Zarządzenie Nr 40/2019
Rektora Państwowej Uczelni Zawodowej
im. Ignacego Mościckiego w Ciechanowie
z dnia 01 października 2019r.

w sprawie: wprowadzenia nowego brzmienia Wewnętrznej Polityki Bezpieczeństwa Danych Osobowych

Na podstawie:

- art. 23 ust. 1 ustawy z dnia 20 lipca 2018r. Prawo o szkolnictwie wyższym i nauce (tj. Dz. U. 2018 poz. 1668 z późn. zm.)
- § 37 ust.1 Statutu Państwowej Uczelni Zawodowej im. Ignacego Mościckiego w Ciechanowie

zarządzam, co następuje:

§1

Wprowadzam nowe brzmienie Wewnętrznej Polityki Danych Osobowych w Państwowej Uczelni Zawodowej im. Ignacego Mościckiego w Ciechanowie, stanowiące załącznik do zarządzenia.

§ 2

Uchylam zarządzenie nr 5/2018 Rektora Państwowej Wyższej Szkoły Zawodowej w Ciechanowie z 25 maja 2018r. w wprowadzające Wewnętrzną Politykę Danych Osobowych w Państwowej Wyższej Szkole Zawodowej w Ciechanowie.

§ 3

Zarządzenie wchodzi w życie z dniem podpisania.

REKTOR
prof. nadzw. dr hab. Leszek Zygner

r. pr. Nadratowska-Malinowska

Załącznik
do Zarządzenia Rektora PUZ im. Ignacego Mościckiego w Ciechanowie
nr 40/2019 z dnia 01.10.2019r.

WEWNĘTRZNA POLITYKA BEZPIECZEŃSTWA DANYCH OSOBOWYCH

PAŃSTWOWA UCZELNIA ZAWODOWA
im. Ignacego Mościckiego w Ciechanowie

Ciechanów, październik 2019 r.

Spis treści

DEKLARACJA KIEROWNICTWA

Najwyższe kierownictwo Państwowej Uczelni Zawodowej im. Ignacego Mościckiego w Ciechanowie (zwanej dalej PUZIM), traktując informację, jako newralgiczny zasób każdej organizacji, świadome zagrożeń wynikających z postępującego rozwoju technologii przetwarzania danych osobowych w systemach informatycznych wprowadza System Zarządzania Bezpieczeństwem Informacji.
Przez bezpieczeństwo informacji rozumie się zapewnienie bezpiecznej dostępności, zabezpieczenie przed nieuprawnionym dostępem, naruszeniem integralności bądź zniszczeniem aktywów związanych z przechowywaniem i przetwarzaniem informacji.

Bezpieczeństwo informacji, a także systemów, w których są one przetwarzane, zapewnienie poufności danych wrażliwych i dostępności wymaganych informacji stanowią priorytetowe cele uczelni oraz gwarancję jej ciągłego rozwoju.

Państwowa Uczelnia Zawodowa im. Ignacego Mościckiego w Ciechanowie przetwarza informacje stanowiące dane osobowe w rozumieniu w rozumieniu art. 4 rozporządzenia Parlamentu Europejskiego i Radu UE z dnia 27 kwietnią 2016r. 2016/679 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 rozporządzenia o ochronie danych); zwane dalej „rozporządzenie RODO".
W celu udokumentowania realizacji Systemu Bezpieczeństwa Danych Osobowych Rektor PUZ im. Ignacego Mościckiego w Ciechanowie zatwierdza i wprowadza Wewnętrzną Politykę Bezpieczeństwa Danych Osobowych.

Wewnętrzna Polityka Bezpieczeństwa Danych Osobowych stanowi ramy do ustalania celów oraz zadań w odniesieniu do wdrażanego w Uczelni systemu zapewnienia bezpieczeństwa przetwarzanych danych osobowych zgodnie z obowiązującymi wymogami prawa.
Rektor deklaruje pełne zaangażowanie przy realizacji wszelkich działań zmierzających do zapewnienia bezpieczeństwa przetwarzanych danych osobowych, a tym samym spełnienie wymaganego poziomu bezpieczeństwa systemów informacyjnych oraz podejmuje się uświadamiania podległym mu pracownikom wagi prowadzonych działań mających na celu zabezpieczenie danych osobowych oraz ich roli w systemie.

Ponadto Rektor Państwowej Uczelni Zawodowej im. Ignacego Mościckiego w Ciechanowie deklaruje nadzór nad działaniem wprowadzonego systemu, jego aktualizację oraz odpowiednią reakcję w przypadkach zdarzeń zagrażających bezpieczeństwu danych osobowych w uczelni, a także zapewnienie środków niezbędnych do realizacji systemu bezpieczeństwa.
Zasady, kompetencje oraz zakresy odpowiedzialności opisane w Wewnętrznej Polityce Bezpieczeństwa Danych Osobowych obowiązują wszystkich pracowników Państwowej

Uczelni Zawodowej im. Ignacego Mościckiego w Ciechanowie oraz pozostałe osoby wykonujące pracę na podstawie umowy zlecenia lub innej umowy cywilno-prawnej, a także osoby odbywająca wolontariat, praktykę lub staż.

Prowadzona Wewnętrzna Polityka Bezpieczeństwa Danych Osobowych jest w pełni zgodna z wymaganiami obowiązujących przepisów prawa oraz będzie nieustannie nadzorowana i doskonalona.

1. WYKAZ PODSTAWOWYCH SKRÓTÓW

Skrót	Opis
u.o.d.o.	Ustawa z dnia 10 maja 2018r. o ochronie danych osobowych (Dz. U. 2018r, poz. 1000).
RODO	Rozporządzenie Parlamentu Europejskiego i Radu UE z dnia 27 kwietnią 2016r. 2016/679 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE
PUODO	Prezes Urzędu Ochrony Danych Osobowych
ADO	Administrator Danych Osobowych
IOD	Inspektor Ochrony Danych
LADO	Lokalny Administrator Bezpieczeństwa Informacji
ASI	Administrator Systemów Informatycznych
SI	System Informatyczny
SBDO	System Bezpieczeństwa Danych Osobowych
WPBDO	Wewnętrzna Polityka Bezpieczeństwa Danych Osobowych
PUZIM	Państwowa Uczelnia Zawodowa im. Ignacego Mościckiego w Ciechanowie

2. WYKAZ PODSTAWOWYCH DEFINICJI

Ilekroć w niniejszej Wewnętrznej Polityce Bezpieczeństwa Danych Osobowych mowa o:

1) **Komórce organizacyjnej** – rozumie się przez to odpowiednio wydziały, o których mowa w Regulaminie Organizacyjnym Państwowej Uczelni Zawodowej im. Ignacego Mościckiego w Ciechanowie (zwanej dalej: PUZIM).

2) **Kierowniku komórki organizacyjnej** – rozumie się przez to dziekana wydziału, działu, koordynatora i samodzielne stanowiska pracy;

3) **Administratorze Danych Osobowych** – rozumie się przez to Państwową Uczelnię Zawodową im. Ignacego Mościckiego w Ciechanowie, która decyduje o celach i środkach przetwarzania danych osobowych;

4) **Inspektor Ochrony Danych** – rozumie się przez to pracownika Państwowej Uczelni Zawodowej im. Ignacego Mościckiego w Ciechanowie / podmiot zewnętrzny wyznaczonego przez Administratora Danych Osobowych, monitorujący przestrzeganie zasad, o których mowa w art. 39 RODO;

6) **Administratorze Systemów Informatycznych** – rozumie się przez to pracownika uczelni, odpowiedzialnego za funkcjonowanie systemów i sieci teleinformatycznych oraz za przestrzeganie zasad i wymogów bezpieczeństwa systemów i sieci teleinformatycznych;

7) **Osobie upoważnionej** – rozumie się przez to osobę upoważnioną przez Administratora Danych Osobowych do przetwarzania danych osobowych. Użytkownikiem może być pracownik uczelni, osoba wykonująca pracę na podstawie umowy zlecenia lub innej umowy cywilno-prawnej, a także osoba odbywająca wolontariat, praktykę lub staż.

8) **Osobie nieupoważnionej** – rozumie się przez to osobę nieposiadającą upoważnienia do przetwarzania danych osobowych;

9) **Osobie nieuprawnionej** – rozumie się przez to osobę nieposiadającą uprawnień nadanych w systemie informatycznym uczelni;

10) **Danych osobowych** – rozumie się przez to informacje o zidentyfikowanej, lub możliwej do zidentyfikowania osobie fizycznej (możliwa do zidentyfikowania osoba fizyczna to osoba, którą może bezpośrednio lub pośrednio zidentyfikować), w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników

określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej;

11) **Zbiorze danych osobowych** – rozumie się przez to uporządkowany zestaw danych osobowych dostępny według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie;

12) **Przetwarzaniu danych osobowych** – rozumie się przez to operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adoptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie; przetwarzanie danych zgodne z prawem, rzetelnie i przejrzyste;

13) **Systemie informatycznym** – rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;

14) **Zabezpieczeniu danych w systemie informatycznym** – rozumie się przez to wdrożenie i eksploatację stosowanych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem;

15) **Bezpieczeństwie informacji** – rozumie się przez to zespół zasad, jakimi należy się kierować projektując oraz wykorzystując systemy i aplikacje służące do przetwarzania informacji by w każdych okolicznościach dostęp do nich był zgodny z założeniami;

16) **Usuwaniu danych** – rozumie się przez to zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą;

17) **Zgodzie osoby, której dane dotyczą** – rozumie się przez to oświadczenie woli, którego treścią jest zgoda na przetwarzanie danych osobowych tego, kto składa oświadczenie. Zgoda nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści. Zgoda może być odwołana w każdym czasie;

18) **Odbiorcy danych** – rozumie się przez to osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią. Organy publiczne, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem Unii lub prawem państwa

członkowskiego, nie są jednak uznawane za odbiorców; przetwarzanie tych danych przez te organy publiczne musi być zgodne z przepisami o ochronie danych mającymi zastosowanie stosownie do celów przetwarzania;

19) **Państwie trzecim** – rozumie się przez to państwo należące do Europejskiego Obszaru Gospodarczego;

20) **Haśle** – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych, znany jedynie użytkownikowi uprawnionemu do pracy w systemie informatycznym;

21) **Identyfikatorze użytkownika** – rozumie się przez to ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych w wyznaczonych przez Administratora Danych Osobowych obszarach systemu informatycznego uczelni;

22) **Teletransmisji danych** – rozumie się przez to przesyłanie informacji za pośrednictwem sieci telekomunikacyjnych;

23) **Poufności danych** – rozumie się przez to właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym osobom lub podmiotom;

24) **Adekwatność** – rozumie się przez to przetwarzanie danych stosowne lub ograniczone do tego, co niezbędne do celów, w których są przetwarzane (minimalizacja danych);

25) **Użytkowniku systemu informatycznego** – rozumie się przez to osobę upoważnioną do przetwarzania danych osobowych w systemach informatycznych, której nadano unikalny identyfikator i hasło;

26) **Uwierzytelnieniu** – rozumie się przez to proces poprawnej identyfikacji użytkownika systemu informatycznego w stopniu umożliwiającym przyznanie odpowiednich uprawnień lub przywilejów w systemie informatycznym uczelni;

27) **Sieci komputerowej** – rozumie się przez to grupę komputerów lub innych urządzeń połączonych ze sobą w celu wymiany danych lub współdzielenia różnych zasobów;

28) **Sieci lokalnej** – rozumie się przez to sieć przeznaczoną do łączenia ze sobą stanowisk komputerowych znajdujących się w uczelni;

29) **Punkcie dystrybucyjnym** – rozumie się przez to miejsce, w którym zlokalizowana jest infrastruktura teleinformatyczna oraz urządzenia umożliwiające dystrybucję połączeń sieciowych w systemie informatycznym;

30) **Stacji roboczej** – rozumie się przez to komputer użytkownika systemu informatycznego podłączony do sieci lokalnej uczelni;

31) **Naruszenie ochrony danych** – rozumie się przez to naruszenie bezpieczeństwa informacji ze względu na poufność, dostępność i integralność;

34) **Zagrożeniu** - rozumie się przez to potencjalną możliwość wystąpienia incydentu;

35) **Działa korygujące** – rozumie się przez to działanie przeprowadzone w celu wyeliminowania przyczyny incydentu lub innej niepożądanej sytuacji;

36) **Działanie zapobiegawcze** – rozumie się przez to działanie, które należy przedsięwziąć, aby wyeliminować przyczyny zagrożenia lub innej potencjalnej sytuacji niepożądanej.

3. WPROWADZENIE

Wewnętrzna Polityka Bezpieczeństwa Danych Osobowych określa reguły przetwarzania danych osobowych oraz sposobów ich zabezpieczenia, jako zestaw praw, zasad i zaleceń regulujących sposób ich zarządzania, ochrony i dystrybucji w Państwowej Uczelni Zawodowej im. Ignacego Mościckiego w Ciechanowie (zwanej dalej: PUZIM).

Polityka zawiera informacje dotyczące rozpoznawania procesów przetwarzania danych osobowych oraz wprowadzonych zabezpieczeń techniczno-organizacyjnych, zapewniających ochronę przetwarzanych danych osobowych.

Niniejszy dokument jest zgodny z obowiązującymi przepisami prawa, a w szczególności z rozporządzeniem Parlamentu Europejskiego i Radu UE z dnia 27 kwietnią 2016r. 2016/679 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE oraz ustawy z dnia 10 maja 2018r. o ochronie danych osobowych.

4. CELE WEWNĘTRZNEJ POLITYKI BEZPIECZEŃSTWA DANYCH OSOBOWYCH

Celem Wewnętrznej Polityki Bezpieczeństwa Danych Osobowych jest określenie oraz wdrożenie zasad bezpieczeństwa i ochrony danych osobowych przetwarzanych w PUZIM, a w szczególności:

1) zapewnienie spełnienia wymagań prawnych;

2) zapewnienie ochrony danych osobowych przed dostępem osób nieupoważnionych;
3) zapewnienie poufności, integralności oraz rozliczalności danych osobowych przetwarzanych w uczelni;
4) podnoszenie świadomości pracowników;
5) zaangażowanie pracowników uczelni w ochronę danych osobowych.

5. ZAKRES STOSOWANIA WEWNĘTRZNEJ POLITYKI BEZPIECZEŃSTWA

Zakresy określone przez Wewnętrzną Politykę Bezpieczeństwa Danych Osobowych mają zastosowanie do całego systemu informacyjnego PUZIM, a w szczególności do:

1) wszelkich istniejących, wdrażanych obecnie lub w przyszłości systemów informatycznych oraz prowadzonych w formie tradycyjnej, w których przetwarzane są dane osobowe;
2) wszystkich nośników magnetycznych, optycznych lub papierowych, na których są lub będą znajdować się informacje zawierające dane osobowe;
3) informacji dotyczących zabezpieczenia danych osobowych, w tym w szczególności nazw kont i haseł w systemach przetwarzania danych osobowych;
4) wszelkich obszarów (budynki, pomieszczenia, części pomieszczeń), w których są lub będą przetwarzane dane osobowe;
5) informacji zawierających dane osobowe, których Administratorem Danych Osobowych jest PUZIM, a także informacji będących własnością Klientów lub Współpracowników uczelni uzyskanych na podstawie stosownie zawartych umów;
6) wszystkich pracowników PUZIM w rozumieniu przepisów Kodeksu Pracy, stażystów, praktykantów, wolontariuszy, w tym treści zawieranych umów;
7) wszystkich danych kandydatów do pracy zbieranych na etapie rekrutacji, a także innych podmiotów lub osób fizycznych, które współuczestniczą w procesie przetwarzania danych osobowych;
8) wszystkich danych kandydatów do podjęcia studiów w PUZIM zebranych na etapie rekrutacji, obecnych studentów i absolwentów;

6. PODSTAWA PRAWNA

Wewnętrzna Polityka Bezpieczeństwa Danych Osobowych odnosi się do sposobu przetwarzania danych osobowych oraz środków ich ochrony określonych w:

1) Rozporządzenie Parlamentu Europejskiego i Radu UE z dnia 27 kwietnią 2016r. 2016/679 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE,

2) Ustawie z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. 2018 poz. 1000);

3) Szczegółowych przepisów dotyczących danych osobowych i ich przetwarzania.

7. STRUKTURA WEWNĘTRZNEJ POLITYKI BEZPIECZEŃSTWA DANYCH OSOBOWYCH

Zestaw dokumentów Polityki Bezpieczeństwa Danych Osobowych składa się z:
1) Wewnętrznej Polityki Bezpieczeństwa Danych Osobowych w PUZIM;
2) Wykazu budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe;
3) Wykazu zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych;
4) Rejestr czynności przetwarzania danych
5) Wzorów formularzy pomocniczych.

Wyżej wymienione dokumenty będą prowadzone w formie odrębnych dokumentów.

8. REJESTR CZYNNOŚCI PRZETWARZANIA DANYCH OSOBOWYCH

Administrator Danych Osobowych odpowiedzialny jest za prowadzenie Rejestru czynności przetwarzania danych osobowych.

Powyższy rejestr stanowi integralną część Wewnętrznej Polityki Bezpieczeństwa Danych Osobowych w PUZIM. Wykaz zbiorów prowadzony jest zarówno w formie papierowej jak i elektronicznej.

W rejestrze tym zamieszcza się następujące informacje:
a) imię i nazwisko lub nazwę oraz dane kontaktowe administratora oraz wszelkich współadministratorów, a także, gdy ma to zastosowanie – przedstawiciela administratora oraz inspektora danych osobowych;
b) cele przetwarzania;
c) opis kategorii osób, których dane dotyczą, oraz kategorii danych osobowych;

d) kategorii odbiorów, którym dane osobowe zostały lub zostaną ujawnione, w tym odbiorców w państwach trzecich lub w organizacjach międzynarodowych;
e) gdy ma to zastosowanie, przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwa tego państwa trzeciego lub organizacji międzynarodowej, a w przypadku przekazań, o których mowa w art. 49 ust. 1 akapit drugi, dokumentacja odpowiednich zabezpieczeń;
f) jeżeli jest to możliwe, planowane terminy usunięcia poszczególnych kategorii danych;
g) jeżeli jest to możliwe, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 32 ust. 1.

Zasoby zawierające dane osobowe przetwarzane metodami tradycyjnymi:

1) dane osobowe kandydatów do pracy.
2) dane osobowe pracowników.
3) dane osobowe byłych pracowników.
4) dane osobowe studentów.
5) dane osobowe absolwentów.
6) ewidencja akt osobowych.
7) ubezpieczenie ZUS i płace.
8) dokumentacja ubezpieczeniowa.
9) dokumentacja powypadkowa.
10) dane osobowe osób zatrudnionych na umowy cywilno – prawnych.
11) dane kontrahentów.

9. ZAKRES ROZPOWSZECHNIANIA

Z treścią niniejszej Wewnętrznej Polityki Bezpieczeństwa Danych Osobowych powinny zapoznać się wszystkie osoby mające dostęp do danych osobowych na podstawie nadanych upoważnień przez Administratora Danych Osobowych.
Dokument ten może być także udostępniany partnerom przetwarzającym dane osobowe PUZIM, z którym uczelnia związana jest odpowiednimi umowami.

7. OBOWIĄZKI ADMINISTRATORA DANYCH OSOBOWYCH

W zakresie zabezpieczenia danych osobowych do obowiązków ADO należy:

1) przetwarzanie danych osobowych zgodnie z prawem;
2) dopełnienie obowiązku informacyjnego ustanowionego w art. 13 oraz 14 RODO;

3) dołożenie szczególnej staranności w celu ochrony interesów osób, których dane dotyczą;
4) respektowanie prawa osób, których dane dotyczą;
5) stosowanie środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności do zabezpieczenia danych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem;
7) wydawanie i odbieranie upoważnień do przetwarzania danych;
8) prowadzenie ewidencji wydanych upoważnień do przetwarzania danych osobowych;
9) podejmowanie działań w przypadku wykrycia naruszeń w systemie bezpieczeństwa danych osobowych;
10) kontrolowanie, jakie dane, kiedy i przez kogo zostały wprowadzone do zbioru i komu są przekazywane;
11) udzielanie informacji o zakresie przetwarzanych danych osobowych;
12) spełnienie obowiązku uzupełniania, uaktualnienia, sprostowania danych, czasowego lub stałego wstrzymania przetwarzania kwestionowanych danych lub ich usunięcia ze zbioru, gdy zażąda tego osoba, której dane są przetwarzane;
13) zapewnienie środków finansowych niezbędnych do ochrony danych osobowych;
14) udzielanie upoważnień do realizacji powyższych obowiązków pracownikom, współpracownikom PUZIM.

8. WYZNACZENIE INSPEKTORA OCHRONY DANYCH (IOD)

1) administrator Danych Osobowych może wyznaczyć Inspektora Ochrony Danych (IOD).
2) IOD jest wyznaczany na podstawie kwalifikacji zawodowych, a w szczególności wiedzy fachowej na temat praw i praktyk w dziedzinie ochrony danych oraz umiejętności wypełniania zadań, o których mowa w art. 39 RODO.
3) administrator Danych publikuje dane kontaktowe IOD i zawiadamia o nich Prezesa Urzędu Ochrony Danych obowiązany do zachowania tajemnicy lub poufności, co do wykonania swoich zadań.

Obowiązki Inspektora Ochrony Danych.

1) informowanie Administratora, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy rozporządzenia RODO oraz innych przepisów Unii lub ustawy UODO i doradzanie im na tej podstawie,

2) monitorowanie przestrzegania przepisów rozporządzenia RODO, innych przepisów Unii lub ustawy UODO oraz polityk administratora lub podmiotu przetwarzającego w dziedzinie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty.
3) udzielanie na żądanie zaleceń, co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania zgodnie z art. 35 RODO;
4) współpraca z Prezesem Urzędu Ochrony Danych Osobowych.
5) pełnienie funkcji punktu kontaktowego dla prezesa Urzędu Ochrony Danych Osobowych w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w art. 36 RODO, oraz w stosownych przypadkach prowadzenia konsultacji we wszelkich innych sprawach.

12. ODPOWIEDZIALNOŚĆ ZA BEZPIECZEŃSTWO DANYCH OSOBOWYCH

Za bezpieczeństwo danych osobowych w PUZIM odpowiadają:
1) administrator danych osobowych.
2) inspektor ochrony danych.
3) osoby upoważnione do przetwarzania danych.
4) administrator systemów informatycznych.

Administrator danych osobowych

1) administrator jest odpowiedzialny za przestrzeganie przepisów Art. 5 ust. 1 RODO;
2) dane osobowe przetwarzane przez Administratora muszą być:
   a) przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą („zgodność z prawem, rzetelność i przejrzystość");
   b) dane osobowe zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzanie dalej w sposób niezgodny z tymi celami;
   c) adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane („minimalizacja danych"),
   d) przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą prze okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane; pod warunkiem, że wdrożone zostaną odpowiednie środki techniczne i organizacyjne w celu ochrony praw i wolności osób, których dane dotyczą („ograniczenie przechowywania");
   e) przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za

pomocą odpowiednich środków technicznych i organizacyjnych („integralność i poufność"),

Inspektor Ochrony Danych

Inspektor Ochrony Danych odpowiedzialny jest za:

1) prowadzenie dokumentacji dotyczącej bezpieczeństwa danych;
2) prowadzenie i nadzorowanie korespondencji z prezesem Urzędu Ochrony Danych Osobowych;
3) prowadzenie rejestru czynności przetwarzania danych osobowych;
4) wydawanie i odbieranie upoważnień do przetwarzania danych;
5) sprawowanie nadzoru nad prawidłowym stosowaniem się do zasad i procedur określonych w wewnętrznej polityce bezpieczeństwa danych osobowych;
6) sprawowanie nadzoru nad fizycznym zabezpieczeniem obszarów przetwarzania danych osobowych oraz kontrolę przebywających w nich osób;
7) sprawowanie nadzoru nad naprawami, konserwacją oraz likwidacją urządzeń komputerowych, na których zapisane są dane osobowe;
8) sprawowanie nadzoru nad bezpieczeństwem danych osobowych zawartych na dyskach wymiennych, palmtopach, pamięciach przenośnych i innych nośnikach, a także w komputerach przenośnych;
9) sprawowanie nadzoru nad obiegiem oraz przechowywaniem dokumentacji zawierającej dane osobowe;
10) Sprawowanie nadzoru nad funkcjonowaniem mechanizmów uwierzytelniania użytkowników w systemach informatycznych oraz kontrolę dostępu do danych;
11) identyfikowanie i analizowanie zagrożeń oraz ryzyka, na które narażone mogą być dane osobowe przetwarzane prze administratora;
12) monitorowanie działania zabezpieczeń wdrożonych w celu ochrony danych osobowych;
13) przeprowadzanie kontroli w zakresie ochrony danych osobowych;
14) określanie potrzeb w zakresie zabezpieczenia danych osobowych;
15) podejmowanie odpowiednich działań w przypadkach naruszenia bezpieczeństwa danych osobowych;
16) prowadzenie rejestru naruszeń i zdarzeń wskazujących na naruszenie bezpieczeństwa danych osobowych;
17) zatwierdzanie procedur bezpieczeństwa i standardów zabezpieczeń wnioskowanych i obowiązujących w PUZIM;
18) dokonywanie modyfikacji i akceptacji proponowanych zmian, jak i okresowych kontroli polityk i procedur;
19) umożliwienie przeprowadzenia kontroli przez służby organu nadzorczego;
20) sprawowanie nadzoru nad procesem przyznawania praw dostępu;
21) organizowanie szkoleń z zakresu ochrony danych;

22) opiniowanie wzorów dokumentów i umów;
23) nadzorowanie osób upoważnionych do przetwarzania danych osobowych.

Administrator Systemów Informatycznych

Administrator Systemów Informatycznych odpowiedzialny jest za:

1) bieżący nadzór oraz zapewnienie ciągłości działania systemów informatycznych;
2) optymalizację wydajności systemów informatycznych;
3) zabezpieczenie systemów informatycznych;
4) zarządzanie konfiguracją systemów i urządzeń wchodzących w skład systemu informatycznego;
5) przeciwdziałanie próbom naruszenia bezpieczeństwa danych osobowych w systemach informatycznych;
6) dokonywanie okresowej analizy ryzyka i dokumentowanie tego dla poszczególnych systemów informatycznych wykorzystywanych do przetwarzania danych osobowych;
7) przyznawanie na wniosek Inspektora Ochrony Danych praw dostępu do określonych systemów informatycznych;
8) współpracę z dostawcami aplikacji i sprzętu komputerowego, w tym sieciowego i serwerowego;
9) wnioskowanie do Inspektora Ochrony Danych oraz współpraca w sprawie opracowywania / aktualizacji procedur bezpieczeństwa i standardów zabezpieczeń;
10) bieżące wykonywanie kopii systemowych, jak i kopii baz danych i aplikacji wykorzystywanych do przetwarzania danych osobowych;
11) świadczenie wsparcia technicznego w ramach oprogramowania oraz serwis sprzętu komputerowego wchodzącego w skład systemów informatycznych PUZIM;
12) prowadzenie dokumentacji dotyczącej opisu przepływu danych pomiędzy systemami informatycznymi zastosowanymi w celu przetwarzania danych osobowych.
13) prowadzenie ewidencji sprzętu i oprogramowania służącego do przetwarzania danych osobowych;
14) umożliwienie przeprowadzenia kontroli przez służby biura prezesa urzędu ochrony danych osobowych;
15) sprawowanie nadzoru nad systemem komunikacji w sieci komputerowej oraz przesyłaniem danych za pośrednictwem urządzeń teletransmisji;
16) wykonywanie likwidacji urządzeń komputerowych oraz elektronicznych nośników zawierających dane osobowe;
17) sprawowanie nadzoru nad profilaktyką antywirusową;
18) zapewnienie szkoleń pracowników PUZIM w zakresie prawidłowego korzystania z aplikacji i urządzeń wchodzących w skład systemów informatycznych służących do przetwarzania danych osobowych;
19) opiniowanie zakupów dotyczących oprogramowania sieciowego, serwerowego oraz narzędziowego.

Osoby upoważnione do przetwarzania danych osobowych

Osoby upoważnione do przetwarzania danych osobowych odpowiedzialne są za:

1) zapoznanie się z przepisami prawa w zakresie ochrony danych osobowych oraz postanowieniami niniejszej Wewnętrznej Polityki Bezpieczeństwa Danych Osobowych PUZIM;
2) stosowanie się do zaleceń inspektora ochrony danych w zakresie ich kompetencji;
3) przetwarzania danych osobowych wyłącznie w zakresie ustalonym indywidualnie w pisemnym upoważnieniu i tylko w celu wykonywania nałożonych obowiązków służbowych;
4) niezwłoczne informowanie inspektora ochrony danych o wszelkich nieprawidłowościach dotyczących bezpieczeństwa przetwarzanych danych osobowych;
5) ochronę danych osobowych oraz środków wykorzystywanych do przetwarzania danych osobowych przed nieuprawnionym dostępem, ujawnieniem, modyfikacją, zniszczeniem lub zniekształceniem;
6) korzystanie z systemów informatycznych w sposób zgodny ze wskazówkami zawartymi w instrukcjach obsługi urządzeń wchodzących w skład systemów informatycznych;
7) zachowanie w tajemnicy danych osobowych oraz przestrzeganie procedur ich bezpiecznego przetwarzania przez cały okres zatrudnienia, a także po ustaniu stosunku pracy lub odwołania z pełnionej funkcji;
8) wykonywania operacji w systemach informatycznych przy użyciu ich identyfikatora oraz hasła;
9) zachowanie szczególnej staranności w trakcie wykonywania operacji przetwarzania danych osobowych w celu ochrony interesów osób, których dane dotyczą.

13. PODSTAWOWE ZASADY OCHRONY DANYCH OSOBOWYCH

W niniejszym rozdziale wskazane zostały zasady ochrony danych osobowych stosowane w PUZIM.

1) administratorem Danych Osobowych (ADO), jest PUZIM w Ciechanowie, a w jej imieniu Rektor.
2) obowiązki wynikające z rozporządzenia RODO, ustawy o ochronie danych osobowych Rektor powierza:
   a) prorektorowi - w zakresie podległych mu pracowników,
   b) dziekanom - w zakresie podległych im pracowników, uczniów i studentów wydziału,
   c) kanclerzowi - w zakresie podległych mu pracowników

d) kierownikom pozostałych jednostek organizacyjnych - w zakresie podległych im pracowników.

3) dane przechowywane są w bazach danych i zbiorach tradycyjnych (dokumenty papierowe) i dokumentach elektronicznych zabezpieczonych przed dostępem niepowołanych osób wg zaleceń rozporządzenia RODO;
4) wszystkie dane osobowe w PUZIM należy przetwarzać zgodnie z obowiązującymi przepismi prawa;
5) w stosunku do osób, których dane osobowe są przetwarzane należy spełnić obowiązek informacyjny wynikający z przepisów RODO;
6) zebrane dane osobowe należy przetwarzać dla oznaczonych i zgodnych z prawem celów i nie poddawać dalszemu przetwarzaniu niezgodnemu z tymi celami;
7) należy zadbać, aby przetwarzanie danych osobowych odbywało się zgodnie z zasadami dotyczącej merytorycznej poprawności oraz adekwatnie do celów, w jakich zostały zebrane;
8) przetwarzane dane osobowe należy przechowywać w postaci umożliwiającej identyfikację osób, których te dane dotyczą;
9) dane osobowe w PUZIM można przetwarzać nie dłużej niż jest to niezbędne do osiągnięcia celu ich przetwarzania;
10) przetwarzane dane osobowe nie mogą być udostępniane bez zgody osób, których dane dotyczą, chyba że udostępnia się te dane osobom, których dane dotyczą, osobom upoważnionym do przetwarzania danych osobowych, podmiotom przetwarzającym, którym przekazano dane na podstawie umowy powierzenia oraz organom państwowym lub organom samorządu terytorialnego w związku z prowadzonym postępowaniem;
11) gromadzenie i przetwarzanie danych osobowych w systemie tradycyjnym (papierowym) odbywa się w odpowiednio zabezpieczonym miejscu.
12) pomieszczenia, w których przetwarza się dane osobowe zabezpieczone są przed dostępem osób nieuprawnionych, to znaczy posiadają odpowiednie zamki do drzwi oraz zabezpieczenie w oknach (w szczególności na parterze).
13) dokumenty i inne nośniki informacji zawierające dane osobowe zabezpieczone są przed dostępem osób nieupoważnionych do przetwarzania. Przechowywane są w szafach metalowych lub innym sprzęcie biurowym zamykanym na klucz lub posiadających inne, odpowiednie zabezpieczenia.
14) w zakresie danych osobowych przetwarzanych w innych systemach niż informatyczne, obowiązują nadal dotychczasowe przepisy o tajemnicy służbowej, obiegu i zabezpieczaniu dokumentów służbowych;
15) wszystkim osobom, których dane są przetwarzane przysługuje prawo do ochrony danych ich dotyczących, do kontroli przetwarzania tych danych oraz do ich uaktualniania, usunięcia jak również do uzyskiwania wszystkich informacji o przysługujących im prawach.

14. UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH

Do przetwarzania danych osobowych i obsługi zbiorów informatycznych zawierających te dane mogą być dopuszczone wyłącznie osoby posiadające upoważnienie do przetwarzania danych osobowych wydane przez Inspektora Ochrony Danych z upoważnienia Administratora Danych Osobowych oraz złożyły stosowne oświadczenie dot. właściwej realizacji przepisów RODO (wzór oświadczenia stanowi załącznik).
Upoważnienie powinno mieć charakter imienny. Powinno też określać dozwolony okres i zakres przetwarzania danych. Upoważnienia mogą być wydawane bezterminowo (wynikające z treści umowy o pracę) lub na czas określony.

Inspektor Ochrony Danych z upoważnienia Administratora Danych Osobowych prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych (wzór ewidencji stanowi załącznik). Administrator Danych Osobowych zobowiązany jest do uzupełnienia zakresów obowiązków pracowników firmy o odpowiedzialność za ochronnę tych danych, zgodnie z przydzielonymi zadaniami.

15. POWIERZENIE PRZETWARZANIA DANYCH OSOBOWYCH

Administrator Danych Osobowych może zlecić innemu podmiotowi przetwarzanie danych osobowych w celu realizacji określonego zadania.

Powierzenie przetwarzania danych osobowych poza granice Rzeczpospolitej Polskiej wymaga zgody Administratora Danych Osobowych i odbywa się po sprawdzeniu wymagań prawnych obowiązujących w tym zakresie.

W sytuacji powierzenia przetwarzania danych osobowych podmiotowi zewnętrznemu, w umowie powierzenia przetwarzania danych osobowych określa się przede wszystkim:
1) cel i zakres przetwarzania danych osobowych;
2) obowiązek zachowania w tajemnicy danych osobowych oraz informacji o zabezpieczeniach tych danych;
3) konsekwencje prawne i kary finansowe wynikające z niestosowania się do warunków umowy;
4) wymagania bezpieczeństwa dla procesu przetwarzania danych osobowych.

W umowach powierzenia przetwarzania danych osobowych oraz w umowach, na podstawie, których dochodzi do wymiany informacji uwzględnić należy następujące elementy:

1) definicję informacji, która ma być chroniona;
2) spodziewany czas trwania umowy, włączając w to przypadki, w których obowiązek zachowania poufności może być bezterminowy;
3) odpowiedzialność i działania sygnatariuszy podejmowane w celu uniknięcia nieupoważnionego ujawnienia informacji;
4) własność informacji;
5) dozwolone użycie danych osobowych oraz praw sygnatariusza do jej użycia;
6) prawa do audytu i monitorowania działań związanych z ochroną danych osobowych;
7) proces powiadamiania i raportowania nieuprawnionego ujawnienia lub naruszenia poufności i integralności danych osobowych;
8) wymagane działania w momencie zakończenia umowy, np.: zasady zwrotu lub niszczenia danych osobowych przy zakończeniu umowy.

Powierzenie przetwarzania danych osobowych poza granice Rzeczpospolitej Polskiej wymaga zgody Administratora Danych Osobowych i odbywa się po sprawdzeniu wymagań prawnych obowiązujących w tym zakresie.

16. WYKAZ MIEJSC, W KTÓRYCH PRZETWARZANE SĄ DANE OSOBOWE

Inspektor Ochrony Danych odpowiedzialny jest za prowadzenie i przechowywanie dokumentacji zawierającej wykaz budynków, pomieszczeń lub części pomieszczeń tworzący obszar, w którym przetwarzane są dane osobowe zarówno w formie papierowej jak i elektronicznej. Wykaz miejsc stanowi załącznik do niniejszego dokumentu.

17. WYKAZ ZBIORÓW DANYCH OSOBOWYCH WRAZ ZE WSKAZANIEM PROGRAMÓW ZASTOSOWANYCH DO PRZETWARZANIA TYCH DANYCH

Inspektor Ochrony Danych odpowiedzialny jest za prowadzenie i przechowywanie dokumentacji zawierającej wykaz wszystkich zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych. Wykaz zbiorów prowadzony jest na podstawie metryczek zbiorów danych.

Zasoby zawierające dane osobowe przetwarzane metodami tradycyjnymi:
1) kandydatów na studentów,
2) dane osobowe studentów,
3) dane osobowe absolwentów,
4) dane osobowe pracowników,

5) dane osobowe kandydatów do pracy,
6) dane osobowe byłych pracowników,
7) dane osobowe osób zatrudnionych na umowy cywilno-prawne,
8) dane osobowe kontrahentów,
9) dane osobowe beneficjentów wniosków unijnych,
10) dane osobowe kadry dydaktycznej zawartych we wnioskach o nowe kierunki,
11) dane osobowe pozyskane w związku ze świadczeniem usług edukacyjnych przez PUZIM.

Dane osobowe w PUZIM przetwarzane są przy wykorzystaniu następujących programów:
a) SIMPLE ERP
b) SIMPLE EDU Bazus
c) System Internetowej Rekrutacji Kandydatów IRK – portal internetowy
d) Płatnik
e) iPKO Biznes – bankowy portal bankowości internetowej
f) System Biblioteczny PATRON
g) Akademicki System Archiwizacji Prac Dyplomowych ASAP
h) Ogólnopolskie Repozytorium Pisemnych Prac Dyplomowych ORPPD – internetowy ministerialny system archiwizacji prac dyplomowych
i) Platforma Moodle – portal e-lerningu
j) System POL-on – Zintegrowany System Informacji o nauce i szkolnictwie wyższym

18. OKREŚLENIE ŚRODKÓW TECHNICZNYCH I ORGANIZACYJNYCH NIEZBĘDNYCH DLA ZAPEWNIENIA BEZPIECZEŃSTWA DANYCH

Inspektor Ochrony Danych odpowiedzialny jest za prowadzenie i przechowywanie dokumentacji zawierającej określone środki techniczne i organizacyjne niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych. Dokumentacja prowadzona jest w konsultacji z Administratorem Systemów Informatycznych. Dokumentacja ta stanowi część Wewnętrznej Polityki Bezpieczeństwa Danych Osobowych w PUZIM. Prowadzona jest zarówno w formie papierowej jak i elektronicznej. Dokumentację należy udostępnić osobom upoważnionym do przetwarzania danych osobowych w PUZIM.

1. Zabezpieczenia organizacyjne:
   1) sporządzono i wdrożono Wewnętrzną Politykę Bezpieczeństwa Danych Osobowych;
   2) powołano IOD;

3) do przetwarzania danych zostały dopuszczone wyłącznie osoby posiadające upoważnienia nadane przez Administratora Danych Osobowych bądź osobę przez niego upoważnioną;
4) stworzono procedurę postępowania w sytuacji naruszenia ochrony danych osobowych;
5) osoby zatrudnione przy przetwarzaniu danych zostały zaznajomione z przepisami dotyczącymi ochrony danych osobowych oraz w zakresie zabezpieczeń systemu informatycznego;
6) osoby zatrudnione przy przetwarzaniu danych osobowych obowiązane zostały do zachowania ich w tajemnicy;
7) przetwarzanie danych osobowych dokonywane jest w warunkach zabezpieczających dane przed dostępem osób nieupoważnionych;
8) dokumenty i nośniki informacji zawierające dane osobowe, które podlegają zniszczeniu, neutralizuje się za pomocą urządzeń do tego przeznaczonych lub dokonując takiej ich modyfikacji, która nie pozwoli na odtworzenie ich treści, aby po dokonaniu usunięcia danych niemożliwa była identyfikacja osób.

2. Zabezpieczenia techniczne
   1) wewnętrzną sieć komputerową zabezpieczono poprzez odseparowanie od sieci publicznej za pomocą rozwiązań zapewniających bezpieczeństwo,
   2) stanowiska komputerowe wyposażono w indywidualną ochronę antywirusową,
   3) komputery zabezpieczono przed możliwością użytkowania przez osoby nieuprawnione do przetwarzania danych osobowych, za pomocą indywidualnego identyfikatora użytkowania i cykliczne wymuszanie zmiany hasła.

3. Środki ochrony fizycznej:
   1) obszar, na którym przetwarzane są dane osobowe, poza godzinami pracy, chroniony jest alarmem,
   2) obszar, na którym przetwarzane są dane osobowe objęty jest całodobowym monitoringiem,
   3) urządzenia służące do przetwarzania danych osobowych umieszcza się w zamykanych pomieszczeniach,
   4) dokumentacja zawierające dane osobowe umieszczona jest w zamkniętych szafach i regałach.

19. WZORY FORMULARZY POMOCNICZYCH

Inspektor Ochrony Danych odpowiedzialny jest za projektowanie, prowadzenie oraz udostępnianie wzorów formularzy pomocniczych. Dokumentacja prowadzona jest w

konsultacji z Administratorem Systemów Informatycznych oraz Lokalnymi Administratorami Bezpieczeństwa Informacji. Wzory formularzy pomocniczych stanowią część Wewnętrznej Polityki Bezpieczeństwa Danych Osobowych w PUZIM. Wzory formularzy pomocniczych prowadzone są zarówno w formie papierowej jak i elektronicznej oraz udostępniane osobom upoważnionym do przetwarzania danych osobowych.

20. INSTRUKCJA ALARMOWA W PRZYPADKU WYSTĄPIENIA INCYDENTU NARUSZAJĄCEGO OCHRONĘ DANYCH OSOBOWYCH

Celem Instrukcji jest minimalizacja skutków wystąpienia incydentów zagrożenia bezpieczeństwa, ograniczenie ryzyka powstania zagrożeń oraz występowania incydentów w przyszłości. Poniższe zasady postępowania mają zastosowanie zarówno w przypadku danych osobowych przetwarzanych w formie tradycyjnej (kartotekach, skorowidzach, księgach, wykazach i innych zbiorach ewidencyjnych) jak i w systemach informatycznych PUZIM.

Do typowych zagrożeń bezpieczeństwa danych osobowych należą:

1) brak lub niewłaściwe zabezpieczenia fizyczne pomieszczeń, urządzeń i dokumentów;
2) brak lub niewłaściwe zabezpieczenie sprzętu IT oraz oprogramowania przed wyciekiem, kradzieżą lub utratą danych osobowych;
3) niestosowanie zasad ochrony danych osobowych przez osoby upoważnione w tym:
   a. nieprzestrzeganie zasad czystego biurka i ekranu,
   b. ochrony haseł,
   c. niezamykanie pomieszczeń, szafek, biurek itp.

Do typowych incydentów bezpieczeństwa danych osobowych należą:

1) zdarzenia losowe zewnętrzne:
   a. pożar obiektu lub pomieszczenia, zalanie wodą,
   b. utrata zasilania,
   c. utrata łączności itp.;
   d. zdarzenia losowe wewnętrzne:
   e. awarie sprzętu komputerowego lub oprogramowania,
   f. pomyłki Administratora Systemów Informatycznych lub osób upoważnionych,
   g. utrata/zagubienie nośników zawierających dane osobowe itp.;
2) umyślne incydenty:
   a. nieuprawniony dostęp do systemów informatycznych lub pomieszczeń (włamanie),
   b. wyciek danych osobowych,
   c. ujawnienie danych osobowych osobom nieupoważnionym,
   d. działanie wirusów lub innego szkodliwego oprogramowania,

e. świadome zniszczenie danych,
f. kradzież danych itp.

Przed przystąpieniem do pracy osoby upoważnione zobowiązane są do zwrócenia szczególnej uwagi, czy nie zaszły okoliczności wskazujące na wystąpienie zagrożenia lub incydentu naruszającego ochronę danych osobowych.

W przypadku stwierdzenia zagrożenia lub incydentu naruszenia ochrony danych osobowych, należy niezwłocznie poinformować o tym fakcie Inspektora Ochrony Danych. W sytuacji braku możliwości zawiadomienia Inspektora Ochrony Danych należy powiadomić Lokalnego kierownika, w której miało miejsce zdarzenie.
Informację o pojawieniu się incydentu należy przekazać osobiście lub telefonicznie. Informacja ta powinna zawierać imię i nazwisko osoby zgłaszającej, miejsce i czas wystąpienia zagrożenia lub incydentu oraz krótki opis sytuacji. Osoba zgłaszająca wystąpienie zagrożenia lub incydentu] może zostać poproszona o potwierdzenie zgłoszenia na piśmie.

Do czasu przybycia Inspektor Ochrony Danych, lokalnego kierownika zgłaszający:
1) powstrzymuje się od rozpoczęcia lub kontynuowania pracy, jak również do podejmowania jakichkolwiek czynności, mogących spowodować zatarcie śladów naruszenia bądź innych dowodów;
2) zabezpiecza elementy systemu informatycznego lub kartotek, przede wszystkim poprzez uniemożliwienie dostępu do nich osobom nieupoważnionym;
3) podejmuje, stosownie do zaistniałej sytuacji, wszelkie niezbędne działania celem zapobieżenia dalszym zagrożeniom, które mogą skutkować utratą danych osobowych.

Dokonywanie zmian w miejscu wystąpienia zagrożenia lub incydentu jest dopuszczalne w przypadku, gdy zachodzi konieczność ratowania osób lub mienia albo zapobieżenia wystąpienia niebezpieczeństwa.

W sytuacji stwierdzenia wystąpienia zagrożenia lub incydentu zagrażającemu bezpieczeństwu danych osobowych, użytkownik może kontynuować pracę dopiero po otrzymaniu pozwolenia od Inspektora Ochrony Danych, przełożonego.
W przypadku, gdy zagrożenie lub incydent jest wynikiem uchybienia obowiązującej w firmie dyscypliny pracy, Inspektor Ochrony Danych wyjaśnia wszystkie okoliczności zaistniałej sytuacji i podejmuje stosowne działania wobec osób, które dopuściły się naruszenia.
Po zakończeniu czynności naprawczych system powinien utrzymać poziom ochrony nie niższy niż przed wystąpieniem zagrożenia lub incydentu związanego z naruszeniem ochrony danych osobowych.

Inspektor Ochrony Danych zobowiązany jest do prowadzenia rejestru incydentów i zdarzeń wskazujących na naruszenie bezpieczeństwa danych osobowych. Stosowne druki stanowią załączniki niniejszego dokumentu.

21. PRZEGLĄDY I AUDYTY SYSTEMU OCHRONY DANYCH

Inspektor Ochrony Danych przeprowadza wewnętrzny audyt zgodności przetwarzania danych z przepisami o ochronie danych osobowych. Zakres, przebieg i rezultaty audytu należy udokumentować na piśmie w protokole podpisywanym przez Administratora Danych Osobowych oraz Administratora Bezpieczeństwa Informacji.

Rektor PUZIM może zlecić przeprowadzenie audytu zewnętrznego także poprzez wyspecjalizowany podmiot.
Po przeprowadzonej kontroli Inspektor Ochrony Danych zobowiązany jest do zainicjowania działań korygujących i zapobiegawczych.

22. DZIAŁANIA KORYGUJĄCE I ZAPOBIEGAWCZE

Inspektor Ochrony Danych jest odpowiedzialny za analizę incydentów bezpieczeństwa lub zagrożeń ochrony danych osobowych. Źródłami informacji o incydentach, zagrożeniach lub słabościach są:
a) zgłoszenia od pracowników;
b) wyniki kontroli.

W przypadku, gdy Inspektor Ochrony Danych stwierdza konieczność podjęcia działań korygujących lub zapobiegawczych, określa:
a) źródło powstania incydentu lub zagrożenia;
b) zakres działań korygujących lub zapobiegawczych;
c) termin realizacji;
d) osobę odpowiedzialną.

Inspektor Ochrony Danych jest odpowiedzialny za nadzór nad poprawą i terminowością wdrażanych działań korygujących lub zapobiegawczych.
Po wprowadzeniu działań korygujących lub zapobiegawczych Inspektor Ochrony Danych jest zobowiązany do oceny efektywności ich zastosowania.

23. PRZEPISY KARNE I PORZĄDKOWE

Wobec osoby, która w przypadku naruszenia zasad ochrony danych osobowych lub uzasadnionego domniemania takiego naruszenia nie podjęła działań określonych niniejszym dokumencie, a w szczególności nie powiadomiła odpowiednich osób zgodnie z określonymi zasadami, można wszcząć postępowanie dyscyplinarne.

Osoba upoważniona dopuszczająca się nieuprawnionego ujawniania lub wykorzystywania danych osobowych w sposób sprzeczny z ich przeznaczeniem, czy też ich przetwarzania w sposób niezgodny z przyjętymi w PUZIM zasadami i procedurami, może zostać ukarany karą upomnienia lub karą nagany.

Naruszenie zasad ochrony danych osobowych przez osobę upoważnioną przez Administratora Danych Osobowych do przetwarzania danych osobowych może skutkować postawieniem zarzutu popełnienia jednego z przestępstwa określonych w RODO, u.o.d.o. lub przestępstwa określonego w art. 266 Kodeksu Karnego.

Przepisy karne i porządkowe reguluje:
1) Rozporządzenie RODO;
2) ustawa z dnia 10 maja 2018r. o ochronie danych osobowych.

24. 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 oraz odbycia szkolenia w zakresie bezpieczeństwa danych osobowych.

Wewnętrzna Polityka Bezpieczeństwa Danych Osobowych nie może być udostępniana osobom postronnym w żadnej formie za wyjątkiem osób upoważnionych do przetwarzania danych osobowych w PUZIM.
W sprawach nieuregulowanych w niniejszej Wewnętrznej Polityce Bezpieczeństwa Danych Osobowych mają zastosowanie przepisy rozporządzenia RODO oraz ustawy z dnia 10 maja 2018r. o ochronie danych osobowych.

ZAŁĄCZNIKI

1) Nr 1 - Upoważnienie do przetwarzania danych osobowych;
2) Nr 2 - Oświadczenie kandydata do pracy;
3) Nr 3 - Oświadczenie pracownika;
4) Nr 4 - Ewidencja osób upoważnionych do przetwarzania danych osobowych;
5) Nr 5 - Wykaz budynków;
6) Nr 6 - Wykaz zbiorów danych osobowych
7) Nr 7 - Rejestr czynności
8) Nr 8 - Opis środków technicznych
9) Nr 9 - Obowiązki przetwarzających dane osobowe
10) Nr 10 - Raport z incydentu
11) Nr 11 - Ewidencja incydentów

REKTOR
prof. nadzw. dr hab. Leszek Zygner

Załącznik nr 1 do Wewnętrznej Polityki Bezpieczeństwa Danych Osobowych wprowadzonej Zarządzeniem Rektora PUZ im. Ignacego Mościckiego w Ciechanowie nr 40/2019 z dnia 01.10.2019 r.

.....

/miejscowość, data/

Upoważnienie
do przetwarzania danych osobowych

Na podstawie art. 29 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych, zwanego dalej RODO upoważniam Panią/Pana:

.....

/Imię i Nazwisko/

zatrudnioną/-nego na stanowisku: .....

do przetwarzania danych osobowych w następującym zakresie:

- wykonywanie obowiązków służbowych na stanowisku pracy i poleceń przełożonego*
- wykonywanie obowiązków zleceniobiorcy*
- w formie papierowej / elektronicznej *,
- w systemie / programie .....
- w zbiorze danych:

☐ Dane osobowe kandydatów na studia	☐ Dane osobowe osób zatrudnionych na umowy cywilno – prawne
☐ Dane osobowe studentów	☐ Dane osobowe beneficjentów wniosków unijnych
☐ Dane osobowe absolwentów	☐ Dane osobowe kontrahentów
☐ Dane osobowe kandydatów do pracy	☐ Dane osobowe kadry dydaktycznej zawartych we wnioskach o nowe kierunki
☐ Dane osobowe pracowników	☐ Zbiór danych osobowych pozyskanych w związku ze świadczeniem usług edukacyjnych przez uczelnię
☐ Dane osobowe byłych pracowników	☐

Niniejsze upoważnienie jest ważne w okresie od ..... do .....

Administrator Danych Osobowych /
Inspektor Ochrony Danych

.....

/podpis/

* niepotrzebne skreślić

Załącznik nr 2 do Wewnętrznej Polityki Bezpieczeństwa Danych Osobowych wprowadzonej Zarządzeniem Rektora PUZ im. Ignacego Mościckiego w Ciechanowie Nr 40/2019 z dnia 01.10.2019 r.

Oświadczenie kandydata do pracy

Ja, niżej podpisana(y)

.....

Oświadczam, iż:
Zgodnie z art. 13 ust. 1 i 2 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych (RODO), zwanego dalej RODO, wyrażam zgodę na przetwarzanie danych kontaktowych oraz zostałem(am) poinformowany i przyjmuję do wiadomości, iż:

1) administratorem danych osobowych jest Państwowa Uczelnia Zawodowa im. Ignacego Mościckiego w Ciechanowie, ul. Narutowicza 9, 06-400 Ciechanów,
2) w razie pytań dotyczących zasad prywatności i przetwarzania danych osobowych należy kontaktować się:
   a) pod adresem Administratora Danych Osobowych: ul. Narutowicza 9, 06-400 Ciechanów, email: rektorat@puzim.edu.pl;
   b) do Inspektora Ochrony Danych, email: iod@puzim.edu.pl;
3) dane osobowe przetwarzane będą w zakresie wskazanym w prawie pracy (ustawa z dnia 26.06.1974r. – Kodeks pracy) dla potrzeb obecnego postępowania rekrutacyjnego; na podstawie art. 6 ust. 1 lit. b RODO, a dane do kontaktu zgodnie z art.6 ust. lit. a RODO.
4) dane osobowe będą przechowywane przez okres rekrutacji, a po pozytywnym wyniku rekrutacji przez okres wymagany przepisami prawa pracy, o ubezpieczeniu społecznym,
5) posiadam prawo dostępu do treści swoich danych oraz prawo ich sprostowania, usunięcia, ograniczenia przetwarzania, praw do przenoszenia danych, prawo wniesienia sprzeciwu, prawo do cofnięcia zgody w dowolnym momencie bez wpływy na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem,
6) mam prawo wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, gdy uznam, że przetwarzanie danych osobowych narusza przepisy RODO,
7) dane osobowe zostaną powierzone innym odbiorcom, niezbędnym w procesie realizacji określonego w pkt. 3 celu,
8) podanie danych osobowych jest dobrowolne, jednak niezbędne do realizacji celu,
9) dane osobowe nie będą poddawane zautomatyzowanemu podejmowaniu decyzji,
10) dane osobowe nie będą przekazywane do państwa trzeciego lub organizacji międzynarodowej.

Ciechanów, dnia .....

(data, czytelny podpis osoby składającej oświadczenie)

Załącznik nr 3 do Wewnętrznej Polityki Bezpieczeństwa Danych Osobowych wprowadzonej Zarządzeniem Rektora PUZ im. Ignacego Mościckiego w Ciechanowie nr 40/2019 z dnia 01.10.2019 r.

Oświadczenie pracownika
w zakresie ochrony danych osobowych

Ja, niżej podpisana(y)

.....

Oświadczam, iż:
Zgodnie z art. 13 ust. 1 i 2 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych (RODO), zwanego dalej RODO; zostałem(am) poinformowany i przyjmuję do wiadomości, iż:

1) administratorem danych osobowych jest Państwowa Uczelnia Zawodowa im. Ignacego Mościckiego w Ciechanowie, ul. Narutowicza 9, 06-400 Ciechanów,
2) w razie pytań dotyczących zasad prywatności i przetwarzania danych osobowych należy kontaktować się: pod adresem Administratora Danych Osobowych: ul. Narutowicza 9, 06-400 Ciechanów, email: rektorat@puzim.edu.pl; lub do Inspektora Ochrony Danych, email: iod@puzim.edu.pl;
3) dane osobowe przetwarzane będą na podstawie art. 6 ust. 1 lit. b, lit. c RODO; w zakresie wskazanym w prawie pracy (ustawa z dnia 26.06.1974r. – Kodeks pracy).
4) dane osobowe będą przechowywane przez okres wskazany w prawie pracy (ustawa z dnia 26.06.1974r. – Kodeks pracy),
5) posiadam prawo dostępu do treści swoich danych oraz prawo ich sprostowania, usunięcia, ograniczenia przetwarzania, praw do przenoszenia danych, prawo wniesienia sprzeciwu, prawo do cofnięcia zgody w dowolnym momencie bez wpływy na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem,
6) mam prawo wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, gdy uznam, że przetwarzanie danych osobowych narusza przepisy RODO,
7) dane osobowe zostaną powierzone innym odbiorcom, niezbędnym w procesie realizacji określonego w pkt. 3 celu,
8) podanie danych osobowych jest dobrowolne, jednak niezbędne do realizacji celu,
9) dane osobowe nie będą poddawane zautomatyzowanemu podejmowaniu decyzji,
10) dane osobowe mogą być przekazywane do państwa trzeciego w przypadku udziału pracownika w programie Erasmus.

Ciechanów, dnia .....

(data, czytelny podpis osoby składającej oświadczenie)

Załącznik nr 4 do Wewnętrznej Polityki Bezpieczeństwa
Danych Osobowych wprowadzonej
Zarządzeniem Rektora PUZ im. Ignacego Mościckiego w Ciechanowie
Nr 40/2019 z dnia 01.10.2019r.

Ewidencja osób upoważnionych do przetwarzania danych osobowych

Lp.	Imię i Nazwisko, zajmowane stanowisko / data zmiany danych		Zakres upoważnienia do przetwarzania danych osobowych	Data wydania upoważnienia	Data ustania upoważnienia
1	2		3	4	5
	Zmiana danych**				
	Zmiana danych**				
	Zmiana danych**				
	Zmiana danych**				

** W przypadku zmiany danych wypełnić należy te rubryki, których zmiany dotyczą – pozostałe należy przekreślić.

Załącznik nr 5 do Wewnętrznej Polityki Bezpieczeństwa
Danych Osobowych
wprowadzonej
Zarządzeniem Rektora PUZ im. Ignacego Mościckiego w Ciechanowie
Nr 40/2019 z dnia 01.10.2019 r.

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

Lp.	Miejsce przetwarzania danych osobowych	Obszar przetwarzania danych osobowych /nazwa pomieszczeń, nr itp.	Zbiory danych osobowych
	Dane osobowe przetwarzane metodami tradycyjnymi		
1	Budynek uczelni – Ciechanów ul. Narutowicza 9.	Pomieszczenia: - Dziekanat Wydziału Inżynierii i Ekonomii, - Rektorat i Kancelaria Uczelni, - Kwestura, - Dział Kształcenia i Spraw Studenckich, - Sekcja Promocji i Biuro Karier, - Sekretariaty Rektora, Prorektora oraz Kanclerza, - Pełnomocnika rektora ds. obronnych bezpieczeństwa wewnętrznego i ochrony informacji niejawnych, - Pełnomocnik Rektora ds. sportu, - Specjalisty ds. BHP i ochrony ppoż. - Sekcja Rekrutacji, - Sekcja współpracy z otoczeniem społeczno – gospodarczym, - Biblioteka Uczelniana.	dane osobowe kandydatów na studia, studentów, uczniów i słuchaczy
	Budynek uczelni - Ciechanów ul. Wojska Polskiego 51.	Pomieszczenia: - Dziekanatu Wydziału Nauk o Zdrowiu i Nauk Społecznych.	
	Budynek uczelni - Mława ul. Warszawska 52	Pomieszczenia: - Dziekanat PUZ im. Ignacego Mościckiego w Ciechanowie filia w Mławie Wydziału Nauk Technicznych i Społecznych	

	Budynek Domu Studenta – Ciechanów, ul. Narutowicza 4A	Pomieszczenia: - Kierownika Domu Studenta - Archiwum uczelnianego	
2	Budynek uczelni – Ciechanów ul. Narutowicza 9	Pomieszczenia: - Dziekanat Wydziału Inżynierii i Ekonomii, - Rektorat i Kancelaria Uczelni, - Kwestura, - Dział Kształcenia i Spraw Studenckich, - Sekcja Promocji i Biuro Karier, - Sekretariaty Rektora, Prorektora oraz Kanclerza, - Pełnomocnika rektora ds. obronnych bezpieczeństwa wewnętrznego i ochrony informacji niejawnych, - Pełnomocnik Rektora ds. sportu, - Specjalisty ds. BHP i ochrony ppoż. - Sekcja Rekrutacji, - Sekcja współpracy z otoczeniem społeczno – gospodarczym, - Biblioteka Uczelniana.	dane osobowe kandydatów na studia, studentów, uczniów i słuchaczy
	Budynek uczelni – Ciechanów ul. Wojska Polskiego 51	Pomieszczenia: - Dziekanatu Wydziału Nauk o Zdrowiu i Nauk Społecznych.	
	Budynek uczelni - Mława ul. Warszawska 52	Pomieszczenia: - Dziekanat PUZ im. Ignacego Mościckiego w Ciechanowie filia w Mławie Wydziału Nauk Technicznych i Społecznych - Akademickie Centrum Kształcenia	
	Budynek Domu Studenta – Ciechanów, ul. Narutowicza 4A	Pomieszczenia: - Kierownika Domu Studenta	

		- Archiwum uczelnianego	
3	Budynek uczelni – Ciechanów, ul. Narutowicza 9 Budynek uczelni – Ciechanów, ul. Wojska Polskiego 51 Budynek uczelni – Mława, ul. Warszawska 52 Budynek Domu Studenta – Ciechanów, ul. Narutowicza 4A	Pomieszczenia: - Rektora, Prorektorów i Kanclerza - Działu Spraw Osobowych - Dziekana Wydziału Inżynierii i Ekonomii Pomieszczenia: - Dziekanatu Wydziału Nauk o Zdrowiu i Nauk Społecznych. Pomieszczenia: - Dziekanat PUZ im. Ignacego Mościckiego w Ciechanowie filia w Mławie Wydziału Nauk Technicznych i Społecznych Pomieszczenia: - Kierownika Domu Studenta - Archiwum uczelnianego	dane osobowe kandydatów do pracy
4	Budynek uczelni – Ciechanów, ul. Narutowicza 9 Budynek uczelni – Ciechanów, ul. Narutowicza 4A	Pomieszczenia: - Działu Spraw Osobowych - Kwestury - Specjalisty ds. BHP i ochrony ppoż. - Pełnomocnik rektora ds. obronnych bezpieczeństwa wewnętrznego i ochrony informacji niejawnych Pomieszczenia: - Archiwum uczelnianego	dane osobowe byłych pracowników
5	Budynek uczelni – Ciechanów, ul. Narutowicza 9	Pomieszczenia: - Działu Spraw Osobowych - Kwestury - Rektora, Prorektorów i Kanclerza	dane osobowe osób zatrudnionych na umowy cywilno-prawne

	Budynek uczelni- Ciechanów, ul. Wojska Polskiego 51 - Budynek uczelni – Mława, ul. Warszawska 52 Budynek Domu Studenta – Ciechanów, ul. Narutowicza 4A	- Dziekana Wydziału Inżynierii i Ekonomii Pomieszczenia: - Dziekana Wydziału Nauk o Zdrowiu i Nauk Społecznych Pomieszczenia: - Dziekanat PUZ im. Ignacego Mościckiego w Ciechanowie filia w Mławie Wydziału Nauk Technicznych i Społecznych Pomieszczenia: - Archiwum uczelnianego	
6	Budynek uczelni - Ciechanów ul. Narutowicza 9 Budynek Domu Studenta – Ciechanów, ul. Narutowicza 4A	Pomieszczenia: - Biura Rektora, Prorektora i Kanclerza - Kwestury - Działu Administracyjno-Inwestycyjny - Sekcja współpracy z otoczeniem społeczno - gospodarczym - Działu Kształcenia i Spraw Studenckich Pomieszczenia: - Kierownika Domu Studenta - Archiwum uczelnianego	dane osobowe kontrahentów
7	Budynek uczelni - Ciechanów ul. Narutowicza 9 Budynek Domu Studenta – Ciechanów, ul. Narutowicza 4A	Pomieszczenia: - Działu Kształcenia i Spraw Studenckich Pomieszczenia: - Archiwum uczelnianego	dane osobowe kandydatów (wnioski o nowe kierunki)
8	Budynek uczelni - Ciechanów ul. Narutowicza 9	- Sekcja pozyskiwania środków realizacji projektów - Sekcja współpracy z otoczeniem społeczno – gosp.	dane osobowe beneficjentów

	Budynek Domu Studenta – Ciechanów, ul. Narutowicza 4A	Pomieszczenia: - Archiwum uczelnianego	
2. Dane osobowe przetwarzane w systemach informatycznych.			
9	Dane przetwarzane są w pomieszczeniach: a) Dziekanatu Wydziału Inżynierii i Ekonomii (ul. Narutowicza 9), b) Rektoratu i Kancelarii Uczelni, Sekretariatu Kanclerza (ul. Narutowicza 9), c) Działu Spraw Osobowych (ul. Narutowicza 9) d) Kwestury (ul. Narutowicza 9), e) Działu Kształcenia i Spraw Studenckich (ul. Narutowicza 9), f) Pełnomocnika rektora ds. obronnych bezpieczeństwa wewnętrznego i ochrony informacji niejawnych (ul. Narutowicza 9), g) Działu Informatycznego (ul. Narutowicza 9), h) Sekcja pozyskiwania środków realizacji projektów (ul. Narutowicza 9), i) Wydziału Nauk o Zdrowiu i Nauk Społecznych (Wojska Polskiego 51), j) Archiwum uczelnianego (ul. Narutowicza 4A), k) Dziekanatu PUZ im. Ignacego Mościckiego w Ciechanowie filia w Mławie Wydziału Nauk Technicznych i Społecznych (Mława, ul. Warszawska 52), l) Kierownika Domu Studenta ul. Narutowicza 4A), m) Sekretariatu ACK.		

Załącznik nr 6 do Wewnętrznej Polityki Bezpieczeństwa Danych Osobowych wprowadzonej Zarządzeniem Rektora PUZ im. Ignacego Mościckiego w Ciechanowie nr 40/2019 z dnia 01.10.2019 r.

Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania danych osobowych

Lp.	Zbiór danych osobowych	Zastosowany program do przetwarzania danych
1	2	3
1	Dane osobowe kandydatów na studia	• System Internetowej Rekrutacji Kandydatów (IRK).
2	Dane osobowe studentów	• SIMPLE EDU / Bazus, • System biblioteczny PATRON, • Ogólnopolskie Repetytorium Pisemnych Prac Dyplomowych ORPPD (system ministerstwa ds. szkolnictwa wyższego), • System POL-on (system ministerstwa ds. szkolnictwa wyższego).
3	Dane osobowe absolwentów	• SIMPLE EDU / Bazus (ze statusem „zakończone studia) • System biblioteczny PATRON • Akademicki System Archiwalnych prac dyplomowyc ASAP • Ogólnopolskie Repetytorium Pisemnych Prac Dyplomowych ORPPD (system ministerstwa ds. szkolnictwa wyższego), • System POL-on (system ministerstwa ds. szkolnictwa wyższego).
4	Dane osobowe kandydatów do pracy	• SIMPLE ERP
5	Dane osobowe pracowników	• SIMPLE ERP, • Płatnik, • System biblioteczny PATRON • Ogólnopolskie Repetytorium Pisemnych Prac Dyplomowych ORPPD (system ministerstwa ds. szkolnictwa wyższego), • System POL-on (system ministerstwa ds. szkolnictwa wyższego – pracownicy dydaktyczni).
6	Dane osobowe byłych pracowników	• SIMPLE ERP, • Płatnik,
7	Dane osobowe osób zatrudnionych na umowy cywilno - prawne	• SIMPLE ERP
8	Dane osobowe beneficjentów wniosków unijnych	• SIMPLE EDU / Bazus
9	Dane osobowe kontrahentów	• SIMPLE ERP, • SIMPLE EDU / Bazus,
10	Dane osobowe kadry dydaktycznej zawartych we wnioskach o nowe kierunki	• System POL-on (system ministerstwa ds. szkolnictwa wyższego).
11	Zbiór danych osobowych pozyskanych w związku ze świadczeniem usług edukacyjnych przez PUZIM	• SIO (System Informacji Oświatowej)

Załącznik nr 7 do Wewnętrznej Polityki Bezpieczeństwa
Danych Osobowych wprowadzonej
Zarządzeniem Rektora PUZ im. Ignacego Mościckiego w Ciechanowie
nr 40/2019 z dnia 01.10.2019r.

REJESTR CZYNNOŚCI PRZETWARZANIA Państwowa
(podstawa prawna art. 30 ogólnego rozporządzenia o ochronie danych RODO)

L.p.	Nazwa oraz dane kontaktowe administratora oraz wszelkich współadministratorów	Cele przetwarzania	Opis kategorii osób, których dane dotyczą, oraz kategorii danych osobowych	Kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w tym odbiorców w państwach trzecich lub w organizacjach międzynarodowych	Informacje o przekazaniu danych osobowych do państwa trzeciego lub organizacji międzynarodowych	Planowane terminy usunięcia poszczególnych kategorii danych	Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa (art. 32 ust. 1)
1.	**Państwowa Uczelnia Zawodowa w Ciechanowie, im. Ignacego Mościckiego ul. Narutowicza 9, 06-400 Ciechanów**	Prowadzenie rejestru pracowników, akt pracowniczych, ewidencji czasu ich pracy, dokumentacja powypadkowa, urlopowa.	Pracownicy	Kancelaria prawna, firmy szkoleniowe, lekarz medycyny pracy.	Nie dotyczy	50 lat lub 10 lat Ustawa z dnia 10 stycznia 2018r. o zmianie niektórych ustaw w związku ze skróceniem okresu przechowywania akt pracowniczych oraz ich elektronizacji (Dz. U. 2018r. poz. 357).	Zamykane szafy w pomieszczeniach zamykanych, dostępnych tylko dla upoważnionych osób. Kontrola dostępu do systemu informatycznego, dostęp tylko dla upoważnionych osób, instalacja oprogramowania zabezpieczającego typu firewall, system antywirusowy.
2.	**Państwowa Uczelnia Zawodowa w Ciechanowie, im. Ignacego Mościckiego ul. Narutowicza 9, 06-400 Ciechanów**	Rekrutacja do pracy	Kandydaci do pracy	Dane nie są przekazywane innym podmiotom.	Nie dotyczy	Po zakończeniu procesu rekrutacyjnego	Zamykane szafy w pomieszczeniach zamykanych, dostępnych tylko dla upoważnionych osób. Kontrola dostępu do systemu informatycznego, dostęp tylko dla upoważnionych osób, instalacja oprogramowania zabezpieczającego typu firewall, system antywirusowy.
3.	**Państwowa Uczelnia Zawodowa w Ciechanowie, im. Ignacego Mościckiego ul. Narutowicza 9, 06-400 Ciechanów**	Zgłoszenie pracowników i członków ich rodzin do ZUS, osób zatrudnionych na podstawie umów cywilno – prawnych, aktualizacja i przekazywanie danych o zwolnieniach.	Pracownicy, osoby zatrudnione na podstawie umów cywilno - prawnych	Kancelaria prawna, lekarz medycyny pracy.	Nie dotyczy	50 lat lub 10 lat Ustawa z dnia 10 stycznia 2018r. o zmianie niektórych ustaw w związku ze skróceniem okresu przechowywania akt pracowniczych oraz ich elektronizacji (Dz. U. 2018r. poz. 357).	Zamykane szafy w pomieszczeniach zamykanych, dostępnych tylko dla upoważnionych osób. Kontrola dostępu do systemu informatycznego, dostęp tylko dla upoważnionych osób, instalacja oprogramowania zabezpieczającego typu firewall, system antywirusowy

L.p.	Nazwa oraz dane kontaktowe administratora oraz wszelkich współadministratorów	Cele przetwarzania	Opis kategorii osób, których dane dotyczą, oraz kategorii danych osobowych	Kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w tym odbiorców w państwach trzecich lub w organizacjach międzynarodowych	Informacje o przekazaniu danych osobowych do państwa trzeciego lub organizacji międzynarodowych	Planowane terminy usunięcia poszczególnych kategorii danych	Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa (art. 32 ust.1)
4.	**Państwowa Uczelnia Zawodowa w Ciechanowie, im. Ignacego Mościckiego ul. Narutowicza 9, 06-400 Ciechanów**	Prowadzenie rozliczeń z pracownikami, osobami zatrudnionymi na podstawie umów cywilno - prawnych, wypłata wynagrodzeń naliczanie obciążeń oraz naliczanie składek do ZUS	Pracownicy, osoby zatrudnione na podstawie umów cywilno - prawnych	Banki.	Nie dotyczy	50 lat lub 10 lat Ustawa z dnia 10 stycznia 2018r. o zmianie niektórych ustaw w związku ze skróceniem okresu przechowywania akt pracowniczych oraz ich elektronizacji (Dz. U. 2018r. poz. 357).	Zamykane szafy w pomieszczeniach zamykanych, dostępnych tylko dla upoważnionych osób. Kontrola dostępu do systemu informatycznego, dostęp tylko dla upoważnionych osób, instalacja oprogramowania zabezpieczającego typu firewall, system antywirusowy.
5.	**Państwowa Uczelnia Zawodowa w Ciechanowie, im. Ignacego Mościckiego ul. Narutowicza 9, 06-400 Ciechanów**	Prowadzenie rozliczeń z kontrahentami	Kontrahenci	Banki. Kancelaria prawna.	Nie dotyczy	5 lat licząc od końca roku kalendarzowego, w którym upłynął termin płatności podatku [art. 70 § 1 Ordynacja podatkowa (Dz.U. 2017, poz. 20 – tekst jednolity ze zm.).	Zamykane szafy w pomieszczeniach zamykanych, dostępnych tylko dla upoważnionych osób. Kontrola dostępu do systemu informatycznego, dostęp tylko dla upoważnionych osób, instalacja oprogramowania zabezpieczającego typu firewall, system antywirusowy.
6.	**Państwowa Uczelnia Zawodowa w Ciechanowie, im. Ignacego Mościckiego ul. Narutowicza 9, 06-400 Ciechanów**	Rekrutacja studentów, prowadzenie dokumentacji studentów, śledzenie losów absolwentów	Kandydaci na studia, studenci.	Ministerstwo ds. szkolnictwa wyższego.	Nie dotyczy	50 lat (Rozporządzenie Ministra Nauki i Szkolnictwa Wyższego z dnia 28 września 2018r. w sprawie studiów (Dz. U. z 2018r., poz.1861 ze zm.).	Zamykane szafy w pomieszczeniach zamykanych, dostępnych tylko dla upoważnionych osób. Kontrola dostępu do systemu informatycznego, dostęp tylko dla upoważnionych osób, instalacja oprogramowania zabezpieczającego typu firewall, system antywirusowy

L.p.	Nazwa oraz dane kontaktowe administratora oraz wszelkich współadministratorów	Cele przetwarzania	Opis kategorii osób, których dane dotyczą, oraz kategorii danych osobowych	Kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w tym odbiorców w państwach trzecich lub w organizacjach międzynarodowych	Informacje o przekazaniu danych osobowych do państwa trzeciego lub organizacji międzynarodowych	Planowane terminy usunięcia poszczególnych kategorii danych	Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa (art. 32 ust.1)
7.	**Państwowa Uczelnia Zawodowa w Ciechanowie, im. Ignacego Mościckiego ul. Narutowicza 9, 06-400 Ciechanów**	Prowadzenie kształcenia na wszystkich szczeblach edukacji dla osób od przedszkola do szkół ponadpodstawowych	Podopieczni, uczniowie, słuchacze, których dane uzyskano w związku ze świadczeniem przez PWSZ usług edukacyjnych.	SIO (System Informacji Oświatowej) Ministerstwa Edukacji Narodowej.	Nie dotyczy	50 lat [ustawa z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach (Dz. U. z 2016 r., poz. 1506 t.j. ze zm.).	Zamykane szafy w pomieszczeniach zamykanych, dostępnych tylko dla upoważnionych osób. Kontrola dostępu do systemu informatycznego, dostęp tylko dla upoważnionych osób, instalacja oprogramowania zabezpieczającego typu firewall, system antywirusowy.
8.	**Państwowa Uczelnia Zawodowa w Ciechanowie, im. Ignacego Mościckiego ul. Narutowicza 9, 06-400 Ciechanów**	Przeprowadzanie wymiany studentów w ramach programu „Erasmus+" – umowy między uczelniami	Studenci, pracownicy wyjeżdżający / przyjeżdżający do PWSZ w ramach programu „Erasmus+" – umowy między uczelniami	Odbiorcami danych osobowych są uczelnie (i instytucje) partnerskie, Narodowa Agencja Programu Erasmus+ (Fundacja Rozwoju Systemu Edukacji) oraz Komisja Europejska.	Uczelnia Kilis 7 Aralik Universitesi, Kilis (TR KILIS01) Turcja	8 lat [umowa przystąpienia Polski do programu Erasmus+].	Odpowiednie zabezpieczenia fizyczne i systemowe stosowane w PWSZ oraz u odbiorców danych osobowych.
9	**Państwowa Uczelnia Zawodowa w Ciechanowie, im. Ignacego Mościckiego ul. Narutowicza 9, 06-400 Ciechanów**	Realizacja usługi hotelowej przez domu studenta	Studenci, osoby z zewnątrz	Podmioty państwowe upoważnione zgodnie z przepisami prawa	Nie dotyczy	5 lat licząc od końca roku kalendarzowego, w którym upłynął termin płatności podatku [art. 70 § 1 Ordynacja podatkowa (Dz.U. 2017, poz. 20 – tekst jednolity ze zm.).	Zamykane szafy w pomieszczeniach zamykanych, dostępnych tylko dla upoważnionych osób. Kontrola dostępu do systemu informatycznego, dostęp tylko dla upoważnionych osób, instalacja oprogramowania zabezpieczającego typu firewall, system antywirusowy.

Rozporządzenie Parlamentu Europejskiego i Rady Europy 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem i w sprawie swobodnego przepływu takich danych (ogólne rozporządzenie o ochronie danych).

Opis stosowanych środków technicznych i organizacyjnych

A. Środki ochrony fizycznej

a) Zbiory danych osobowych przechowywane są w pomieszczeniach zabezpieczonych drzwiami zwykłymi.

b) Dostęp do pomieszczeń, w których przetwarzane są zbiory danych osobowych jest w czasie nieobecności zatrudnionych tam pracowników objęty systemem antywłamaniowym.

c) Zbiory danych osobowych w formie papierowej przechowywane są w zamkniętych szafach.

B. Środki sprzętowe infrastruktury informatycznej i telekomunikacyjnej

Zasady ogólne

a) Komputery służące do przetwarzania danych osobowych są połączone z lokalną siecią komputerową.

b) Zastosowano urządzenia, chroniące system informatyczny służący do przetwarzania danych osobowych przed skutkami awarii zasilania – UPS w serwerowni.

Zasady korzystania z komputerów przenośnych, na których przetwarzane są dane osobowe

a) W komputerze przenośnym wykorzystywany jest akumulator pozwalający na bezawaryjną pracę po zaistnieniu awarii zasilania, co stanowi ochronę systemów informatycznych służących do przetwarzania danych osobowych.

b) Dostęp do komputera przenośnego, na których mają być przetwarzane dane osobowe umożliwiony jest po podaniu hasła dostępu.

C. Środki ochrony w ramach oprogramowania urządzeń teletransmisji

a) Wdrożono oprogramowanie zabezpieczeń typu firewall w systemach informatycznych uczelnianych.

b) Systemy informatyczne zarządzanie przez ministerstwo ds. szkolnictwa wyższego chronione są na poziomie ministerstwa.

c) Wprowadzono mechanizmy kontroli przepływu informacji pomiędzy systemem informatycznym Administratora Danych Osobowych, a siecią publiczną.

D. Środki ochrony w ramach narzędzi baz danych i innych narzędzi programowych

a) Zastosowano system rejestracji dostępu do systemu/zbioru danych osobowych.

b) Dostęp do zbioru danych osobowych wymaga uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła.

E. Środki organizacyjne

a) Do przetwarzania danych osobowych dopuszczono wyłącznie osoby posiadające upoważnienie nadane przez Administratora Danych Osobowych.

b) Prowadzona jest ewidencja osób upoważnionych do przetwarzania danych osobowych.

Załącznik nr 9 do Wewnętrznej Polityki Bezpieczeństwa
Danych Osobowych wprowadzonej
Zarządzeniem Rektora PUZ im. Ignacego Mościckiego w Ciechanowie
Nr 40/2019 z dnia 01.10.2019r.

Obowiązki osób upoważnionych do przetwarzania danych osobowych

1. Przetwarzać dane osobowe, a więc dokonywać na nich jakikolwiek operacji, mogą dokonywać osoby upoważnione przez Administratora Danych Osobowych (ADO) Państwowej Uczelni Zawodowej im. Ignacego Mościckiego w Ciechanowie (PUZIM).
2. Osoby upoważnione do przetwarzania danych osobowych obowiązane są przetwarzać te dane wyłącznie we wskazanym zakresie.
3. Osoba, która otrzymała od administratora upoważnienie do przetwarzania danych osobowych zobowiązana jest równocześnie do zachowania tych danych oraz sposobów i zabezpieczenia w tajemnicy.
4. Kopiowanie, skanowanie, powielanie dokumentacji w celu niewchodzącym w zakres upoważnienia jest zabronione.
5. Wynoszenie dokumentów, w których zawarte są dane osobowe na zewnątrz PUZIM jest zabronione.
6. Przetwarzający dane osobowe zobowiązany jest zachować wszelkie możliwe środki ostrożności, aby dane osobowe zostały udostępnieniu osobom postronnym, zniszczeniu itd.:
   1) Ekrany monitorów komputerów ustawione w sposób uniemożliwiający wgląd w nie interesantom.
   2) Obowiązuje zasad „czystego biurka" podczas pracy (pozostawiona na biurku tylko niezbędna ilość dokumentów).
   3) Dokumenty znajdujące się na biurkach podczas pracy z nimi pozostawione w sposób uniemożliwiający wgląd w nie osobom postronnym.
   4) Przenoszenie dokumentów do innych pomieszczeń musi odbywać się w sposób uniemożliwiający przypadkowe ich wypadnięcie itp.
   5) Po zakończeniu pracy dokumentacja musi zostać umieszczona w przeznaczonych do tego celu szafach, regałach itp. i zamknięta dla osób postronnych.
   6) Egzemplarze kopii dokumentów po nieudanej operacji kopiowania muszą być zniszczone w sposób uniemożliwiający uzyskanie zawartych w nich danych osobowych przez osoby postronne.
7. Wszelkie zauważone przez przetwarzających dane osobowe nieprawidłowości związane z procedurami w tym zakresie muszą być niezwłocznie zgłaszane przełożonym, Inspektorowi Ochrony Danych (IOD).
8. Osoba przetwarzająca dane osobowe zobowiązana jest do zachowania danych osobowych w tajemnicy, co oznacza zakaz ich ujawniania innym osobom, przekazywania, wykorzystywania. Naruszenie tego obowiązku może skutkować odpowiedzialnością karną przewidzianą stosownymi przepisami.

Załącznik 10 do Wewnętrznej Polityki Bezpieczeństwa
Danych Osobowych wprowadzonej
Zarządzeniem Rektora PUZ im. Ignacego Mościckiego w Ciechanowie
Nr 40/2019 z dnia 01.10.2019r.

Raport z incydentu naruszenia bezpieczeństwa informacji

(miejscowość, data) .....

.....

.....

.....

(nazwa i adres miejsca zdarzenia)

.....
(imię i nazwisko)

Administrator Danych Osobowych

Raport z incydentu naruszenia bezpieczeństwa informacji .....
(nr/rok)

Data i godzina incydentu			
Miejsce incydentu (nr pomieszczenia)			
System/aplikacja			
Dane osoby zgłaszającej			
Imię i nazwisko,			
Dział			
Charakter zdarzenia *			
	Nieuprawniony dostęp do systemu		Kradzież danych
	Nieuprawniony dostęp do danych		Utrata danych
	Nieuprawniony przekaz danych		Mechaniczne uszkodzenie urządzeń do przetwarzania danych
	Wykrycie wirusa (podać rodzaj):		
	Inne (podać jakie):		
Świadkowie zdarzenia			
Imię i nazwisko, stanowisko, komórka organizacyjna			

* Należy zaznaczyć właściwe pola.

VERTE →

Załącznik 10 do Wewnętrznej Polityki Bezpieczeństwa
Danych Osobowych wprowadzonej
Zarządzeniem Rektora PUZ im. Ignacego Mościckiego w Ciechanowie
Nr 40/2019 z dnia 01.10.2019r.

Opis incydentu i wnioski:***

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

Administrator Danych Osobowych /

Inspektor Ochrony Danych

.....

(imię i nazwisko)

.....

(data, podpis)

*** Należy podać:
- opis przebiegu zdarzenia,
- opis zabezpieczonych dowodów,
- wpływ incydentu na infrastrukturę systemu informatycznego,
- wpływ incydentu na stan zbiorów informacji,
- opis podjętych decyzji i przeprowadzonych czynności wraz z uzasadnieniem,
- wnioski i propozycje w celu podniesienia poziomu bezpieczeństwa informacji.

Załącznik nr 11 do Wewnętrznej Polityki Bezpieczeństwa
Danych Osobowych wprowadzonej
Zarządzeniem Rektora PUZ im. Ignacego Mościckiego w Ciechanowie
Nr 40 /2019 z dnia 01.10.2019r.

Rejestr naruszeń ochrony danych osobowych

Administrator Danych Osobowych: Państwowa Uczelnia Zawodowa im. Ignacego Mościckiego w Ciechanowie

Lp.	Rodzaj naruszeń	Obowiązek zgłoszenia organowi nadzorczemu / zagrożenie naruszenia praw i wolności	Obowiązek zawiadomienia osoby, której dane dotyczą	Okoliczności naruszenia (krótki opis)	Skutki naruszenia	Podjęte działania zaradcze