Załącznik nr 1

do zarządzenia

Wojewody Lubuskiego

z dnia .....

ZATWIERDZAM

.....

..

Polityka
Bezpieczeństwa Informacji

Spis treści

SPIS ZAŁĄCZNIKÓW:

Załącznik Nr 1. Wzór Ewidencji osób uprawnionych do przetwarzania danych osobowych oraz Ewidencji oświadczeń o zachowaniu w tajemnicy danych osobowych osób zatrudnionych przy przetwarzaniu danych osobowych.

Załącznik Nr 2. Wzór upoważnienia do przetwarzania danych osobowych.

Załącznik Nr 3. Wzór oświadczenia.

Załącznik Nr 4. Wzór wykazu zbiorów danych osobowych przetwarzanych w systemie informatycznym.

Załącznik Nr 5. Wzór wykazu serwerów zlokalizowanych w LUW.

Załącznik Nr 6. Wzór struktury zbiorów danych osobowych oraz sposobu przepływu danych.

Załącznik Nr 7. Wzór wykazu systemów informatycznych niepodlegających zasadom bezpieczeństwa LUW.

I. Wstęp

Polityka Bezpieczeństwa Informacji w Lubuskim Urzędzie Wojewódzkim w Gorzowie Wlkp. jest zbiorem zasad i procedur obowiązujących przy zbieraniu, przetwarzaniu i wykorzystywaniu danych osobowych we wszystkich zbiorach administrowanych przez osoby upoważnione do przetwarzania tych danych.

Mając na uwadze zagrożenia bezpieczeństwa danych osobowych, wydaje się niniejszy dokument w celu zagwarantowania, że podejmuje się wszelkie możliwe działania konieczne do ochrony przetwarzanych danych osobowych w przypadku zagrożeń takich jak:

1) sytuacje losowe lub nieprzewidziane oddziaływanie czynników zewnętrznych na zasoby systemu, jak np. pożar, zalanie pomieszczeń, katastrofa budowlana, napad, kradzież, włamanie, działania terrorystyczne;
2) niewłaściwe parametry środowiska, zakłócające pracę urządzeń komputerowych (nadmierna wilgotność lub bardzo wysoka temperatura, oddziaływanie pola elektromagnetycznego i inne);
3) awarie sprzętu lub oprogramowania, które wyraźnie wskazują na umyślne naruszenia ochrony danych, niewłaściwe działanie serwisantów, w tym pozostawienie serwisantów bez nadzoru, a także przyzwolenie na naprawę sprzętu zawierającego dane poza siedzibą administratora danych;
4) podejmowanie pracy z zaniechaniem stosowania procedur ochrony danych, np. praca osoby, która nie jest upoważniona do przetwarzania, próby stosowania nie swojego hasła i identyfikatora przez osoby upoważnione;
5) ataki z internetu;
6) naruszenia zasad i procedur określonych w dokumentacji z zakresu ochrony danych osobowych przez osoby upoważnione do przetwarzania danych osobowych, związane z nieprzestrzeganiem procedur ochrony danych, w tym zwłaszcza:
   - niezgodne z procedurami zakończenie pracy lub opuszczenie stanowiska pracy (nieprawidłowe wyłączenie komputera, niezablokowanie wyświetlenia treści pracy na ekranie komputera przed tymczasowym opuszczeniem stanowiska pracy, pozostawienie po zakończeniu pracy nieschowanych do zamykanych na klucz szaf dokumentów zawierających dane osobowe, niezamknięcie na klucz pokoju po jego opuszczeniu, nieoddanie klucza na portiernię),
   - naruszenie bezpieczeństwa danych przez nieautoryzowane ich przetwarzanie,
   - ujawnienie osobom nieupoważnionym procedur ochrony danych stosowanych u administratora danych,

- ujawnienie osobom nieupoważnionym danych przetwarzanych przez administratora danych, w tym również nieumyślne ujawnienie danych osobom postronnym, przebywającym bez nadzoru lub niedostatecznie nadzorowanym w pomieszczeniach administratora danych,
- niewykonywanie stosownych kopii zapasowych,
- przetwarzanie danych osobowych w celach prywatnych.

II. Postanowienia ogólne

1. Podstawa prawna

Niniejszy dokument jest zgodny z obowiązującymi przepisami, w szczególności z:

- ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926, z późn. zm.),
- ustawą z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. Nr 182, poz. 1228),
- ustawą z dnia 6 września 2001r. o dostępie do informacji publicznej (Dz. U. Nr 112, poz. 1198, z późn. zm.),
- rozporządzeniem Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz.1024),
- rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. poz. 526).

2. Definicje

Ilekroć w polityce bezpieczeństwa jest mowa o:

1) **LUW** - rozumie się przez to Lubuski Urząd Wojewódzki w Gorzowie Wlkp.,
2) **Oddziale Informatyki** – rozumie się przez to Oddział Informatyki w Biurze Logistyki,
3) **administratorze danych** – rozumie się przez to administratora danych Lubuskiego Urzędu Wojewódzkiego – Wojewodę Lubuskiego,
4) **administratorze bezpieczeństwa informacji (ABI)** – rozumie się przez to osobę, której administrator danych powierzył pełnienie obowiązków administratora bezpieczeństwa informacji,
5) **administratorze systemu** – rozumie się przez to osobę wyznaczoną przez Dyrektora Generalnego Lubuskiego Urzędu Wojewódzkiego, zarządzającą

systemami informatycznymi w LUW,

6) **haśle** – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, znany jedynie użytkownikowi,
7) **identyfikatorze** – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym,
8) **integralności danych** – rozumie się przez to właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany,
9) **osobie upoważnionej do przetwarzania danych osobowych** – rozumie się przez to osobę, która upoważniona została na piśmie do przetwarzania danych osobowych przez administratora danych lub osobę wyznaczoną do wydawania odpowiedniego upoważnienia,
10) **poufności danych** – rozumie się przez to właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym podmiotom,
11) **przetwarzającym** – rozumie się przez to podmiot, któremu zostało powierzone przetwarzanie danych osobowych na podstawie umowy zawieranej zgodnie z art. 31 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926, z późn. zm.),
12) **raporcie** – rozumie się przez to przygotowane przez system informatyczny zestawienia zakresu i treści przetwarzanych danych,
13) **rozliczalności** – rozumie się przez to właściwość zapewniającą, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi,
14) **rozporządzeniu** – rozumie się przez to rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024),
15) **sieci publicznej** – rozumie się przez to sieć publiczną w rozumieniu art. 2 pkt 22 ustawy z dnia 21 lipca 2000 r. – Prawo telekomunikacyjne (Dz.U nr 73, poz. 852
ze zm.),
16) **sieci telekomunikacyjnej** – rozumie się przez to sieć telekomunikacyjną w rozumieniu art. 2 pkt 23 ustawy z dnia 21 lipca 2000 r. – Prawo telekomunikacyjne,
17) **serwisancie** – rozumie się przez to firmę lub pracownika firmy zajmującej się

sprzedażą, instalacją, naprawą i konserwacją sprzętu komputerowego,

18) **systemie informatycznym administratora danych** – rozumie się przez to sprzęt komputerowy, oprogramowanie, dane eksploatowane w zespole współpracujących ze sobą urządzeń, programów procedur przetwarzania informacji i narzędzi programowych; w systemie tym pracuje co najmniej jeden komputer centralny i system ten tworzy sieć teleinformatyczną administratora danych,

19) **teletransmisji** – rozumie się przez to przesyłanie informacji za pośrednictwem sieci telekomunikacyjnej,

20) **ustawie** – rozumie się przez to ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U z 2002 r. Nr 101, poz. 926, z późn. zm.),

21) **uwierzytelnianiu** – rozumie się przez to działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu,

22) **użytkowniku** – rozumie się przez to osobę upoważnioną do przetwarzania danych osobowych, której nadano identyfikator i przyznano hasło.

2. Cele Polityki Bezpieczeństwa Informacji

Polityka bezpieczeństwa w LUW ma na celu zabezpieczenie przetwarzanych przez niego danych osobowych, w tym danych przetwarzanych w systemach informatycznych administratora danych i poza nimi, poprzez wykonanie obowiązków wynikających z ustawy i rozporządzenia.

W związku z tym, że w zbiorach administratora danych przetwarzane są między innymi dane wrażliwe, a systemy informatyczne administratora danych posiadają szerokopasmowe połączenie z internetem, niniejsza polityka bezpieczeństwa służy zapewnieniu wysokiego poziomu bezpieczeństwa danych w rozumieniu § 6 rozporządzenia. Niniejszy dokument opisuje niezbędny do uzyskania tego bezpieczeństwa zbiór procedur i zasad dotyczących przetwarzania danych osobowych oraz ich zabezpieczenia.

3. Zakres stosowania

Niniejsza polityka bezpieczeństwa dotyczy zarówno danych osobowych przetwarzanych w sposób tradycyjny w księgach, wykazach i innych zbiorach ewidencyjnych, jak i w systemach informatycznych.

Procedury i zasady określone w niniejszym dokumencie stosuje się do wszystkich osób upoważnionych do przetwarzania danych osobowych, zarówno zatrudnionych, jak i innych, np. stażystów, praktykantów.

III. Organizacja przetwarzania danych osobowych

1. Administrator danych osobowych

Administrator danych osobowych realizuje zadania w zakresie ochrony danych osobowych, w tym zwłaszcza:

1) podejmuje decyzje o celach i środkach przetwarzania danych osobowych z uwzględnieniem przede wszystkim zmian w obowiązującym prawie, organizacji administratora danych oraz technik zabezpieczenia danych osobowych;
2) upoważnia poszczególne osoby do przetwarzania danych osobowych w określonym indywidualnie zakresie, odpowiadającym zakresowi jego obowiązków;
3) wyznacza administratora bezpieczeństwa informacji oraz określa zakres jego zadań i czynności;
4) wyznacza osobę do prowadzenia ewidencji osób upoważnionych do przetwarzania danych osobowych oraz pozostałej dokumentacji z zakresu ochrony danych;
5) zleca Dyrektorowi Biura Logistyki, by we współpracy z administratorem systemu oraz administratorem bezpieczeństwa informacji zapewnił użytkownikom odpowiednie stanowiska pracy umożliwiające bezpieczne przetwarzanie danych;
6) podejmuje odpowiednie działania w przypadku naruszenia lub podejrzenia naruszenia procedur bezpiecznego przetwarzania danych osobowych.

2. Administrator bezpieczeństwa informacji

Administrator bezpieczeństwa informacji realizuje zadania w zakresie nadzoru nad przestrzeganiem zasad ochrony danych osobowych, w tym zwłaszcza:

1) sprawuje nadzór nad wdrożeniem stosownych środków fizycznych, a także organizacyjnych i technicznych – w celu zapewnienia bezpieczeństwa danych,
2) sprawuje nadzór nad funkcjonowaniem systemu zabezpieczeń, w tym także nad prowadzeniem ewidencji z zakresu ochrony danych osobowych,
3) koordynuje wewnętrzne audyty przestrzegania przepisów o ochronie danych osobowych,
4) przygotowuje wnioski zgłoszeń rejestracyjnych i aktualizacyjnych zbiorów danych oraz prowadzi inną korespondencję z Generalnym Inspektorem Ochrony Danych Osobowych,
5) zatwierdza wzory dokumentów dotyczących ochrony danych osobowych, przygotowywane przez komórki organizacyjne administratora danych,
6) prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych (wzór ewidencji - załącznik Nr 1; wzór upoważnienia - załącznik Nr 2),

7) prowadzi ewidencję oświadczeń o zachowaniu w tajemnicy danych osobowych osób zatrudnionych przy przetwarzaniu danych osobowych (wzór ewidencji - załącznik Nr 1; wzór oświadczenia - załącznik Nr 3)
8) prowadzi ewidencję zbiorów danych w systemach informatycznych, w których przetwarzane są dane osobowe (wzór ewidencji - załącznik Nr 4),
9) występuje z wnioskiem do administratora danych o nadanie upoważnienia do przetwarzania danych osobowych,
10) występuje z wnioskiem do administratora systemu o nadanie identyfikatora i przyznanie hasła osobie upoważnionej do przetwarzania danych osobowych,
11) prowadzi oraz aktualizuje dokumentację opisującą sposób przetwarzania danych osobowych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych,
12) podejmuje odpowiednie działania w przypadku naruszenia lub podejrzenia naruszenia systemu informatycznego,
13) przygotowuje materiały szkoleniowe z zakresu ochrony danych osobowych i prowadzi szkolenia osób upoważnianych do przetwarzania danych osobowych.

3. Administrator systemu

Administrator systemu realizuje zadania w zakresie zarządzania i bieżącego nadzoru nad systemem informatycznym administratora danych, w tym zwłaszcza:

1) zarządza systemem informatycznym, w którym przetwarzane są dane osobowe, posługując się hasłem dostępu do wszystkich stacji roboczych z pozycji administratora,
2) przeciwdziała dostępowi osób niepowołanych do systemu informatycznego, w którym przetwarzane są dane osobowe,
3) przydziela, na wniosek osoby do tego upoważnionej, każdemu użytkownikowi identyfikator oraz hasło do systemu informatycznego oraz dokonuje ewentualnych modyfikacji uprawnień, a także usuwa konta użytkowników zgodnie z zasadami określonymi w instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych,
4) nadzoruje działanie mechanizmów uwierzytelniania użytkowników oraz kontroli dostępu do danych osobowych,
5) podejmuje działania w zakresie ustalania i kontroli identyfikatorów dostępu do systemu informatycznego,
6) wyrejestrowuje użytkowników na polecenie administratora danych lub na wniosek kierownika Oddziału Kadr i Szkolenia w Biurze Organizacyjnym i Kadr,

7) w sytuacji stwierdzenia naruszenia zabezpieczeń systemu informatycznego informuje ABI o naruszeniu i współdziała z nim przy usuwaniu skutków naruszenia,
8) prowadzi szczegółową dokumentację naruszeń bezpieczeństwa danych osobowych przetwarzanych w systemie informatycznym,
9) sprawuje nadzór nad wykonywaniem napraw, konserwacją oraz likwidacją urządzeń komputerowych, na których zapisane są dane osobowe, nad wykonywaniem kopii zapasowych, ich przechowywaniem oraz okresowym sprawdzaniem pod kątem ich dalszej przydatności do odtwarzania danych w przypadku awarii systemu informatycznego,
10) podejmuje działania służące zapewnieniu niezawodności zasilania komputerów, innych urządzeń mających wpływ na bezpieczeństwo przetwarzania danych oraz zapewnieniu bezpiecznej wymiany danych w sieci wewnętrznej i bezpiecznej teletransmisji,
11) prowadzi ewidencję haseł do stanowisk roboczych poszczególnych użytkowników oraz ich identyfikatorów.

4. Osoba upoważniona do przetwarzania danych osobowych

Osoba upoważniona do przetwarzania danych osobowych jest zobowiązana do przestrzegania następujących zasad:

1) może przetwarzać dane osobowe wyłącznie w zakresie ustalonym indywidualnie przez administratora danych w upoważnieniu i tylko w celu wykonywania nałożonych na nią obowiązków. Zakres dostępu do danych przypisany jest do niepowtarzalnego identyfikatora użytkownika, niezbędnego do rozpoczęcia pracy w systemie. Rozwiązanie stosunku pracy, odwołanie z pełnionej funkcji powoduje wygaśnięcie upoważnienia do przetwarzania danych osobowych;
2) ma obowiązek zachowania tajemnicy danych osobowych oraz przestrzegania procedur ich bezpiecznego przetwarzania. Przestrzeganie tajemnicy danych osobowych *obowiązuje przez cały okres zatrudnienia u administratora danych, a także po ustaniu stosunku pracy lub odwołaniu z pełnionej funkcji*;
3) zapoznaje się z przepisami prawa w zakresie ochrony danych osobowych oraz postanowieniami niniejszej polityki i instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych;
4) stosuje określone przez administratora danych oraz administratora bezpieczeństwa informacji procedury oraz wytyczne mające na celu zgodne z prawem przetwarzanie danych;
5) korzysta z systemu informatycznego administratora danych w sposób zgodny ze wskazówkami zawartymi w instrukcjach obsługi urządzeń wchodzących

w skład systemu informatycznego, oprogramowania i nośników;

6) zabezpiecza dane przed ich udostępnianiem osobom nieupoważnionym.

IV. Infrastruktura przetwarzania danych osobowych

1. Obszar przetwarzania danych osobowych

W celu zapewnienia bezpiecznych warunków przetwarzania danych w systemach LUW, określa się obszary przetwarzania danych jako:

1) obiekty, wydzielone pomieszczenia lub części pomieszczeń, w których przetwarzane są dane (także w postaci tradycyjnej – papierowej),
2) części obiektów, w których znajdują się informatyczne urządzenia wyjścia (np. monitory, drukarki itp.).

Pomieszczenie określone jako obszar przetwarzania danych powinno spełniać następujące warunki:

1) być wyposażone w zamek mechaniczny lub elektroniczny zamykany każdorazowo, gdy opuszczają je pracownicy zatrudnieni przy przetwarzaniu danych,
2) monitory komputerów, na których wykonuje się przetwarzanie danych, powinny być ustawione w sposób uniemożliwiający ich podgląd osobom nieuprawnionym.

Wydzielona część pomieszczenia określona jako obszar przetwarzania danych powinna spełniać następujące warunki:

1) wyposażenie (meble) w tej części pomieszczenia muszą być tak ustawione, aby uniemożliwić dostęp do tego obszaru osobom nieuprawnionym,

Obszary przetwarzania danych w obiektach i pomieszczeniach LUW nie mogą być dostępne dla osób nieuprawnionych. Dopuszczalne odstępstwo stanowią pomieszczenia, w których przyjmowani są interesanci. Jeżeli pomieszczenia te wyposażone są jednocześnie w urządzenia z dostępem do systemów bazodanowych albo tradycyjne kartoteki, należy w nich stosować szczególne środki ostrożności, w tym:

1) interesanci powinni wchodzić pojedynczo i pozostawać w pomieszczeniu tylko w obecności użytkownika systemu,
2) kartoteki tradycyjne należy zabezpieczyć przed dostępem osób nieuprawnionych,
3) nie należy pozostawiać dokumentów papierowych i nośników elektronicznych w miejscach umożliwiających ich wykorzystanie przez osoby nieuprawnione,
4) drukarki i urządzenia peryferyjne powinny być usytuowane tak,

aby znajdowały się z dala od przestrzeni, po której poruszają się osoby nieuprawnione.

Wykaz budynków i pomieszczeń wchodzących w skład obszaru przetwarzania danych osobowych w LUW przedstawia poniższa tabela:

Adres budynków LUW	Nazwa pomieszczenia
Gorzów Wlkp.: ul. Jagiellończyka 8	- serwerownia w przyziemiu budynku LUW - pokoje biurowe zlokalizowane na 14 piętrach budynku LUW,
ul. Jagiellończyka 13	- parter
ul. Fabryczna 71	- Archiwum Zakładowe Urzędu
ul. Młyńska 12 Zielona Góra (Delegatura LUW):	- pokoje biurowe
ul. Podgórna 7 ul. Różana 13	- pokoje biurowe zlokalizowane na parterze i I piętrze - Archiwum Zakładowe Urzędu - Centrum Powiadamiania Ratunkowego

2. Zbiory danych

Wykaz zbiorów danych osobowych przetwarzanych w systemie informatycznym prowadzi administrator bezpieczeństwa informacji według wzoru określonego w załączniku Nr 4.

3. System informatyczny[1]

[1] Zgodnie z art. 7 pkt 2a ustawy system informatyczny to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych. Pojęcie „system informatyczny" obejmuje elementy zaliczone do czterech kategorii. Są to:
1) urządzenia,
2) programy,
3) procedury przetwarzania informacji,
4) narzędzia programowe.
Urządzenie to „rodzaj mechanizmu lub zespół elementów, przyrządów służących do wykonania określonej czynności, ułatwiający pracę". Program – według znaczenia przyjmowanego w informatyce – to odpowiednio uporządkowana sekwencja instrukcji, mająca na celu wykonanie określonych zadań. Procedury przetwarzania informacji mogłyby być utożsamiane z programem, lecz wobec ich odrębnego wskazania w analizowanej definicji należy przyjąć, że są to procedury inne niż przyjęte w stosowanych w konkretnym przypadku programach. Narzędzia programowe także mieszczą się w kategorii oprogramowania.

System informatyczny administratora danych obsługiwany jest przez serwery zlokalizowane w serwerowni i wyznaczonych pomieszczeniach budynków LUW (załącznik Nr 5). System ten ma bezpieczne połączenie z internetem. Poszczególne stacje robocze są zlokalizowane w pokojach biurowych znajdujących się w obszarze przetwarzania danych, określonym w pkt 1 bieżącego rozdziału.

Lista systemów informatycznych, które podlegają odrębnym zasadom bezpieczeństwa niż te które reguluje niniejszy dokument oraz Instrukcja Zarządzania Systemami Informatycznymi w LUW, znajduje się w załączniku nr 7.

V. Struktury zbiorów danych osobowych i sposób przepływu danych

Opisy struktur zbiorów danych osobowych oraz powiązań między zbiorami jak również sposób przepływu danych pomiędzy poszczególnymi systemami prowadzi administrator bezpieczeństwa informacji według wzoru określonego w Załączniku Nr 6. Opracowane opisy będą dostępne administratorom i/lub użytkownikom systemów informatycznych przetwarzających dane osobowe w tym systemie na pisemny wniosek złożony do ABI przez Dyrektora Wydziału/Biura, w którym dane zbiory są przetwarzane.

VI. Strategia zabezpieczenia danych osobowych (działania niezbędne do zapewnienia poufności, integralności i rozliczalności przetwarzanych danych)

1. Bezpieczeństwo osobowe

1.1. Zachowanie poufności

1) Ryzyko utraty bezpieczeństwa danych przetwarzanych przez administratora danych pojawiające się ze strony osób trzecich, które mają dostęp do danych osobowych (np. serwisanci firm zewnętrznych), jest minimalizowane przez podpisanie umów powierzenia przetwarzania danych osobowych.
2) Ryzyko ze strony osób, które potencjalnie mogą w łatwiejszy sposób uzyskać dostęp do danych osobowych (np. osoby sprzątające pomieszczenia administratora danych), jest minimalizowane przez zobowiązywanie ich do zachowania tajemnicy na podstawie odrębnych, pisemnych oświadczeń.

1.2. Szkolenia w zakresie ochrony danych osobowych

Administrator bezpieczeństwa informacji zakłada następujący plan szkoleń:

1) szkoli się każdą osobę, która ma zostać upoważniona do przetwarzania danych osobowych,

2) szkolenia wewnętrzne wszystkich osób upoważnionych do przetwarzania danych osobowych przeprowadzane są w przypadku znaczących zmian zasad lub procedur ochrony danych osobowych,

3) przeprowadza się szkolenia dla osób innych niż upoważnione do przetwarzania danych, jeśli pełnione przez nie funkcje wiążą się z zabezpieczeniem danych osobowych.

2. Strefy bezpieczeństwa

W siedzibie administratora danych wydzielono umowne strefy bezpieczeństwa klasy I, klasy II i klasy III.

Klasa I, w skład której wchodzą systemy nie przetwarzające danych osobowych. Systemy są połączone z publiczną siecią telekomunikacyjną.

W strefie bezpieczeństwa klasy I stosuje się podstawowe środki bezpieczeństwa stanowiska komputerowego w danej komórce organizacyjnej.

Klasa II, w skład której wchodzą systemy przetwarzające dane osobowe (w tym: dane wrażliwe). Systemy nie są połączone z publiczną siecią telekomunikacyjną.

W strefie bezpieczeństwa klasy II do danych osobowych mają dostęp wszystkie osoby upoważnione do przetwarzania danych osobowych zgodnie z zakresami upoważnień do ich przetwarzania, a osoby postronne mogą w niej przebywać tylko w obecności pracownika upoważnionego do przetwarzania danych osobowych. Strefa ta obejmuje wszystkie pozostałe pomieszczenia zaliczone do obszaru przetwarzania danych w siedzibie administratora danych.

W skład strefy klasy II, w której dostęp do informacji zabezpieczony jest wewnętrznymi środkami kontroli, wchodzą m.in.:

1) pomieszczenia w Oddziale Mandatów Wydziału Finansów, Budżetu i Certyfikacji,

2) pomieszczenia w Oddziale Paszportów Wydziału Spraw Obywatelskich, Cudzoziemców i Certyfikacji,

3) pomieszczenia w Oddziale Cudzoziemców Wydziału Spraw Obywatelskich, Cudzoziemców i Certyfikacji,

4) pomieszczenie księgowości z kasą pancerną, w którym mogą przebywać pracownicy księgowości, inni użytkownicy danych tylko w towarzystwie pracowników księgowości. Osoby z zewnątrz, wpłacające pieniądze do kasy LUW mogą przebywać tylko w wyznaczonym miejscu, odgrodzonym kratami od stanowiska kasjerki.

Klasa III, w skład której wchodzą systemy przetwarzające dane osobowe (w tym: dane wrażliwe). Systemy są połączone z publiczną siecią telekomunikacyjną - występują zagrożenia pochodzące z sieci publicznej.

W strefie tej obowiązuje ochrona danych osobowych jak w strefie klasy II a

ponadto system informatyczny chroni się przed zagrożeniami pochodzącymi z sieci publicznej poprzez wdrożenie fizycznych i logicznych zabezpieczeń chroniących przed nieuprawnionym dostępem.

W przypadku zastosowania logicznych zabezpieczeń obejmą one:

1) kontrolę przepływu informacji pomiędzy systemem informatycznym administratora danych a siecią publiczną;
2) kontrolę działań inicjowanych z publicznej sieci telekomunikacyjnej i systemu informatycznego administratora danych;
3) środki kryptograficznej ochrony wobec danych wykorzystywanych do uwierzytelnienia, które są przesyłane w sieci publicznej.

W skład strefy klasy III, w której dostęp do informacji zabezpieczony jest wewnętrznymi środkami kontroli, wchodzą m.in.:

1) serwerownia, w której mogą przebywać wyłącznie uprawnieni pracownicy Oddziału Informatyki oraz inne osoby upoważnione do przebywania w serwerowni tylko w obecności tych pracowników,
2) pomieszczenia w Oddziale Kadr i Szkolenia Biura Organizacyjnego i Kadr, w których przetwarzane dane osobowe są eksportowane do ZUS poprzez publiczną sieć telekomunikacyjną.

3. Zabezpieczenie sprzętu

1) Serwer jest zlokalizowany w odrębnym, klimatyzowanym pomieszczeniu (serwerowni), zamykanym drzwiami antywłamaniowymi. Okna tego pomieszczenia zabezpieczone są żaluzjami antywłamaniowymi. Wewnątrz pomieszczenia znajdują się urządzenia sygnalizujące zdarzenia losowe (pożar, zalanie wodą, itp.). W serwerowni mogą przebywać wyłącznie pracownicy Oddziału informatyki, inne osoby upoważnione do przetwarzania tylko w ich obecności, a osoby postronne w ogóle nie mają dostępu.
2) Pracownicy Oddziału informatyki wskazują użytkownikom, jak postępować, aby zapewnić prawidłową eksploatację systemu informatycznego, a zwłaszcza:
    a) ochronę nośników danych, na których przechowywane są kopie zapasowe,
    b) prawidłową lokalizację komputerów przetwarzających dane osobowe.
3) Bieżąca konserwacja sprzętu wykorzystywanego przez administratora danych do przetwarzania danych prowadzona jest przez pracowników Oddziału Informatyki oraz pracowników firm zewnętrznych, którym poprzez zlecenie powierzane jest wykonywanie określonych działań w tym zakresie. Natomiast naprawy sprzętu objętego gwarancją wykonywane przez personel zewnętrzny realizowane są w siedzibie administratora danych w obecności uprawnionych pracowników LUW.

4) Administrator systemu dopuszcza konserwowanie i naprawę sprzętu poza siedzibą administratora danych jedynie po trwałym usunięciu danych osobowych. Zużyty sprzęt służący do przetwarzania danych osobowych może być zbywany dopiero po trwałym usunięciu danych, a urządzenia uszkodzone mogą być przekazywane w celu utylizacji (jeśli trwałe usunięcie danych wymagałoby nadmiernych nakładów ze strony administratora) właściwym podmiotom.

4. Monitorowanie dostępu do systemu i jego użycia

Monitorowanie dostępu do systemu i jego użycia odbywa się poprzez zapisy na serwerach LUW. Ponadto zapewnia się odnotowanie:

1) daty pierwszego wprowadzenia danych do systemu;
2) identyfikatora użytkownika wprowadzającego dane osobowe do systemu;
3) źródła danych - w przypadku zbierania danych nie od osoby, której one dotyczą;
4) informacji o odbiorcach w rozumieniu art. 7 pkt 6 ustawy, którym dane osobowe zostały udostępnione, o dacie i zakresie tego udostępnienia;
5) sprzeciwu wobec przetwarzania danych osobowych, o którym mowa w art. 32 ust. 1 pkt 8 ustawy.

Odnotowanie informacji, o których mowa w pkt 1 i 2, następuje automatycznie po zatwierdzeniu przez użytkownika operacji wprowadzenia danych.

Dla każdej osoby, której dane osobowe są przetwarzane w systemie informatycznym, system zapewnia sporządzenie i wydrukowanie raportu zawierającego w powszechnie zrozumiałej formie informacje, o których mowa w pkt 1-5.

System informatyczny administratora danych umożliwia zapisywanie zdarzeń wyjątkowych i przechowywanie informacji o nich przez określony czas. Zapisy takie obejmują:

1) identyfikator użytkownika;
2) datę i czas zalogowania i wylogowania się z systemu;
3) zapisy udanych i nieudanych prób dostępu do systemu;
4) zapisy udanych i nieudanych prób dostępu do danych osobowych i innych zasobów systemowych.

5. Przeglądy okresowe zapobiegające naruszeniom obowiązku szczególnej staranności administratora danych (art. 26 ust. 1 ustawy o ochronie danych osobowych)

1) Administrator bezpieczeństwa informacji przeprowadza raz w roku przegląd przetwarzanych danych osobowych pod kątem celowości ich dalszego

przetwarzania. Osoby upoważnione do przetwarzania danych osobowych są zobowiązani współpracować z administratorem bezpieczeństwa informacji w tym zakresie i wskazywać mu dane osobowe, które powinny zostać usunięte ze względu na zrealizowanie celu przetwarzania danych osobowych lub brak ich adekwatności do realizowanego celu.

2) Administrator bezpieczeństwa informacji może zarządzić przeprowadzenie dodatkowego przeglądu w wyżej określonym zakresie w razie zmian w obowiązującym prawie, ograniczających dopuszczalny zakres przetwarzanych danych osobowych. Dodatkowy przegląd jest możliwy także w sytuacji zmian organizacyjnych administratora danych.

3) Z przebiegu usuwania danych osobowych należy sporządzić protokół podpisywany przez administratora bezpieczeństwa informacji i Dyrektora Wydziału/Biura, w którym usunięto dane osobowe.

6. Odpowiedzialność osób upoważnionych do przetwarzania danych osobowych

Niezastosowanie się do prowadzonej przez administratora danych polityki bezpieczeństwa przetwarzania danych osobowych, której założenia określa niniejszy dokument, i naruszenie procedur ochrony danych przez pracowników upoważnionych do przetwarzania danych osobowych może być potraktowane jako ciężkie naruszenie obowiązków pracowniczych, skutkujące rozwiązaniem stosunku pracy bez wypowiedzenia na podstawie art. 52 Kodeksu pracy.

Niezależnie od rozwiązania stosunku pracy osoby popełniające przestępstwo będą pociągane do odpowiedzialności karnej zwłaszcza na podstawie art. 51-52 ustawy oraz art. 266 Kodeksu karnego.

VII. Przeglądy polityki bezpieczeństwa i audyty systemu

Polityka bezpieczeństwa powinna być poddawana przeglądowi przynajmniej raz na rok. W razie istotnych zmian dotyczących przetwarzania danych osobowych administrator bezpieczeństwa informacji może zwrócić się do administratora danych o zarządzenie przeglądu polityki bezpieczeństwa stosownie do potrzeb.

Administrator bezpieczeństwa informacji analizuje, czy polityka bezpieczeństwa i pozostała dokumentacja z zakresu ochrony danych osobowych jest adekwatna do:

1) zmian w budowie systemu informatycznego;
2) zmian organizacyjnych administratora danych, w tym również zmian statusu osób upoważnionych do przetwarzania danych osobowych;
3) zmian w obowiązującym prawie.

Administrator bezpieczeństwa informacji po uzgodnieniu z administratorem danych może, stosownie do potrzeb, przeprowadzić wewnętrzny audyt zgodności przetwarzania danych z przepisami o ochronie danych osobowych. Przeprowadzenie audytu wymaga uzgodnienia jego zakresu z administratorem systemu. Zakres, przebieg i rezultaty audytu dokumentowane są protokolarnie na piśmie.

VIII. Postanowienia końcowe

Każda osoba upoważniona do przetwarzania danych osobowych zobowiązana jest zapoznać się przed dopuszczeniem do przetwarzania danych z niniejszym dokumentem oraz złożyć stosowne oświadczenie, potwierdzające znajomość jego treści.

Każda osoba upoważniona do przetwarzania danych posiada wgląd do Polityki Bezpieczeństwa Informacji oraz Instrukcji Zarządzania Systemami Informatycznymi, które są zamieszczone w INTRANECIE.

Polityka Bezpieczeństwa Informacji wchodzi w życie z dniem ..... 2014r.