgodność ze stanem faktycznym, kompletność i aktualność;
skutek	efekt materializacji ryzyka;
strona trzecia lub osoba trzecia	osoba fizyczna lub prawna, organ publiczny, jednostka lub podmiot inny niż osoba, której dane dotyczą, administrator, podmiot przetwarzający czy osoby, które – z upoważnienia administratora lub podmiotu przetwarzającego – mogą przetwarzać dane;
system informatyczny	zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;
szacowanie ryzyka	całościowy proces analizy i oceny ryzyka;
tolerancja ryzyka lub akceptowalny poziom ryzyka	poziom i wartość pojedynczego ryzyka jakie kierownictwo jest w stanie podjąć i zaakceptować w odniesieniu do konkretnego ryzyka;
właściciel ryzyka	osoba, która ze względu na zajmowane stanowisko i przydział odpowiedzialności zarządza głównymi czynnikami ryzyka, przypisanego do niej. Właścicielami ryzyka mogą być dyrektorzy, kierownicy,

	samodzielne stanowiska lub pełnomocnicy odpowiadający za zarządzane przez nich procesy przetwarzania danych;
wpływ	potencjalne skutki materializacji ryzyka;
upoważnienie	oświadczenie nadane przez administratora wskazujące z imienia i nazwiska osobę, która ma prawo przetwarzać dane w zakresie wskazanym w tym oświadczeniu, nad którą administrator sprawuje bezpośrednią kontrolę w procesie przetwarzania danych realizowanym przez tę osobę;
uwierzytelnianie	działanie, którego celem jest weryfikacja deklarowanej tożsamości osoby upoważnionej;
zabezpieczenie	środki służące zarządzaniu ryzykiem, łącznie z politykami, procedurami, zaleceniami, praktyką lub strukturami organizacyjnymi, które mogą mieć naturę administracyjną, techniczną, zarządczą lub prawną;
zagrożenie	niepożądane zdarzenie, które powoduje, że ryzyko materializuje się w postaci wymiernej straty poprzez wystawienie informacji na utratę, ujawnienie, zniszczenie lub zmianę;
zarządzanie ryzykiem	skoordynowane działania w celu identyfikacji, minimalizacji lub eliminacji prawdopodobieństwa oraz skutków realizacji zagrożeń;

III. Wstęp

Tworzy się niniejszą Politykę bezpieczeństwa informacji zgodnie z przepisami Rozporządzenia Rady Ministrów z 12 kwietnia 2012 r. w sprawie Krajowym Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań systemów teleinformatycznych.

Głównym celem niniejszej Polityki jest odpowiednie zabezpieczenie przetwarzanych przez Instytut informacji poprzez zachowanie poufności, dostępności, integralności i rozliczalności tych informacji.

Uwzględniając charakter, zakres, kontekst i cele przetwarzania administrator wdrożył odpowiednie środki techniczne i organizacyjne, zapewniające bezpieczeństwo przetwarzanych informacji.

Aby zapewnić bezpieczeństwo informacji będących w zasobach administratora, ich przetwarzanie obywa się z zachowaniem następujących zasad:

- zgodności z prawem;
- rzetelności,
- przejrzystości;
- ograniczoności celu;
- prawidłowości;
- poufności, integralności, dostępności i rozliczalności danych.

Polityka bezpieczeństwa informacji jest na bieżąco aktualizowana wraz ze zmieniającym się otoczeniem, które ma znaczący wpływ na treść niniejszego dokumentu.

Zakres podmiotowy stosowania niniejszej Polityki obejmuje wszystkich pracowników lub współpracowników mających dostęp do informacji.

Informacje chronione niniejszą Polityką przetwarzane są w siedzibie Instytut mieszczącej się przy ul. Spartańskiej 1, 02-637 Warszawa.

IV. Określenie obowiązków

Instytut jest zobowiązany do:

- zapewnienia niezbędnych środków do stworzenia i funkcjonowania systemu bezpieczeństwa informacji;
- wdrożenia niezbędnych środków organizacyjnych i technicznych zapewniających rozliczalność, dostępność, integralność oraz poufność przetwarzanych informacji;
- zapewnienia, by systemy informatyczne wykorzystywane do przetwarzania danych spełniały odpowiednie środki techniczne zapewniające stopień bezpieczeństwa odpowiadający ryzyku naruszenia ich bezpieczeństwa;
- wdrożenia odpowiednich środków organizacyjnych, zapewniających stopień bezpieczeństwa odpowiadający ryzyku naruszenia ich bezpieczeństwa;
- zapewnienia, aby osoby dopuszczone do przetwarzania danych przestrzegały postanowień niniejszej regulacji;
- zapewnienia, by dostęp do danych udzielany był wyłącznie osobom uprawnionym do ich przetwarzania;
- zapewniania, by ASI był właściwie i niezwłocznie włączany we wszystkie sprawy dotyczące bezpieczeństwa informacji;
- zatwierdzania Polityki bezpieczeństwa informacji oraz dokumentów opracowanych na jej podstawie.

Instytut systemu informatycznego jest zobowiązany do:

- informowania administratora informacji oraz pracowników, którzy przetwarzają dane, o obowiązkach spoczywających na nich na podstawie niniejszej Polityki;
- monitorowania przestrzegania postanowień niniejszej polityki poprzez wykonywanie audytów bezpieczeństwa informacji;
- opracowywania, po każdorazowym przeprowadzeniu audytu bezpieczeństwa informacji, raportu dla administratora informacji;
- nadzorowania wdrażania zabezpieczeń będących wynikiem audytu bezpieczeństwa informacji oraz analizy ryzyka;
- podejmowania działań zwiększających świadomość z zakresu bezpieczeństwa informacji, w tym informowanie o zagrożeniach związanych z dostępem do danych;
- reagowania na zgłaszane incydenty związane z naruszeniem bezpieczeństwa informacji, analizowanie ich przyczyn;
- aktualizacji Polityki bezpieczeństwa informacji;
- nadzorowania stosowanych środków technicznych i organizacyjnych zapewniających bezpieczeństw informacji przetwarzanych w systemie informatycznym;
- bieżącego utrzymania systemów informatycznych służących do przetwarzania informacji i ich funkcjonowania, zapewniającego ich poufność, integralność, dostępność i rozliczalność, m.in. poprzez właściwą aktualizację tych systemów;

- zarządzania systemem komunikacji w sieci komputerowej oraz przesyłania danych za pośrednictwem urządzeń teletransmisji w sposób zapewniający bezpieczeństwo wymiany informacji;
- nadzorowania funkcjonowania mechanizmów uwierzytelniania użytkowników w systemie informatycznym oraz kontroli dostępu do danych;
- wykonywania kopii bezpieczeństwa informacji przetwarzanych w sposób elektroniczny;
- okresowego sprawdzania kopii bezpieczeństwa pod kątem ich dalszej przydatności do odtwarzania informacji w przypadku awarii systemu informatycznego;
- prowadzenia depozytu kopii bezpieczeństwa i logów danych;
- przydzielania użytkownikom indywidualnych identyfikatorów i haseł do systemu informatycznego oraz dokonywania ewentualnych modyfikacji uprawnień, a także usuwania kont użytkowników;
- okresowego zmieniania haseł dostępu użytkowników do systemu informatycznego w przypadkach, gdy system informatyczny nie wymusza okresowej zmiany haseł użytkowników;
- prowadzenia bieżącej ewidencji wszystkich użytkowników systemów informatycznych służących do przetwarzania danych (Rejestr identyfikatorów);
- osobistego wykonywania lub sprawowania nadzoru na wykonaniem napraw, konserwacji oraz likwidacji urządzeń, dysków lub innych elektronicznych nośników informacji, zawierających dane;
- uczestniczenia w procesie zakupów aplikacji oraz oprogramowania zatwierdzonego do włączenia do sytemu informatycznego służącego do przetwarzania danych;
- zapewnienia legalności oprogramowania wykorzystywanego w systemie informatycznym służącym do przetwarzania informacji oraz zarządza licencjami do odpowiednich elementów systemu informatycznego;
- zapewnienia właściwej konfiguracji systemów zarządzania hasłami;
- inwentaryzacji sprzętu komputerowego oraz systemów informatycznych;
- bieżącej inwentaryzacji przepływów informacji pomiędzy systemami informatycznymi;

Osoba uprawniona jest zobowiązana do:

- przestrzegania przyjętych u administratora zasad bezpieczeństwa informacji;
- informowania bezpośredniego przełożonego, ASI o incydentach godzących w bezpieczeństwo przetwarzanych informacji;
- dochowywania szczególnej staranności przy przetwarzaniu informacji;
- zachowania w poufności przetwarzanych informacji oraz sposobów ich zabezpieczania;
- uporządkowania swojego stanowiska pracy, wykonania czynności zabezpieczających adekwatnych do zastosowanych rozwiązań technicznych i organizacyjnych, w szczególności: zabezpieczenia komputerów i wszelkich nośników danych, wyłączenia wszystkich urządzeń elektrycznych (niewymagających stałego zasilania), zamknięcia okien i drzwi oraz zdania kluczy po zakończeniu pracy.

V. Odpowiedzialność

Instytut za naruszenie zasad bezpieczeństwa informacji może ponieść odpowiedzialność cywilną lub odpowiedzialność administracyjną.

Osoba uprawniona za naruszenie zasad bezpieczeństwa danych może ponieść odpowiednio odpowiedzialność wskazaną w art. 52 lub 108 kodeksu pracy albo odpowiedzialność kontraktową przewidzianą w art. 471 kodeksu cywilnego. Osoba uprawniona może także ponieść odpowiedzialność karną przewidzianą w art. 266 kodeksu karnego.

Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszej Polityki mogą zostać potraktowane jako ciężkie naruszenie obowiązków pracowniczych. Wobec osoby, która w przypadku wykrycia incydentu lub uzasadnionego podejrzenia powstania incydentu nie podjęła działania określonego w niniejszej Polityce, a w szczególności nie powiadomiła odpowiedniej osoby zgodnie z określonymi zasadami, a także gdy nie udokumentowała takiego przypadku, możne zostać wszczęte postępowanie dyscyplinarne.

Kara dyscyplinarna nałożona na osobę uchylającą się od powiadomienia, o którym mowa powyżej, nie wyklucza odpowiedzialności karnej tej osoby oraz możliwości kierowania wobec takiej osoby roszczeń cywilnych przez administratora o zrekompensowanie poniesionych strat.

VI. Zapewnienie poufności, integralności, dostępności oraz rozliczalności informacji

Instytut zapewnia poufność, integralność, dostępność oraz rozliczalność przetwarzanych danych, poprzez zastosowanie niezbędnych środków organizacyjnych oraz technicznych.

Dobór powyższych środków ma na celu obniżyć poziom ryzyka wystąpienia incydentów, związanych z bezpieczeństwem przetwarzania danych, do poziomu akceptowalnego przez administratora.

Wprowadzenie omawianych środków, zostało poprzedzone przeprowadzeniem analizy kosztów ich wdrożenia w odniesieniu do stopnia bezpieczeństwa przetwarzania danych, jaki administrator zamierza osiągnąć po ich wdrożeniu.

W ramach grupy środków organizacyjnych wprowadza się, w szczególności:

- monitorowanie przestrzegania niniejszej Polityki przez wyznaczonego ASI;
- nadzór środowiska informatycznego przez wyznaczonego ASI;
- uprawnienia do przetwarzania danych, które są wydawane każdemu pracownikowi zgodnie z zakresem obowiązków;
- ewidencję uprawnień do przetwarzania danych;
- oświadczenia o zachowaniu w poufności danych i sposobów zabezpieczenia danych, które są zbierane od osób uprawnionych;
- szkolenia dla osób uprawnionych z zasad bezpiecznego przetwarzania danych;
- zasadę, zgodnie z którą osoby trzecie przebywają w obszarze przetwarzania danych wyłącznie w obecności osoby uprawnionej. Osoby trzecie mogą w wyjątkowych okolicznościach przebywać bez obecności osoby upoważnionej - w obszarze przetwarzania danych - po uprzednim wydaniu na to zgody przez administratora danych.

Ponadto, została określona odpowiedzialność pracownika za działania związane z naruszeniem bezpieczeństwa przetwarzania danych.

W ramach grupy środków technicznych, wprowadza się w szczególności:

- zabezpieczenia techniczne zapewniające poufność przetwarzanych danych:
  - obszar przetwarzania danych jest zabezpieczony przed dostępem osób nieupoważnionych poprzez zastosowanie zamków patentowych lub kart wejściowych;
  - dane przetrzymywane w formie papierowej są przechowywane w zamykanych szafkach, szafach lub szufladach;
  - dostęp do danych w systemie informatycznym jest możliwy wyłącznie po udanym uwierzytelnieniu użytkownika;
  - hasła składają się z 8 znaków (małe, wielkie litery, przynajmniej jedna cyfra lub znak specjalny);
  - zmiana haseł nie rzadziej niż co 90 dni;

- na stacjach roboczych, za pomocą których są przetwarzane dane, zainstalowano oprogramowanie antywirusowe automatycznie ściągające najnowsze sygnatury wirusów;
- monitorowanie działania systemu informatycznego;
- logiczna i fizyczna separacja sieci;
- logiczny dostęp do danych z sieci publicznej ograniczony jest poprzez zastosowanie zapory ogniowej (firewall). Chroni ona wszystkie systemy informatyczne przed nieuprawnionym dostępem i atakami z zewnątrz.

- zabezpieczenia techniczne zapewniające integralność przetwarzanych danych:
  - ochrona przed nieautoryzowanym dostępem;
  - na stacjach roboczych, za pomocą których są przetwarzane dane, zainstalowano oprogramowanie antywirusowe automatycznie ściągające najnowsze sygnatury wirusów;
  - awaryjne podtrzymywanie zasilania serwerów oraz stacji roboczych za pomocą UPS;
  - właściwe okablowanie sieci;
  - cykliczna weryfikacja integralności baz danych poprzez odtwarzanie danych zawartych na kopiach zapasowych.

- zabezpieczenia techniczne zapewniające rozliczalność przetwarzanych danych:
  - dostęp do danych w systemie informatycznym możliwy wyłącznie po udanym uwierzytelnieniu użytkownika;
  - awaryjne podtrzymywanie zasilania serwerów oraz stacji roboczych za pomocą UPS;
  - zapis zdarzeń w systemach informatycznych.

Przetwarzanie danych poza obszarem przetwarzania dopuszczalne jest wyłącznie po spełnieniu poniższych przesłanek:

- zachowanie szczególnej ostrożności podczas transportu, przechowywania i użytkowania nośników zawierających dane;
- stosowanie środków ochrony kryptograficznej wobec przetwarzanych danych;
- zakaz pozostawiania nośników zawierających dane w miejscach powszechnie dostępnych;
- wykorzystywanie nośników wyłącznie w celach służbowych.

Urządzenia, dyski lub inne elektroniczne nośniki informacji, zawierające dane, przeznaczone do:

- likwidacji – pozbawia się wcześniej zapisu tych danych, a w przypadku gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie;
- przekazania podmiotowi nieuprawnionemu do przetwarzania danych – pozbawia się wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie;

- naprawy – pozbawia się wcześniej zapisu tych danych w sposób umożliwiający ich odzyskanie.

VII. Procedura monitorowania sposobu używania sprzętu i oprogramowania

Instytut wyposażył pracownika w sprzęt, w tym sprzęt komputerowy (dalej „Sprzęt) i oprogramowanie komputerowe (dalej „Oprogramowanie") niezbędne do prawidłowego wykonywania powierzonych zadań. Pracownik w trakcie wykonywania tych zadań może mieć dostęp do informacji stanowiących: tajemnicę, tajemnicę przedsiębiorstwa, dane, informacje poufne lub dane, co do których administrator informacji zobowiązał się do ich zabezpieczenia przed nieuprawnionym ujawnieniem. Do niniejszej procedury stosuje się odpowiednio zasady opisane w procedurze monitorowania sposobu używania sprzętu i oprogramowania, stanowiącej integralną część Polityki ochrony danych osobowych.

VIII. Procedura nadawania i odbierania uprawnień

Celem niniejszej procedury jest określenie zasad nadawania uprawnień do przetwarzania danych w systemie informatycznym służącym do przetwarzania danych. Dostęp do systemu informatycznego służącego do przetwarzania danych, użytkownikom nadaje ASI, zgodnie z Polityką ochrony danych osobowych.

VIII. Procedura zabezpieczenia systemu informatycznego

Celem niniejszej procedury jest określenie zabezpieczenia systemu informatycznego przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego oraz wirusami komputerowymi. Do niniejszej procedury stosuje się odpowiednio, zasady opisane w procedurze zabezpieczeń systemu informatycznego stanowiącej integralną część Polityki ochrony danych osobowych.

IX. Procedura tworzenia kopii zapasowych

Celem niniejszej procedury jest określenie zasad tworzenia kopii zapasowych danych przetwarzanych w systemie informatycznym służącym do przetwarzania informacji. Do niniejszej procedury stosuje się odpowiednio zasady opisane w procedurze tworzenia kopii zapasowych, stanowiącej integralną część Polityki ochrony danych osobowych.

X. Procedura przechowywania elektronicznych nośników informacji

Celem niniejszej procedury jest określenie zasad przechowywania elektronicznych nośników informacji takich jak: pendrive, dyskietka, dysk magnetooptyczny, dysk twardy lub komputer przenośny. Do niniejszej procedury stosuje się odpowiednio zasady opisane w procedurze przechowywania elektronicznych nośników informacji, stanowiącej integralną część Polityki ochrony danych osobowych.

XI. Procedura wykonywania przeglądów i konserwacji

Celem niniejszej procedury jest określenie zasad wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych. Do niniejszej procedury stosuje się odpowiednio zasady opisane w procedurze wykonywania przeglądów i konserwacji, stanowiącej integralną część Polityki ochrony danych osobowych.

XII. Procedura zarządzania systemem monitoringu wizyjnego

Celem niniejszej procedury jest określenie zasad korzystania i dostępu do systemu monitoringu wizyjnego rejestrującego obraz na terenie siedziby administratora. Do niniejszej procedury stosuje się odpowiednio zasady opisane w procedurze zarządzania systemem monitoringu wizyjnego, stanowiącej integralną część Polityki ochrony danych osobowych.

XIII. Procedura dostępu fizycznego do pomieszczeń

Celem niniejszej procedury jest określenie zasad pobierania kluczy do pomieszczeń, w których przetwarzane są dane, dla pracowników komórek organizacyjnych pracujących w trybie jednodniowym, jak również do innych pomieszczeń zamykanych na noc. Do niniejszej procedury stosuje się odpowiednio zasady opisane w procedurze dostępu fizycznego do pomieszczeń, stanowiącej integralną część Polityki ochrony danych osobowych.

XIV. Procedura przeprowadzania szkoleń pracowniczych

Celem niniejszej procedury jest zapewnienie realizacji zadań ASI jakim jest informowanie pracowników, którzy przetwarzają dane, o obowiązkach spoczywających na nich , wynikających z niniejszej Polityki.

1. Każda osoba uprawniona do przetwarzania danych, przed dopuszczeniem do pracy, jest poddawana szkoleniu stanowiskowemu, które przeprowadza jego bezpośredni przełożony lub osoba wyznaczona przez bezpośredniego przełożonego.

2. Szkolenie stanowiskowe obejmuje zaznajomienie pracownika z regulacjami wewnętrznymi obowiązującymi u administratora, w tym z niniejszą Polityką, a także omówienie sposobu bezpiecznego postępowania z danymi.

3. ASI z chwilą nadania uprawnień informuje osobę uprawnioną o obowiązkach wynikających z niniejszej Polityki.

4. Instytut zapewnia odpowiednie warunki do przeprowadzenia ewentualnych szkoleń grupowych.

5. Pracownicy potwierdzają swój udział w szkoleniu własnoręcznym podpisem na liście obecności, którą przechowuje komórka właściwa ds. kadr.

XV. Procedura zgłaszania incydentów

Procedura definiuje katalog zagrożeń i incydentów mogących prowadzić do naruszenia bezpieczeństwa danych przetwarzanych przez administratora oraz sposób reagowania na ww. zagrożenia i incydenty. Do niniejszej procedury stosuje się odpowiednio zasady opisane w procedurze zgłaszania incydentów, stanowiącej integralną część Polityki ochrony danych osobowych.

XVI. Procedura zarządzania ryzykiem

Procedura zarządzania ryzykiem to szereg skoordynowanych działań podejmowanych przez dyrekcję Instytut, kierowników poszczególnych komórek organizacyjnych, jak i pozostałych pracowników oraz współpracowników Instytutu, którzy poprzez identyfikację i analizę ryzyka oraz określanie adekwatnych reakcji na ryzyko zwiększają poziom bezpieczeństwa informacji w ramach poszczególnych procesów ich przetwarzania. Do niniejszej procedury stosuje się odpowiednio zasady opisane w procedurze zarządzania ryzykiem, stanowiącej integralną część Polityki ochrony danych osobowych.

XVII. Procedura przeprowadzania audytów bezpieczeństwa informacji

Celem niniejszej procedury jest określenie trybu i zasad monitorowania przez ASI przestrzegania niniejszej Polityki przeprowadzanie audytów bezpieczeństwa informacji. Audyty bezpieczeństwa informacji przeprowadza ASI. Do niniejszej procedury stosuje się odpowiednio zasady opisane w

procedurze przeprowadzania audytów zgodności, stanowiącej integralną część Polityki ochrony danych osobowych.

XVIII. Postanowienia końcowe

1. Polityka bezpieczeństwa informacji jest dokumentem wewnętrznym i osoby, które uzyskały wgląd w jej treść, zobowiązane są do zachowania jej w poufności.

2. Przypadki nieuzasadnionego zaniechania obowiązków określonych w niniejszym dokumencie mogą zostać potraktowane jako ciężkie naruszenie podstawowych obowiązków pracowniczych.

3. W sprawach nieuregulowanych w niniejszej Polityce bezpieczeństwa informacji mają zastosowanie przepisy Rozporządzenia Rady Ministrów z 12 kwietnia 2012 r. w sprawie Krajowym Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań systemów teleinformatycznych.