Załącznik Nr 1 do zarządzenia Nr 64/18 Rektora
Państwowej Wyższej Szkoły Informatyki i Przedsiębiorczości w Łomży
z dnia 25.05.2018 r. w sprawie ochrony danych osobowych w PWSIiP w Łomży

Polityka Bezpieczeństwa Ochrony Danych Osobowych

w Państwowej Wyższej Szkole Informatyki
i Przedsiębiorczości w Łomży
wraz z Instrukcją zarządzania systemem
informatycznym i wykazem zabezpieczeń

Spis treści

Część I. Organizacja systemu ochrony danych osobowych

1. Wprowadzenie

Niniejszy dokument opisuje zasady ochrony danych osobowych stosowane przez Państwową Wyższą Szkołę Informatyki i Przedsiębiorczości w Łomży – zwaną dalej PWSIiP lub Uczelnią, w celu spełnienia wymagań Rozporządzenia 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 dnia 04.05.2016 r. i reguły dotyczące procedur zapewnienia bezpieczeństwa przetwarzanych danych osobowych.

Celem Polityki Bezpieczeństwa Ochrony Danych Osobowych, dalej zwaną Polityką Bezpieczeństwa, jest wskazanie działań, jakie należy wykonać oraz ustanowienie zasad i reguł postępowania, które należy stosować, aby zapewnić bezpieczeństwo przetwarzania i właściwą ochronę danych osobowych w związku z czynnościami przetwarzania, a w szczególności zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną oraz zapewnić ochronę prywatności osób, których dane są przetwarzane.

Opisane zasady i reguły określają granice dopuszczalnego zachowania wszystkich osób przetwarzających dane osobowe, w tym użytkowników systemów informatycznych wspomagających prace PWSIiP.

Polityka Bezpieczeństwa, wskazuje sposób postępowania w sytuacji naruszenia bezpieczeństwa danych osobowych i jest w szczególności przeznaczona dla osób pracujących przy przetwarzaniu danych osobowych na Uczelni. Wykonywanie postanowień tego dokumentu ma zapewnić właściwą reakcję, ocenę i udokumentowanie przypadków naruszenia bezpieczeństwa w trakcie czynności przetwarzania danych.

Polityka bezpieczeństwa stanowi jeden ze środków organizacyjnych, mających na celu wykazanie, że przetwarzanie danych osobowych odbywa się zgodnie z przepisami powyższego Rozporządzenia. Ustanawia też wykaz procedur oraz stosowanych środków technicznych i logicznych mających na celu zabezpieczenie przetwarzanych danych

osobowych przed przypadkowym lub niezgodnym z prawem zniszczeniem, utratą, modyfikacją, nieuprawnionym ujawnieniem lub nieuprawnionym do nich dostępem.
Opisane i zastosowane w niej zabezpieczenia mają zapewnić:

1.) poufność danych - rozumianą jako właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym osobom,
2.) integralność danych - rozumianą jako właściwość zapewniającą, że dane osobowe nie zostały w sposób nieautoryzowany zmienione lub zniszczone,
3.) rozliczalność danych - rozumianą jako właściwość zapewniającą, że działania osoby mogą być przypisane w sposób jednoznaczny tylko tej osobie, a także jako możliwość udokumentowania przed organem nadzorczym prawidłowości i zgodności z prawem działań związanych z przetwarzaniem danych osobowych,
4.) integralność systemu - rozumianą jako nienaruszalność systemu, niemożność dokonania jakiejkolwiek manipulacji, zarówno zamierzonej, jak i przypadkowej.

1.1 Przez użyte w Polityce Bezpieczeństwa określenia, należy rozumieć:

1.) Administrator – Państwowa Wyższa Szkoła Informatyki i Przedsiębiorczości w Łomży, podmiot decydujący o celach i środkach przetwarzania danych osobowych;
2.) Podmiot przetwarzający - osoba fizyczna lub prawna, organ publiczny lub jakikolwiek inny podmiot przetwarzający dane osobowe w imieniu administratora;
3.) Inspektor Ochrony Danych (IOD) – osoba wyznaczona przez administratora, wspomagająca administratora w monitorowaniu przestrzegania przepisów o ochronie danych i doradzająca administratorowi w zakresie prowadzonych operacji przetwarzania danych osobowych;
4.) Rozporządzenie (RODO) – rozporządzenie 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);
5.) Dane osobowe (dane) - wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej;
6.) Zbiór danych – uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów oraz celów;
7.) Usuwanie danych – zniszczenie danych osobowych lub taką ich modyfikację , która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą,

8.) Przetwarzanie danych - wykonywanie jakichkolwiek operacji na danych osobowych, takich jak np. zbieranie, utrwalanie, przeglądanie, przechowywanie, modyfikowanie, opracowywanie, porządkowanie, udostępnianie w jakiejkolwiek formie, zmienianie, usuwanie lub niszczenie;

9.) Odbiorca danych – osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, któremu ujawnia się dane osobowe niezależnie od tego, czy jest stroną trzecią. Nie jest uznawany za odbiorcę organ publiczny, który może otrzymywać dane osobowe w ramach konkretnego postępowania;

10.) Rejestr czynności przetwarzania – prowadzony przez administratora rejestr, mający na celu udokumentowanie zapewnienia zgodności wykonywanych czynności przetwarzania z RODO oraz umożliwiający organowi nadzorczemu monitorowanie prowadzonego przetwarzania;

11.) System informatyczny (system) – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;

12.) Administrator Systemu Informatycznego (ASI) - osoba nadzorująca pracę systemu informatycznego oraz wykonująca w nim czynności wymagające specjalnych uprawnień;

13.) Użytkownik – osoba posiadająca uprawnienia do pracy w systemie informatycznym zgodnie z zakresem obowiązków służbowych;

14.) Zabezpieczenie systemu informatycznego – wdrożenie stosownych środków administracyjnych, technicznych i fizycznych w celu zabezpieczenia zasobów technicznych oraz ochrony przed nieuprawnioną modyfikacją, zniszczeniem, nieuprawnionym dostępem i ujawnieniem lub pozyskaniem danych osobowych, a także ich utratą,

15.) Nośnik komputerowy – nośnik służący do zapisu i przechowywania informacji, np. pendrive, płyty CD/DVD, dyski twarde;

16.) Kierownik komórki organizacyjnej – należy przez to rozumieć kierowników komórek organizacyjnych, w których zatrudnieni są pracownicy przetwarzający dane osobowe, a także samodzielne stanowiska pracy;

17.) PWSIiP, Uczelnia – Państwowa Wyższa Szkoła Informatyki i Przedsiębiorczości w Łomży;

18.) UODO – Urząd Ochrony Danych Osobowych;

19.) Incydent - naruszenie ochrony danych osobowych ze względu na poufność, dostępność i integralność danych, wywołujący ryzyko naruszenia praw lub wolności osób fizycznych;

20.) Zagrożenie – potencjalna możliwość wystąpienia incydentu;

21.) Działanie korygujące – działanie przeprowadzane w celu wyeliminowania przyczyny i skutku incydentu lub innej niepożądanej sytuacji;

22.) Działanie zapobiegawcze – działanie, które należy przedsięwziąć, aby wyeliminować przyczyny zagrożenia lub innej potencjalnej sytuacji niepożądanej;

23.) Kontrola (Monitorowanie) – systematyczna, niezależna i udokumentowana ocena skuteczności systemu ochrony danych osobowych, na podstawie wymagań wynikających z przepisów prawa, Polityki Bezpieczeństwa Ochrony Danych Osobowych;

24.) Identyfikator użytkownika — rozumie się przez to ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym;

25.) Haśle — rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym;

26.) Uwierzytelnianie — rozumie się przez to działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu;

1.2 Zakresy określone przez Politykę Bezpieczeństwa mają zastosowanie do całego systemu informacyjnego Państwowej Wyższej Szkoły Informatyki i Przedsiębiorczości w Łomży, w szczególności do:

1.) wszystkich istniejących, wdrażanych obecnie lub w przyszłości systemów informatycznych oraz zbiorów papierowych, w których przetwarzane są informacje podlegające ochronie,

2.) informacji będących własnością Państwowej Wyższej Szkoły Informatyki i Przedsiębiorczości w Łomży lub jej kontrahentów, o ile zostały przekazane na podstawie umów,

3.) wszystkich lokalizacji – budynków i pomieszczeń, w których są lub będą przetwarzane informacje podlegające ochronie.

2. Ochrona danych osobowych

2.1 Zasady ogólne

Ochrona danych osobowych w Państwowej Wyższej Szkole Informatyki i Przedsiębiorczości w Łomży opiera się na następujących filarach:

1.) Legalność – PWSIiP dba o ochronę prywatności i przetwarza dane zgodnie z prawem.
2.) Bezpieczeństwo - PWSIiP zapewnia odpowiedni poziom bezpieczeństwa danych podejmując stale działania w tym zakresie.
3.) Ochrona praw osób fizycznych - PWSIiP umożliwia osobom, których dane przetwarza, wykonywanie swoich praw i prawa te realizuje.
4.) Rozliczalność - PWSIiP dokumentuje to, w jaki sposób spełnia obowiązki, aby w każdej chwili móc wykazać zgodność z przepisami rozporządzenia.

2.2 Zasady ochrony danych osobowych

Państwowa Wyższa Szkoła Informatyki i Przedsiębiorczości w Łomży przetwarza dane osobowe z poszanowaniem następujących zasad:

1.) W oparciu o podstawę prawną i zgodnie z prawem (legalizm)
2.) Rzetelnie i uczciwie (rzetelność)
3.) W sposób przejrzysty dla osoby, której dane dotyczą (transparentność)
4.) W konkretnych celach i nie „na zapas” (minimalizacja)
5.) W ilości nie większej niż potrzeba (adekwatność)
6.) Z dbałością o prawidłowość danych (prawidłowość)
7.) Nie dłużej niż wynika to z potrzeby przetwarzania (czasowość)
8.) Zapewniając odpowiednie bezpieczeństwo danych (bezpieczeństwo).

2.3 System ochrony danych

Państwowa Wyższa Szkoła Informatyki i Przedsiębiorczości w Łomży, tworząc system ochrony danych osobowych:

1.) dokonuje identyfikacji zasobów danych osobowych, kategorii przetwarzanych danych, zależności między zasobami danych i identyfikacji sposobów wykorzystania danych, a także identyfikuje przypadki współadministrowania danymi i postępuje w tym zakresie zgodnie z przepisami rozporządzenia (inwentaryzacja);
2.) opracowuje i prowadzi Rejestr Czynności Przetwarzania. Rejestr jest narzędziem rozliczania zgodności ochrony danych z przepisami prawa;

3.) zapewnia, identyfikuje i weryfikuje podstawy prawne przetwarzania danych, w tym utrzymuje system zarządzania zgodami na przetwarzanie danych umożliwiający rejestrację i weryfikację posiadania zgody osoby na przetwarzanie jej konkretnych danych w konkretnym celu oraz rejestrację cofnięcia zgody i podobnych czynności (sprzeciw, ograniczenie przetwarzania itp.). Wzór Rejestru oświadczeń o wyrażeniu zgody zawiera Załącznik Nr 1 do PB PWSIiP. Rejestr może być prowadzony w formie elektronicznej;

4.) zapewnia obsługę praw osób fizycznych, których dane przetwarza, zgodnie z procedurą stanowiącą Załącznik Nr 2 do PB PWSIiP - Zasady wykonywania obowiązków informacyjnych i obsługi żądań, realizując otrzymane w tym zakresie żądania, w tym:

   a. przekazuje osobom prawem wymagane informacje przy zbieraniu danych oraz organizuje i zapewnia udokumentowanie realizacji tych obowiązków;
   b. weryfikuje i zapewnia możliwość efektywnego wykonania każdego typu żądania przez siebie i swoich przetwarzających;
   c. zapewnia odpowiednie nakłady i procedury, aby żądania osób były realizowane w terminie i w sposób wymagany przez przepisy prawa oraz dokumentowane;

5.) stosuje zasadę minimalizacji przetwarzania danych pod kątem adekwatności danych do celów przetwarzania, dostępu do danych i czasu przechowywania danych, dokonując w tym celu okresowego przeglądu przetwarzanych danych nie rzadziej niż raz na rok. Szczegółowe zasady dostępu fizycznego i logicznego zawarte są w procedurach bezpieczeństwa fizycznego i bezpieczeństwa informatycznego opisanych w dalszej części Polityki Bezpieczeństwa;

6.) zapewnia odpowiedni poziom bezpieczeństwa danych, w tym:

   a. przeprowadza analizy ryzyka dla czynności przetwarzania danych,
   b. przeprowadza analizy oceny skutków dla ochrony danych tam, gdzie ryzyko naruszenia praw i wolności osób jest wysokie,
   c. dostosowuje środki ochrony danych do ustalonego ryzyka,

7.) stosuje procedury postępowania w przypadku naruszenia ochrony danych osobowych, procedury pozwalające na identyfikację, ocenę i zgłoszenie zidentyfikowanego naruszenia ochrony danych organowi nadzorczemu oraz procedury pozwalające na zawiadamianie osób, których dane dotyczą, o naruszeniu ochrony danych, jeżeli to konieczne,

8.) zapewnia zasady doboru i weryfikacji podmiotów przetwarzających w jej imieniu dane osobowe, opracowane w celu zapewnienia, aby przetwarzający dawali wystarczające gwarancje wdrożenia odpowiednich środków organizacyjnych i technicznych dla zapewnienia bezpieczeństwa, realizacji praw osób, których dane są przetwarzane i innych obowiązków związanych z ochroną danych osobowych,

9.) zarządza zmianami mającymi wpływ na prywatność. W tym celu procedury uruchamiania nowych projektów związanych z przetwarzaniem danych osobowych, uwzględniają konieczność oceny wpływu zmiany na ochronę danych, zapewnienie prywatności (w tym zgodności celów przetwarzania, bezpieczeństwa danych i minimalizacji) już w fazie projektowania zmiany.

3. Administrator danych

3.1 Obowiązkiem administratora jest zapewnienie, aby przestrzegane były zasady dotyczące przetwarzania danych osobowych.

3.2 Administrator podejmuje odpowiednie środki, aby udzielić osobie, której dane dotyczą wszelkich informacji w sprawie przetwarzania oraz ułatwić tej osobie wykonywanie przysługujących jej praw.

3.3 Administrator wdraża odpowiednie środki techniczne i organizacyjne, w celu skutecznej realizacji zasad ochrony danych oraz w celu nadania przetwarzaniu niezbędnych zabezpieczeń a także, aby domyślnie przetwarzane były wyłącznie te dane osobowe, które są niezbędne dla osiągnięcia każdego konkretnego celu przetwarzania. Środki te są w razie potrzeby poddawane przeglądom i uaktualniane.

3.4 Obowiązkiem administratora jest prowadzenie w formie pisemnej (w tym elektronicznej) rejestru czynności przetwarzania danych, zawierającego informacje pozwalające monitorować prawidłowość procesów przetwarzania.

3.5 Administrator zobowiązany jest w każdym przypadku do przeprowadzenia oceny ryzyka związanego z przetwarzaniem, a jeżeli dany rodzaj przetwarzania może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator przed rozpoczęciem przetwarzania dokonuje oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych.

3.6 Obowiązkiem administratora jest zapewnienie, aby każda osoba fizyczna działająca z upoważnienia administratora lub podmiotu przetwarzającego, która

ma dostęp do danych osobowych, przetwarzała je wyłącznie na polecenie administratora.

3.7 Administrator dokumentuje wszelkie naruszenia ochrony danych osobowych, uwzględniając w szczególności okoliczności naruszenia, jego skutki oraz podjęte działania zaradcze.

3.8 Administrator jest zobowiązany do zgłoszenia organowi nadzorczemu faktu naruszenia ochrony danych osobowych oraz powiadomienia o takim naruszeniu osoby, której dane dotyczą, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych.

3.9 Administrator wyznacza Inspektora Ochrony Danych w celu monitorowania przestrzegania przepisów z zakresu ochrony danych osobowych.

3.10 Administrator wspiera Inspektora Ochrony Danych w wypełnianiu jego zadań i zapewnia, by Inspektor Ochrony Danych był włączany we wszystkie sprawy dotyczące ochrony danych osobowych.

3.11 Administrator upoważnia Inspektora Ochrony Danych do:

1.) reprezentowania Administratora w zakresie określonym w upoważnieniu,
2.) udzielania i odwoływania upoważnień do przetwarzania danych osobowych pracownikom, osobom zatrudnionym na podstawie umów cywilnoprawnych, stażystom;
3.) udzielania i odwoływania upoważnień do przebywania w obszarze przetwarzania danych osobowych pracownikom PWSIiP oraz pracownikom firm zewnętrznych świadczących usługi na rzecz PWSIiP.

3.12 Upoważnienie, o którym mowa w pkt. 3.11, ma postać pisemną - Załącznik nr 3 do PB PWSIiP w Łomży.

4. Inspektor Ochrony Danych

4.1 Do obowiązków Inspektora Ochrony Danych należy:

1.) Informowanie Administratora oraz pracowników i współpracowników PWSIiP, przetwarzających dane osobowe, o obowiązkach spoczywających na nich z mocy przepisów prawa oraz doradzanie im w sprawach związanych z przetwarzaniem danych osobowych,
2.) Monitorowanie przestrzegania przepisów prawa i polityk Administratora w zakresie ochrony danych osobowych, podejmowanie wszelkich działań zwiększających

świadomość i szkolenie osób uczestniczących w procesach przetwarzania oraz przeprowadzanie związanych z tym audytów,

3.) Udzielanie na żądanie Administratora zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania,

4.) Pełnienie funkcji punktu kontaktowego dla osób, których dane są przetwarzane przez Administratora, a także dla organu nadzorczego w kwestiach związanych z przetwarzaniem danych osobowych oraz współpraca z organem nadzorczym we wszelkich innych sprawach.

4.2 Do pozostałych obowiązków IOD scedowanych przez Administratora należy:

1.) organizacja bezpieczeństwa i ochrony danych osobowych zgodnie z wymogami Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679,

2.) wydawanie i odwoływanie upoważnień do przetwarzania danych osobowych,

3.) prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych,

4.) prowadzenie postępowań wyjaśniających w przypadku naruszenia ochrony danych osobowych,

5.) nadzór nad bezpieczeństwem danych osobowych,

6.) prowadzenie rejestru czynności przetwarzania,

7.) kontrola działań komórek organizacyjnych pod względem zgodności przetwarzania danych z przepisami o ochronie danych osobowych,

8.) inicjowanie i podejmowanie przedsięwzięć w zakresie doskonalenia ochrony danych osobowych.

4.3 Inspektor Ochrony Danych ma prawo :

1.) wyznaczania, rekomendowania i egzekwowania wykonania zadań związanych z ochroną danych osobowych w całej organizacji,

2.) wstępu do pomieszczeń, w których zlokalizowane są zbiory danych i przeprowadzenia niezbędnych badań lub innych czynności kontrolnych, w celu oceny zgodności przetwarzania danych z przepisami prawa,

3.) żądania złożenia pisemnych lub ustnych wyjaśnień w zakresie niezbędnym do ustalenia stanu faktycznego,

4.) żądania okazania dokumentów i wszelkich danych mających bezpośredni związek z problematyką kontroli,

5.) żądania udostępnienia do kontroli urządzeń, nośników oraz systemów informatycznych służących do przetwarzania danych.

5. Obowiązki pracowników przetwarzających dane osobowe

5.1 Kierownik komórki organizacyjnej PWSIiP ma obowiązek w szczególności:

1.) znać podstawy prawne, na jakich komórka przez niego kierowana dokonuje konkretnych czynności przetwarzania danych osobowych;
2.) sprawowania kontroli nad wprowadzaniem i udostępnianiem danych osobowych;
3.) nadzorowania fizycznych zabezpieczeń pomieszczeń, w których przetwarzane są dane osobowe oraz kontroli przebywających w nich osób;
4.) niezwłocznego informowania administratora oraz Inspektora Ochrony Danych o przypadkach naruszenia przepisów o ochronie danych osobowych.

5.2 Pozostałe obowiązki pracowników w zakresie ochrony danych osobowych opisane zostały w Instrukcji w sprawie zasad postępowania przy przetwarzaniu danych osobowych w PWSIiP w Łomży, stanowiącej Załącznik Nr 4 do PB PWSIiP.

6. Sposób zapewnienia odnotowania informacji o odbiorcach, którym dane osobowe zostały udostępnione, dacie i zakresie tego udostępnienia

6.1 Dane osobowe udostępnia się odbiorcy danych na pisemny wniosek ze wskazaniem przez odbiorcę podstawy prawnej legalizującej przetwarzanie danych.

6.2 Zgody na udostępnienie danych udziela IOD, który odpowiada również za udostępnienie danych osobowych w sposób zgodny z ich przeznaczeniem.

6.3 IOD odnotowuje zdarzenia udostępnienia w rejestrze odbiorców danych osobowych. W rejestrze odnotowywane są między innymi: imię i nazwisko lub nazwa odbiorcy, adres odbiorcy, podstawa prawna udostępnienia, data udostępnienia oraz zakres udostępnienia. Dopuszcza się załączanie do rejestru wydruku/kopii papierowej przekazanego zbioru danych. Wzór rejestru odbiorców danych osobowych stanowi Załącznik Nr 5 do PB PWSIiP.

6.4 W sytuacji kiedy system informatyczny umożliwia odnotowywanie informacji o odbiorcach danych, możliwe jest prowadzenie rejestru elektronicznego.

6.5 Na żądanie osoby, której dane zostały udostępnione odbiorcy danych, IOD udostępnia właściwe informacje na podstawie prowadzonego rejestru lub wygenerowanego raportu w systemie informatycznym, jeśli program udostępnia funkcjonalność rejestracji odbiorców danych.

7. Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe

7.1 Obszar, w którym przetwarzane są dane osobowe stanowią budynki, w których Państwowa Wyższa Szkoła Informatyki i Przedsiębiorczości w Łomży realizuje swoje zadania statutowe.

7.2 Szczegółowe rozmieszczenie zbiorów w postaci dokumentacji papierowej i elektronicznej, zawierających dane osobowe, opisane jest w Wykazie budynków i pomieszczeń stanowiących obszar przetwarzania danych osobowych, którego wzór stanowi Załącznik Nr 6 do PB PWSIiP.

7.3 Administrator budynku zobowiązany jest przekazać Inspektorowi Ochrony Danych niezwłocznie, nie później jednak niż w terminie 7 dni, informację o zmianach w przeznaczeniu pomieszczeń.

8. Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych

8.1 Dane osobowe w Państwowej Wyższej Szkole Informatyki i Przedsiębiorczości w Łomży przetwarzane są w celu realizacji statutowych celów szkoły wyższej. W szczególności dane osobowe przetwarza się:

1.) dla zabezpieczenia prawidłowego toku realizacji zadań dydaktycznych, naukowych i organizacyjnych Uczelni, wynikających z przepisów ustawy z dnia 27 lipca 2005 r. Prawo o szkolnictwie wyższym (Dz.U. Nr 164, poz. 1365 z późn. zm.),

2.) w celu zapewnienia prawidłowej, zgodnej z prawem i celami Uczelni polityki personalnej oraz bieżącej obsługi stosunków pracy, a także innych stosunków zatrudnienia, nawiązywanych przez Uczelnię, działającą jako pracodawca w rozumieniu art. 3 Kodeksu pracy lub strona innych stosunków zatrudnienia,

3.) dla wykonywania zadań realizowanych w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi, z poszanowaniem praw i wolności osób powierzających Uczelni swoje dane.

8.2 Wykaz zbiorów danych osobowych w postaci dokumentacji papierowej i elektronicznej opisany jest w Wykazie zbiorów danych osobowych, którego wzór stanowi Załącznik Nr 7 do PB PWSIiP.

8.3 Wykaz programów stosowanych do przetwarzania danych osobowych zawartych w w/w zbiorach zawarty jest w Wykazie programów zastosowanych do przetwarzania danych osobowych, którego wzór stanowi Załącznik Nr 8 do PB PWSIiP.

9. Środki organizacyjne stosowane dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych

9.1 Zabezpieczenia organizacyjne:

Opracowano i wdrożono Politykę Bezpieczeństwa Ochrony Danych Osobowych wraz z Instrukcją zarządzania systemem informatycznym i wykazem zabezpieczeń.

Wyznaczono Inspektora Ochrony Danych i nadano mu upoważnienia do reprezentowania Administratora oraz do nadawania i odwoływania w jego imieniu upoważnień do przetwarzania danych osobowych.

Do przetwarzania danych osobowych zostały dopuszczone wyłącznie osoby posiadające upoważnienia nadane przez Administratora.

Prowadzona jest ewidencja osób upoważnionych do przetwarzania danych.

Stosowana jest zasada zapoznania każdej osoby z przepisami dotyczącymi ochrony danych osobowych przed przystąpieniem do pracy przy przetwarzaniu danych osobowych.

Osoby zatrudnione przy przetwarzaniu danych osobowych zobowiązane zostały do zachowania ich w tajemnicy.

Przetwarzanie danych osobowych dokonywane jest w warunkach zabezpieczających dane przed dostępem osób nieupoważnionych.

Przebywanie osób nieuprawnionych w pomieszczeniach, gdzie przetwarzane są dane osobowe jest dopuszczalne tylko w obecności osoby upoważnionej do przetwarzania danych osobowych.

Powierzanie przetwarzania danych osobowych innemu podmiotowi odbywa się w drodze umowy zawartej na piśmie.

W przypadku żądania udostępniania danych osobowych pracownicy PWSIiP w Łomży postępują zgodnie z przepisami o ochronie danych osobowych.

Niezależnie od niniejszych zasad, w zakresie bezpieczeństwa mają zastosowanie wszelkie wewnętrzne regulaminy lub instrukcje dotyczące bezpieczeństwa zasobów informacyjnych oraz indywidualne zakresy obowiązków pracowników.

Administrator za pośrednictwem Inspektora Ochrony Danych sprawuje nadzór nad przestrzeganiem zasad ochrony danych osobowych wynikających z przepisów prawa oraz zasad ustanowionych w niniejszym dokumencie.

10. Rejestr Czynności Przetwarzania

10.1 Rejestr Czynności Przetwarzania stanowi formę dokumentowania czynności przetwarzania danych i jest jednym z kluczowych elementów umożliwiających realizację fundamentalnej zasady, na której opiera się cały system ochrony danych osobowych, czyli zasady rozliczalności.

10.2 PWSIiP prowadzi Rejestr Czynności Przetwarzania, w którym inwentaryzuje i monitoruje sposób, w jaki wykorzystuje dane osobowe.

10.3 Rejestr jest jednym z podstawowych narzędzi umożliwiających Uczelni rozliczanie większości obowiązków ochrony danych.

10.4 W rejestrze, dla każdej czynności przetwarzania danych, którą uznano za odrębną dla potrzeb rejestru, PWSIiP odnotowuje co najmniej:

1.) nazwę czynności,
2.) cel przetwarzania,
3.) opis kategorii osób,
4.) opis kategorii danych,
5.) podstawę prawną przetwarzania,
6.) sposób zbierania danych,
7.) opis kategorii odbiorców danych (w tym przetwarzających),
8.) informację o przekazaniu poza EU/EOG, jeśli dotyczy;
9.) ogólny opis technicznych i organizacyjnych środków ochrony danych.

10.5 Wzór rejestru stanowi Załącznik nr 9 do PB PWSIiP – Wzór Rejestru Czynności Przetwarzania. Wzór rejestru zawiera także kolumny nieobowiązkowe. W kolumnach nieobowiązkowych rejestruje się w miarę potrzeb i możliwości informacje, z uwzględnieniem tego, że pełniejsza treść rejestru ułatwia zarządzanie zgodnością ochrony danych i rozliczenie się z niej.

11. Analiza ryzyka

11.1 Procedura opisuje sposób przeprowadzenia analizy ryzyka w celu zabezpieczenia danych osobowych adekwatnie do zidentyfikowanych zagrożeń wynikających z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych.

11.2 Opis procedury zawarty jest w Załączniku Nr 10 do PB PWSIiP.

12. Ocena skutków dla ochrony danych

12.1 Ocena skutków jest formalną, określoną w art. 35 Rozporządzenia procedurą przeprowadzenia analizy ryzyka - jeżeli dany rodzaj przetwarzania może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych - za wykonanie której odpowiada Administrator.

12.2 Ocena skutków powinna być wykonana przy współudziale Inspektora Ochrony Danych.

Część II. Zabezpieczenia fizyczne, techniczne, logiczne i procedury

Część druga dokumentu stanowi zestaw procedur dedykowanych zasadom zabezpieczania danych osobowych i opisuje w szczególności sposób zarządzania systemami informatycznymi służącymi do przetwarzania tych danych w Państwowej Wyższej Szkole Informatyki i Przedsiębiorczości w Łomży wskazując jednocześnie pozostałe sposoby ich zabezpieczenia przed przypadkowym lub niezgodnym z prawem zniszczeniem, utratą, modyfikacją, nieuprawnionym ujawnieniem oraz nieuprawnionym dostępem.

1. Zabezpieczenia fizyczne pomieszczeń z danymi osobowymi w wersji papierowej i elektronicznej.

1.1 W celu zapewnienia bezpieczeństwa przetwarzania danych w PWSIiP w Łomży stosuje się między innymi następujące rozwiązania:

1.) budynki PWSIiP są objęte ochroną przeciwpożarową oraz chronione przez alarmowy system antywłamaniowy;
2.) w budynkach funkcjonują portiernie;
3.) klucze do pomieszczeń pobierane są z portierni;
4.) pobranie i zwrot klucza odnotowywane jest w książce pobrań lub rejestrowane elektronicznie w programie SYSTEM_KLUCZY.
5.) kontrolowane jest otwieranie i zamykanie pomieszczeń, w których są przetwarzane dane osobowe, poprzez otwieranie pomieszczenia przez pierwszą osobę, która rozpoczyna pracę oraz zamykanie pomieszczenia przez ostatnią wychodzącą osobę i niepozostawianie pomieszczenia w czasie pracy bez nadzoru;
6.) dokumenty i wydruki trwałe z danymi osobowymi przechowuje się w archiwum lub w zabezpieczonych fizycznie pomieszczeniach, biurkach i szafach.

1.2 Zabezpieczenia fizyczne opisane są w sposób szczegółowy w Załączniku Nr 6 - Wykaz budynków i pomieszczeń stanowiących obszar przetwarzania danych osobowych w PWSIiP w Łomży.

2. Zabezpieczenia techniczne

2.1 W celu ochrony danych osobowych przetwarzanych w PWSIiP w Łomży stosuje się między innymi następujące zabezpieczenia techniczne:

1.) zastosowano monitoring wizyjny w obrębie obiektów i w otoczeniu;
2.) serwerownia wyposażona jest w system gaszenia (gaśnice);
3.) monitoring środowiskowy w serwerowni - czujnik temperaturowy, dymu, wilgotności;
4.) klimatyzacja w serwerowni;
5.) podłoga techniczna w serwerowni;
6.) powiadamianie e-mailem i sms o alertach;
7.) wszystkie komputery, na których są przetwarzane dane osobowe, są zaopatrzone w urządzenia typu UPS podtrzymujące zasilanie, a tym samym zabezpieczające SI przed utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej.

2.2 Szczegółowe informacje na temat zabezpieczeń technicznych zawarte są w Załączniku Nr 12 do PB PWSIiP Wykaz zabezpieczeń.

3. Zabezpieczenia infrastruktury informatycznej

3.1 W celu ochrony danych osobowych przetwarzanych w PWSIiP w Łomży stosuje się następujące metody:

1.) Konta użytkowników zabezpieczone hasłem.
2.) Dostęp do komputerów zainstalowanych w obszarze przetwarzania danych możliwy jest po zalogowaniu do systemu operacyjnego.
3.) Użytkownicy komputerów zainstalowanych w obszarze przetwarzania danych posiadają ograniczone uprawnienia do zasobów systemu operacyjnego.
4.) Na komputerach zainstalowanych w obszarze przetwarzania danych uruchomione jest oprogramowanie antywirusowe.
5.) Komunikacja między siecią lokalną, a siecią publiczną jest separowana za pomocą urządzeń typu Firewall z funkcjonalnościami filtrowania antyspamowego i antywirusowego.

6.) Możliwość wglądu w pełny zestaw danych osobowych oraz ich modyfikacji ograniczono tylko do komputerów zainstalowanych w pomieszczeniach stanowiących obszar przetwarzania danych.
7.) W systemach dostępnych z sieci publicznej istnieje jedynie możliwość wglądu w podstawowe dane identyfikacyjne typu imię, nazwisko, nr indeksu, nr telefonu, adres e-mail, w celach komunikacyjnych oraz przypisywania innych informacji np. wysyłanie wiadomości tekstowych, wpisywanie ocen, przydzielanie zadań, materiałów dydaktycznych i testów.
8.) Stosuje się zabezpieczenia kryptograficzne aplikacji dostępnych z sieci publicznej.
9.) Ogranicza się do niezbędnego minimum ilość interfejsów, do których można inicjować komunikację z sieci publicznej.
10.) W uzasadnionych sytuacjach możliwy jest zdalny dostęp do zasobów w obszarze przetwarzania danych za pomocą szyfrowanych połączeń VPN z użyciem technik pulpitu zdalnego, w celu wyeliminowania przesyłania danych na komputer znajdujący się poza obszarem przetwarzania danych. Dostęp zdalny realizowany jest na podstawie „Regulaminu Sieci Komputerowej PWSIiP w Łomży”.
11.) Wykonywane są regularnie kopie zapasowe zbiorów zawierających dane osobowe.

3.2 Szczegółowe informacje na temat zabezpieczeń systemu informatycznego zawarte są w Załączniku Nr 12 do PB PWSIiP - Wykaz zabezpieczeń.

4. Stosowane metody i środki uwierzytelniania

4.1 Podstawową metodą uwierzytelniania użytkowników w systemach komputerowych służących do przetwarzania danych osobowych są konta użytkowników. Konto składa się z identyfikatora użytkownika i hasła. W zależności od systemu dla danego konta można stosować zamiennie identyfikatory użytkownika (np. adres e-mail, numer indeksu, PESEL) z zachowaniem kontroli właściwego hasła.

4.2 Identyfikator użytkownika jest jawny i może być nadawany przez administratora właściwego systemu informatycznego indywidualnie, generowany automatycznie lub wyznaczany na podstawie zapisanych danych użytkownika (np. adres e-mail, nr indeksu), w zależności od specyfiki systemu komputerowego i uwierzytelniania użytkowników.

4.3 Identyfikator użytkownika, który stracił prawo do przetwarzania danych, należy niezwłocznie zablokować lub zmodyfikować uprawnienia w taki sposób, aby przetwarzanie nie było możliwe w systemie, do którego odwołano uprawnienia.

4.4 Ważność identyfikatora użytkownika w systemie służącym do przetwarzania danych, może być określana przez ASI na podstawie informacji zawartych na upoważnieniu lub na podstawie danych kadrowych, tj. dacie rozpoczęcia i zakończenia umowy o pracę lub zlecenia.

4.5 W przypadku utraty uprawnień użytkownika do przetwarzania danych, w/w identyfikatora nie można przydzielać innej osobie.

4.6 Hasło użytkownika powinno spełniać następujące wymagania:

1.) hasło nie może być jednakowe z identyfikatorem użytkownika i nie może zawierać danych personalnych (np. imienia, nazwiska, daty urodzenia użytkownika),
2.) hasło musi składać się z co najmniej 8 znaków, zawierać małe i wielkie litery oraz cyfry lub znaki specjalne,
3.) hasło musi być unikalne i nie powinno być powtarzane.

4.7 Hasło nie może być wyświetlane na ekranie w trakcie wpisywania. Użytkownik zobowiązany jest do zachowania hasła w tajemnicy, również po ustaniu jego ważności.

4.8 Hasło użytkownika musi być zmieniane nie rzadziej niż co 30 dni. Jeżeli zmiana nie jest w tym czasie możliwa, to należy wykonać ją w najbliższym możliwym terminie. Zasada ta nie dotyczy kont systemowych służących do automatycznej wymiany danych między systemami.

4.9 Hasła głównych kont systemowych, kont administracyjnych, interfejsów wymiany danych mogą być znane administratorom systemu i mają oni obowiązek zachowania ich w tajemnicy.

4.10 W przypadku złamania poufności hasła, użytkownik zobowiązany jest do jego natychmiastowej zmiany oraz do zgłoszenia tego faktu IOD oraz ASI.

4.11 W przypadku, gdy użytkownik zapomniał hasła, powinien:

1.) samodzielnie wykonać procedurę resetowania hasła pod warunkiem, że aplikacja udostępnia taką funkcjonalność i istnieje możliwość dodatkowej weryfikacji tożsamości użytkownika,

2.) zgłosić się do właściwego ASI w celu zresetowania hasła. Hasło wpisane przez ASI powinno być niezwłocznie zmienione przez użytkownika.

4.12 Zabrania się przesyłania haseł jawnym tekstem w wiadomościach e-mail.

5. Procedura nadawania uprawnień do przetwarzania danych osobowych i przebywania w obszarze przetwarzania danych i rejestrowania tych uprawnień

5.1 Upoważnienia do przetwarzania danych osobowych nadawane są w związku z wykonywaniem przez upoważnioną osobę obowiązków lub zadań związanych z przetwarzaniem danych osobowych.

5.2 Upoważnienia nadaje i odwołuje, w imieniu Administratora, Inspektor Danych Osobowych na podstawie wniosku kierownika właściwej komórki organizacyjnej, kierownika/koordynatora projektu, kierownika pionu organizacyjnego lub Kierownika Działu Spraw Osobowych. Wzór wniosku stanowi Załącznik Nr 14 do PB PWSIiP. Wykaz programów służących do przetwarzania danych osobowych wraz ze wskazaniem administratorów zawiera Załącznik nr 8 do PB w PWSIiP.

5.3 Przed nadaniem upoważnienia, IOD zobowiązany jest do sprawdzenia, czy osoba upoważniona:

1.) została przeszkolona z zakresu przestrzegania zasad bezpieczeństwa danych osobowych oraz zapoznana z Polityką Bezpieczeństwa,
2.) będzie przetwarzać dane osobowe w zakresie i celu określonym w upoważnieniu,
3.) podpisała oświadczenie o zachowaniu poufności.

5.4 Podpisane oświadczenia o poufności są przechowywane w aktach osobowych pracowników, bądź dołączane do umów cywilnoprawnych zawieranych ze współpracownikami. Wzór oświadczenia o poufności zawiera Załącznik Nr 15 do PB PWSIiP.

5.5 W przypadku zmiany stanowiska pracy, wydanie nowego upoważnienia jest konieczne, jeżeli zmianie ulega zakres czynności przetwarzania i cel przetwarzania danych przez pracownika posiadającego upoważnienie.

5.6 Upoważnienie, bądź jego odwołanie sporządzane są na piśmie w dwóch egzemplarzach – do akt pracownika/osoby zatrudnionej na podstawie umowy zlecenia oraz dla IOD. Nie wymaga się złożenia podpisu przez osobę upoważnianą. Wzór upoważnienia/odwołania upoważnienia stanowią Załączniki Nr 16 i Nr 17 do PB PWSIiP.

5.7 W sytuacjach wyjątkowych (np. stan zagrożenia dla ochrony danych osobowych, nieobecność IOD) upoważnienie może odwołać kierownik komórki organizacyjnej, kierownik/koordynator projektu, kierownik pionu organizacyjnego lub Kierownik Działu Spraw Osobowych. Decyzja kierownika wymaga akceptacji IOD, dokonanej w najbliższym możliwym terminie.

5.8 Wydane upoważnienia do przetwarzania danych osobowych oraz ich odwołanie, rejestrowane są w rejestrze osób upoważnionych do przetwarzania danych osobowych. Wzór rejestru osób upoważnionych do przetwarzania danych osobowych stanowi Załącznik Nr 18 PB PWSIiP. Rejestr osób upoważnionych prowadzi IOD.

5.9 Czynności konfiguracyjne związane z przydzieleniem lub odebraniem praw do wykonywania czynności przetwarzania w danym zbiorze danych, lub programach do przetwarzania danych wykonuje administrator właściwego systemu informatycznego na podstawie przedstawionego upoważnienia/odwołania upoważnienia, lub rejestru osób upoważnionych.

5.10 Osoby sprzątające pomieszczenia po godzinach pracy, mogą zostać dopuszczone do przebywania w pomieszczeniach, gdzie przetwarzane są dane osobowe po odbyciu przeszkolenia z zasad ochrony danych osobowych i podpisaniu oświadczenia o poufności, o których mowa w pkt 5.3. 1) i 3). Wzór upoważnienia do przebywania w obszarze przetwarzania danych stanowi Załącznik Nr 19 do PB PWSIiP. Z wnioskiem o udzielenie upoważnienia

występują kierownicy jednostek zatrudniających pracownika lub zlecających prace.

6. Instrukcja postępowania w przypadku naruszenia ochrony danych osobowych w PWSIiP w Łomży (postępowanie z incydentami)

6.1 Instrukcja w sprawie postępowania w przypadku naruszenia ochrony danych określa tryb postępowania w przypadku, gdy ujawniono naruszenie bezpieczeństwa informacji w PWSIiP w Łomży. Szczegółowy opis procedury zawiera Załącznik Nr 20 do PB PWSIiP.

6.2 Każda osoba upoważniona do przetwarzania danych osobowych oraz zobowiązana do zachowania poufności danych osobowych, w przypadku stwierdzenia zagrożenia lub naruszenia ochrony danych osobowych, zobowiązana jest poinformować o tym fakcie bezpośredniego przełożonego lub Inspektora Ochrony Danych. Wzór zgłoszenia zawiera Załącznik Nr 21 do PB PWSIiP - Meldunek o naruszeniu bezpieczeństwa.

6.3 Celem procedury jest minimalizacja skutków wystąpienia incydentów zagrażających bezpieczeństwu oraz ograniczenie ryzyka powstania zagrożeń i występowania incydentów w przyszłości.

6.4 W celu zapewnienia zgodności z przepisami prawa, Administrator dokumentuje wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia, jego skutki oraz podjęte działania zaradcze. Wzór prowadzonego przez Administratora Rejestru naruszeń ochrony danych zawiera Załącznik Nr 22 do PB PWSIiP.

7. Sposób przepływu danych pomiędzy poszczególnymi systemami

7.1 Przetwarzanie danych osobowych w PWSIiP w Łomży odbywa się z wykorzystaniem systemów informatycznych wykonanych w różnych technologiach, przechowujących informacje w różnych systemach zarządzania bazą danych. W celu ograniczenia ilości pracy związanej wprowadzaniem danych oraz z eliminacją błędów, które mogą być popełniane przez użytkowników, stosuje się techniki integracji systemów informatycznych, zapewniające przepływ danych między systemami. Przepływ danych pomiędzy poszczególnymi systemami może odbywać się za pomocą plików tekstowych,

komunikacji bezpośredniej z wykorzystaniem interfejsów SQL lub komunikacji pośredniej z wykorzystaniem interfejsów typu API.

7.2 Sposób przepływu danych osobowych pomiędzy systemami, w których przetwarzane są dane osobowe przedstawiono w załączniku pod nazwą Sposób przepływu danych, którego wzór stanowi Załącznik Nr 23 do PB PWSIiP.

7.3 Przetwarzanie danych osobowych w PWSIiP w Łomży realizowane jest w różnych systemach informatycznych, dostępnych również poza podstawowym obszarem przetwarzania danych. W związku z dostępnością niektórych systemów z sieci publicznej stosuje się wysoki poziom zabezpieczenia systemów informatycznych służących do przetwarzania danych osobowych.

8. Sposób zabezpieczenia systemu informatycznego, sposób i miejsce przechowywania elektronicznych nośników danych i kopii zapasowych

Informacje dotyczące tego zagadnienia zawiera Załącznik Nr 24 do PB PWSIiP.

9. Procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych osobowych oraz procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania

Informacje dotyczące tego zagadnienia zawiera Załącznik Nr 25 do PB PWSIiP.

10. Procedura dostępu podmiotów zewnętrznych

10.1 Celem procedury jest zapewnienie bezpiecznego przetwarzania danych osobowych przez podmioty zewnętrzne, gdy cel i zakres tego przetwarzania określa Administrator.

10.2 W przypadku przekazywania zbioru danych osobowych zapisanych na nośnikach elektronicznych podmiotom zewnętrznym, zaleca się stosowanie następujących zasad bezpieczeństwa:

1.) Należy zabezpieczyć ten zbiór przed przejęciem przez osobę nieuprawnioną, za pomocą co najmniej pliku skompresowanego zabezpieczonego hasłem,

2.) Hasło nie może być zapisane na nośniku elektronicznym i może być znane tylko osobie wykonującej zabezpieczenie, osobie odbierającej zbiór oraz IOD, przy czym hasło powinno być podane adresatowi inną drogą,

3.) Adresat powinien zostać powiadomiony o przesyłce,
4.) Należy stosować bezpieczne koperty depozytowe,
5.) Przesyłkę należy przekazać osobiście do rąk osoby odbierającej lub przesłać za pośrednictwem firmy kurierskiej.

10.3 Z podmiotami zewnętrznymi przetwarzającymi na polecenie Administratora dane osobowe zawiera się Umowę powierzenia przetwarzania danych.

10.4 Podmiot zewnętrzny zobowiązany jest do zachowania poufności powierzonych danych i przetwarzania ich zgodnie z celem umowy. Wzór umowy powierzenia przetwarzania danych zawiera Załącznik Nr 28 do PB PWSIiP w Łomży.

10.5 Inspektor Ochrony Danych prowadzi rejestr podmiotów zewnętrznych, które Administrator upoważnił do przetwarzania danych osobowych. Wzór rejestru zawiera Załącznik Nr 29 do PB PWSIiP w Łomży.

11. Postanowienia końcowe

11.1 Polityka Bezpieczeństwa wraz z załącznikami jest dokumentem wewnętrznym i nie może być udostępniania osobom i instytucjom postronnym w żadnej formie bez zgody Administratora.

11.2 Polityka Bezpieczeństwa może być udostępniania osobom i instytucjom postronnym bez zgody Administratora, jeżeli nie zawiera w treści informacji o zabezpieczeniach danych osobowych, a wszelkie załączniki występują w formie niewypełnionych szablonów.

11.3 Osoby przetwarzające dane osobowe, zarówno pracownicy w rozumieniu Kodeksu Pracy, jak i osoby świadczące pracę na podstawie umów cywilnoprawnych, stażyści oraz inne osoby mające dostęp do informacji podlegających ochronie, zobowiązane są do stosowania postanowień zawartych w niniejszej Polityce Bezpieczeństwa.

11.4 Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu potraktowane będą jako ciężkie naruszenie obowiązków pracowniczych.

11.5 W sprawach nieuregulowanych w niniejszej Polityce Bezpieczeństwa mają zastosowanie przepisy Rozporządzenia 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 dnia 04.05.2016 r. oraz ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. 2018, poz.1000)

Część III. Spis załączników do Polityki Bezpieczeństwa:

Załącznik Nr 1 - Wzór rejestru oświadczeń o wyrażeniu zgody

Załącznik Nr 2 - Zasady wykonywania obowiązków informacyjnych i obsługi żądań

Załącznik Nr 3 - Wzór upoważnienia dla IOD

Załącznik Nr 4 - Instrukcja w sprawie zasad postępowania przy przetwarzaniu danych osobowych w PWSIiP w Łomży

Załącznik Nr 5 - Wzór rejestru odbiorców danych osobowych

Załącznik Nr 6 - Wzór wykazu budynków i pomieszczeń stanowiących obszar przetwarzania danych

Załącznik Nr 7 - Wzór wykazu zbiorów danych osobowych

Załącznik Nr 8 - Wzór programów zastosowanych do przetwarzania danych osobowych

Załącznik Nr 9 - Wzór rejestru czynności przetwarzania

Załącznik Nr 10 - Procedura analizy ryzyka

Załącznik Nr 11 - Wzór wykazu zagrożeń

Załącznik Nr 12 - Wzór wykazu zabezpieczeń

Załącznik Nr 13 - Wzór arkusza analizy ryzyka

Załącznik Nr 14 - Wzór wniosku o nadanie uprawnień

Załącznik Nr 15 - Oświadczenie o poufności

Załącznik Nr 16 - Wzór upoważnienia do przetwarzania danych

Załącznik Nr 17 - Wzór odwołania upoważnienia do przetwarzania danych

Załącznik Nr 18 - Wzór rejestru osób upoważnionych do przetwarzania danych

Załącznik Nr 19 - Wzór upoważnienia do przebywania w obszarze przetwarzania danych

Załącznik Nr 20 - Instrukcja postępowania w przypadku naruszenia ochrony danych osobowych

Załącznik Nr 21 - Wzór meldunku o naruszeniu bezpieczeństwa

Załącznik Nr 22 - Wzór rejestru naruszeń

Załącznik Nr 23 - Wzór sposób przepływu danych

Załącznik Nr 24 - Procedury - Sposób zabezpieczenia systemu informatycznego

Załącznik Nr 25 - Procedury wykonywania przeglądów i konserwacji systemów oraz nośników

Załącznik Nr 26 - Wzór dziennika eksploatacji systemu

Załącznik Nr 27 - Procedury wykonywania kopii zapasowych

Załącznik Nr 28 - Wzór umowy powierzenia przetwarzania danych

Załącznik Nr 29 - Wzór rejestru podmiotów zewnętrznych

Załącznik Nr 30 - Wzór rejestru kategorii czynności przetwarzania.