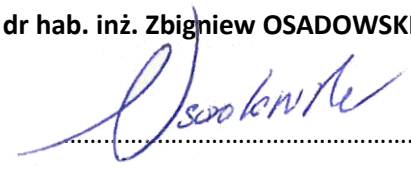
Załącznik nr 1 do zarządzenia nr R.021.57.21 z dnia 13 maja 2021 roku

Polityka Bezpieczeństwa Informacji (PBI)
i Instrukcja zarządzania systemami teleinformatycznymi
w zakresie danych osobowych

ZATWIERDZIŁ

JM REKTOR
dr hab. inż. Zbigniew OSADOWSKI, prof. AP



.....

/podpis na oryginale/

Słupsk 2021 r.

Spis treści

1. POSTANOWIENIA OGÓLNE.

1.1. Celem Polityki Bezpieczeństwa przetwarzania danych osobowych w Akademii Pomorskiej w Słupsku dalej nazywaną *Polityką Bezpieczeństwa Informacji* (PBI), jest uzyskanie optymalnego i zgodnego z wymogami obowiązujących aktów prawnych, sposobu przetwarzania informacji zawierających dane osobowe, a przede wszystkim zapewnienie ochrony przetwarzanych danych osobowych przed wszelkiego rodzaju zagrożeniami, tak zewnętrznymi jak i wewnętrznymi. Jest ona oparta na analizie zagrożeń i ryzyku przy przetwarzaniu danych osobowych.

1.2. Uczelnia realizując politykę bezpieczeństwa danych wyznacza osoby odpowiedzialne za bieżącą realizację polityki na jej terenie oraz jednostek organizacyjnych, **w szczególności osoby odpowiedzialne za bezpieczeństwo danych osobowych:**

1.2.1. **lokalni administratorzy danych osobowych** (LADO), odpowiedzialni za nadzór nad przetwarzaniem danych osobowych, w podległej sobie strukturze, zgodnie z przepisami niniejszej PBI i SZBI;

1.2.2. **inspektor ochrony danych (INSPEKTOR)**, odpowiedzialny za nadzór nad przestrzeganiem zasad ochrony danych osobowych na obszarze Uczelni;

1.2.3. **administratorzy systemów informatycznych** (ASI);

1.2.4. **podmiot przetwarzający -** oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora;

1.2.5. **Osoby odpowiedzialne** w Uczelni za nadzór oraz za funkcjonowanie systemu przetwarzania i ochrony danych osobowych, zobowiązane są do współdziałania z organem ochrony danych osobowych, w przypadku kontroli lub zapytań kierowanych do Uczelni, mając świadomość, iż udaremnianie lub utrudnianie wykonania czynności kontrolnej podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności.

1.3. Przetwarzanie danych osobowych oraz dokumenty w zakresie przetwarzania danych osobowych podlega planowemu i doraźnemu sprawdzeniu przez **INSPEKTORA.**

1.4. Schemat organizacyjny struktury odpowiedzialności funkcjonalnej w zakresie ochrony danych osobowych obrazuje *załącznik nr 8 do niniejszej PBI*.

2. Przywołania prawne.

2.1. Dokumentacja ochrony danych osobowych, którą stanowi PBI i instrukcja zarządzania systemami teleinformatycznymi służącymi do przetwarzania danych osobowych została opracowana na podstawie niżej wymienionych aktów prawnych:

2.1.1. Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych – zwana dalej „ustawą" (Dz. U. 2019 r., poz. 1781);

2.1.2. Ustawa z dnia 5 sierpnia 2010 roku o ochronie informacji niejawnych (Dz. U. z 2010 roku, Nr 182, poz. 1228 z późn. zm.);

2.1.3. Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2014 r. poz. 1114 z późn. zm.) albo bezpiecznego podpisu elektronicznego weryfikowanego za pomocą ważnego kwalifikowanego certyfikatu, na

zasadach określonych w ustawie z dnia 18 września 2001 r. o podpisie elektronicznym (Dz. U. z 2013 r. poz. 262 z późn. zm.);

2.1.4. Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. 2016 z roku, poz. 113 z późn. zm.);

2.1.5. Rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE, zwane dalej rozporządzeniem.

2.2. Dokumentacja ochrony danych osobowych w Akademii Pomorskiej w Słupsku służy realizacji zadań wynikających z art.11 ust.1[1] ustawy z dnia 20 lipca 2018 r. - Prawo o szkolnictwie wyższym i nauce (tj. Dz. U. z 2021 r., poz. 478). W szczególności dane osobowe przetwarza się:

2.2.1. Dla zabezpieczania prawidłowego toku realizacji zadań dydaktycznych, naukowych i organizacyjnych Uczelni wynikających z przywołanych powyżej przepisów;

2.2.2. Dla zapewnienia prawidłowej, zgodnej z prawem i celami Uczelni polityki personalnej oraz bieżącej obsługi stosunków pracy nawiązywanych przez Uczelnię;

2.2.3. Dla realizacji innych celów i zadań Uczelni – z poszanowaniem praw i wolności osób powierzających Uczelni swoje dane.

3. Definicje stosowane w niniejszej Polityce Bezpieczeństwa Informacji.

1) Administrator (ADO) - osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych;

[1] Art. 11. 1. Podstawowymi zadaniami uczelni są:
1) prowadzenie kształcenia na studiach;
2) prowadzenie kształcenia na studiach podyplomowych lub innych form kształcenia;
3) prowadzenie działalności naukowej, świadczenie usług badawczych oraz transfer wiedzy i technologii do gospodarki;
4) prowadzenie kształcenia doktorantów;
5) kształcenie i promowanie kadr uczelni;
6) stwarzanie osobom niepełnosprawnym warunków do pełnego udziału w:
a) procesie przyjmowania na uczelnię w celu odbywania kształcenia,
b) kształceniu,
c) prowadzeniu działalności naukowej;
7) wychowywanie studentów w poczuciu odpowiedzialności za państwo polskie, tradycję narodową, umacnianie zasad demokracji i poszanowanie praw człowieka;
8) stwarzanie warunków do rozwoju kultury fizycznej studentów;
9) upowszechnianie i pomnażanie osiągnięć nauki i kultury, w tym przez gromadzenie i udostępnianie zbiorów bibliotecznych, informacyjnych i archiwalnych;
10) działanie na rzecz społeczności lokalnych i regionalnych.
2. Podstawowym zadaniem uczelni zawodowej jest również prowadzenie kształcenia specjalistycznego.
3. Zadania, o których mowa w ust. 1 pkt 3, 4 i pkt 6 lit. c, nie są podstawowymi zadaniami uczelni zawodowej.
4. Zadaniem uczelni publicznej prowadzącej kształcenie w zakresie nauk medycznych lub nauk o zdrowiu albo w zakresie nauk weterynaryjnych może być także uczestniczenie w sprawowaniu opieki medycznej albo weterynaryjnej w zakresie i formach określonych w przepisach o działalności leczniczej albo przepisach o zakładach leczniczych dla zwierząt.
5. Uczelnia może prowadzić domy studenckie i stołówki studenckie.

2) **INSPEKTOR –** inspektor ochrony danych – osoba fizyczna, którą administrator danych osobowych wyznaczył do zapewnienia przestrzegania przepisów o ochronie danych osobowych;
3) **ASI** – administrator systemu informatycznego – osoba odpowiedzialna za: przetwarzanie danych osobowych w systemach teleinformatycznych, opiniowanie wniosków o nadawanie/cofanie zakresu uprawnień dostępu do systemu i sposobu zabezpieczenia tego dostępu, w tym w szczególności za przeciwdziałanie dostępowi osób trzecich do systemów oraz podejmowanie odpowiednich działań w przypadku wykrycia naruszeń w tych systemach;
4) **Dane osobowe** - oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można 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;
5) **Główny Użytkownik Systemu (GUS)** - jednostka organizacyjna Uczelni odpowiedzialna za całokształt przetwarzania i utrzymywania systemu teleinformatycznego eksploatowanego w zakresie swojego działania, kierujący jednostką organizacyjną;
6) **Hasło** - ciąg znaków literowych, cyfrowych lub innych specjalnych znany jedynie osobie uprawnionej do pracy w systemie informatycznym;
7) **LADO** - lokalny administrator danych osobowych **– prorektorzy**, **dyrektor ds. organizacyjny, dyrektorzy instytutów (kierownicy samodzielnych katedr), dyrektor Biblioteki Uczelnianej, kierownik Osiedla Akademickiego.**;
8) **Identyfikator** – elektroniczne, indywidualne oznaczenie pracowników Uczelni w systemie teleinformatycznym, tzw. login, który tworzy ciąg znaków literowych, cyfrowych lub innych specjalnych, jednoznacznie identyfikujących osobę upoważnioną do przetwarzania danych w systemie informatycznym;
9) **Integralność danych** — właściwość zapewniająca, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany;
10) **Poufność danych** — właściwość zapewniająca, że dane nie są udostępniane nieupoważnionym podmiotom;
11) **Odbiorca danych** - oznacza 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;
12) **Strona trzecia** - osoba fizyczna lub prawna, organ publiczny, jednostka lub podmiot inny niż osoba, której dane dotyczą, administrator, podmiot przetwarzający czy osoby, które – z upoważnienia administratora lub podmiotu przetwarzającego – mogą przetwarzać dane osobowe;
13) **Pracownik** – osoba zatrudniona w AP w oparciu o umowę o pracę lub umowę cywilno-prawną oraz osoba odbywającą na Uczelni staż absolwencki, praktykę studencką, wolontariat, student, doktorant;

14) **Przetwarzanie danych** – oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak **zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie….;**
15) **System teleinformatyczny** – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;
16) **Podmiot przetwarzający** - oznacza **osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora**.
17) **Użytkownik** – pracownik Uczelni, zatrudniony na podstawie umowy o pracę, umowy zlecenia lub innych umów przewidzianych przepisami prawa oraz osoba odbywającą na Uczelni staż absolwencki, praktykę studencką, wolontariat, student, doktorant, który przetwarza dane osobowe znajdujące się w zbiorach danych Uczelni i posiada upoważnienie wydane przez Inspektora;
18) **Zbiór danych** – uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie;
19) **Ograniczenie przetwarzania** - oznaczenie przechowywanych danych osobowych w celu ograniczenia ich przyszłego przetwarzania;
20) **Profilowanie** - dowolna forma zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się;
21) **Pseudonimizacja** - przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej;
22) **Zgoda osoby, której dane dotyczą** - dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych;
23) **Naruszenie ochrony danych osobowych** - naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych;
24) **Podmiot Systemu Teleinformatycznego –** podmiot przetwarzający, który przetwarza dane osobowe znajdujące się w zbiorach danych Uczelni, posiada nadane uprawnienia do dostępu do zbiorów i upoważnienie wydane przez ADO;
25) **Dane genetyczne -** dane osobowe dotyczące odziedziczonych lub nabytych cech genetycznych osoby fizycznej, które ujawniają niepowtarzalne informacje o fizjologii lub zdrowiu tej osoby i które wynikają w szczególności z analizy próbki biologicznej pochodzącej od tej osoby fizycznej;

26) Dane biometryczne - dane osobowe, które wynikają ze specjalnego przetwarzania technicznego, dotyczą cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej oraz umożliwiają lub potwierdzają jednoznaczną identyfikację tej osoby, takie jak wizerunek twarzy lub dane daktyloskopijne;

27) Dane dotyczące zdrowia - dane osobowe o zdrowiu fizycznym lub psychicznym osoby fizycznej – w tym o korzystaniu z usług opieki zdrowotnej – ujawniające informacje o stanie jej zdrowia;

4. Polityka Bezpieczeństwa Informacji zakresie ochrony danych osobowych:

4.1. Administratorem danych osobowych gromadzonych i przetwarzanych jest Akademia Pomorska w Słupsku.

4.2. Zakres danych osobowych przetwarzanych przez podmiot nie może być szerszy niż powierzony do przetwarzania przez Administratora danych osobowych.

4.3. Dane osobowe przetwarzane na Uczelni są wykorzystywane wyłącznie do realizacji celów i zadań AP;

4.4. Polityka Bezpieczeństwa Informacji (wersja 1.0) została wprowadzona Zarządzeniem Rektora Nr R.021.53.18 z dnia 30 maja 2018 r., w dniu 6 maja 2021 r. wprowadzono aktualizowaną PBI (wersja 2,0) oraz została udostępniona wszystkim pracownikom na stronie internetowej AP (www.si.apsl.edu.pl);

4.5. Polityka bezpieczeństwa określa:

4.5.1. sposób przetwarzania danych osobowych oraz środki organizacyjne i techniczne zapewniające ochronę tych danych;

4.5.2. podstawowe warunki techniczne i organizacyjne, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych;

4.5.3. wymagania w zakresie odnotowywania udostępniania i bezpieczeństwa przetwarzania danych osobowych;

4.5.4. instrukcję postępowania w sytuacji naruszenia ochrony danych osobowych;

4.5.5. wykaz budynków, pomieszczeń lub części pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe;

4.5.6. wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych;

4.5.7. rejestr czynności przetwarzanych danych osobowych;

4.5.8. opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi;

4.5.9. sposób przepływu informacji pomiędzy poszczególnymi systemami;

4.5.10. środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności i rozliczalności przy przetwarzaniu danych osobowych.

4.5.11. wykaz podmiotów, którym powierzono przetwarzanie danych osobowych.

5. Zastosowane zabezpieczenia.

Zastosowane zabezpieczenia mają służyć osiągnięciu powyższych celów i zapewnić:

1) **poufność danych** – rozumianą, jako właściwość zapewniającą, że dane osobowe nie są udostępniane nieupoważnionym osobom;
2) **integralność danych** – rozumianą, jako właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany;
3) **rozliczalność danych** - rozumianą, jako właściwość zapewniającą, że działania osoby mogą być przypisane w sposób jednoznaczny tylko tej osobie;
4) **integralność systemu** - rozumianą, jako nienaruszalność systemu, niemożność jakiejkolwiek manipulacji zamierzonej, jak i przypadkowej;
5) **dostępność informacji** - rozumianą, jako zapewnienie, że osoby upoważnione mają dostęp do informacji i związanych z nią zasobów wtedy, gdy jest to potrzebne;
6) **zarządzanie ryzykiem** - rozumiane, jako proces identyfikowania, kontrolowania i minimalizowania lub eliminowania ryzyka dotyczącego bezpieczeństwa, które może dotyczyć systemów informacyjnych służących do przetwarzania danych osobowych.

6. ZASADY PRZETWARZANIA DANYCH OSOBOWYCH.

6.1 Podstawy prawne przetwarzania danych.

6.1.1 Uczelnia przetwarza dane osobowe wyłącznie w przypadku, jeśli spełniony jest co najmniej jeden z poniższych warunków:

6.1.1.1 przetwarzanie jest niezbędne do **wypełnienia obowiązku prawnego** ciążącego na Uczelni;

6.1.1.2 przetwarzanie jest **niezbędne do wykonania umowy**, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy;

6.1.1.3 przetwarzanie jest niezbędne do wykonania **zadania realizowanego w interesie publicznym** lub w ramach sprawowania władzy publicznej powierzonej Uczelni;

6.1.1.4 przetwarzanie jest niezbędne do celów wynikających z **prawnie uzasadnionych interesów realizowanych przez Uczelnię**, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych;

6.1.1.5 osoba, której dane dotyczą **wyraziła zgodę** na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów;

6.1.1.6 przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej.

6.2 Przetwarzanie danych osobowych przez uczelnie publiczne opiera się przede wszystkim na obowiązku prawnym administratora (art. 6 ust. 1 lit. c RODO, przepisy ustawy Prawo o szkolnictwie wyższym i nauce, a w zakresie kształtowania praw, obowiązków i sytuacji kandydatów/studentów w drodze decyzji administracyjnych wydawanych w trybie przepisów kodeksu postępowania administracyjnego), a także na realizacji umowy (art. 6 ust. 1 lit. b RODO) lub na uzasadnionym interesie administratora (art. 6 ust. 1 lit. f RODO)/realizacji zadań w interesie publicznym (art. 6 ust. 1 lit. e RODO).

6.3 W szczególnie uzasadnionych przypadkach przetwarzanie może być oparte na przesłance żywotnych interesów osoby fizycznej lub innych osób (art. 6 ust. 1 lit. d. RODO).

6.4 Zgoda osoby, której dane dotyczą (art. 6 ust. 1 lit. a RODO) będzie stanowić podstawę przetwarzania danych osobowych studentów, doktorantów lub innych osób w sytuacjach, gdy przetwarzanie nie wynika z przepisu prawa i wiąże się z dobrowolnym przekazywaniem danych osobowych, nie związanym bezpośrednio z tokiem kształcenia.

6.5 Legalność przetwarzania zapewniona jest w przypadku przetwarzania danych w oparciu o jedną z przesłanek wymienionych w ust. 6.1.

6.6 Uczelnia przetwarza dane osobowe należące do szczególnych kategorii wyłącznie w przypadku, jeśli spełniony jest co najmniej jeden z poniższych warunków:

6.6.1 przetwarzanie jest niezbędne do **wypełnienia obowiązków i wykonywania szczególnych praw przez uczelnię lub osobę, której dane dotyczą, w dziedzinie prawa pracy, zabezpieczenia społecznego i ochrony socjalnej**, o ile jest to dozwolone prawem Unii lub prawem państwa członkowskiego, lub porozumieniem zbiorowym na mocy prawa państwa członkowskiego przewidującymi odpowiednie zabezpieczenia praw podstawowych i interesów osoby, której dane dotyczą;

6.6.2 przetwarzanie jest niezbędne ze względów związanych z **ważnym interesem publicznym**, realizowanym na podstawie przepisów prawa;

6.6.3 przetwarzanie jest niezbędne do **celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych**;

6.6.4 osoba, której dane dotyczą, wyraziła **wyraźną zgodę** na przetwarzanie tych danych osobowych w jednym lub kilku konkretnych celach;

6.6.5 przetwarzanie jest niezbędne do **ochrony żywotnych interesów osoby**, której dane dotyczą, lub innej osoby fizycznej, a osoba, której dane dotyczą, jest fizycznie lub prawnie niezdolna do wyrażenia zgody.

6.7 Obszary przetwarzania danych w uczelni

6.7.1 Przetwarzanie <u>w oparciu o obowiązek prawny uczelni</u> (art. 6 ust. 1 lit. c RODO) znajduje zastosowanie w następujących procesach:

6.7.1.1 rekrutacja kandydatów na studia I, II lub III stopnia lub studia podyplomowe realizowana w oparciu o przepisy ustawy Prawo o szkolnictwie wyższym i nauce;

6.7.1.2 dokumentowanie przebiegu studiów realizowane w oparciu o przepisy ustawy Prawo o szkolnictwie wyższym i nauce, rozporządzenia ministra do spraw szkolnictwa wyższego w sprawie dokumentacji przebiegu studiów, rozporządzenia ministra do spraw szkolnictwa wyższego w sprawie podejmowania i odbywania przez

cudzoziemców studiów i szkoleń oraz ich uczestniczenia w badaniach naukowych i pracach rozwojowych, w tym przetwarzanie danych osobowych studentów, nauczycieli akademickich – w zakresie związanym z dokumentacją przebiegu studiów;

6.7.1.3 recenzowania osiągnięć naukowych w postępowaniach o nadanie stopnia doktora lub tytułu naukowego doktora habilitowanego;

6.7.1.4 udzielanie pomocy materialnej, przydzielanie miejsca w domu studenckim, stypendia, zapomogi, realizowane w trybie przepisów K.P.A., ustawy Prawo o szkolnictwie wyższym i nauce oraz uczelnianych regulaminów w zakresie ustalania, przyznawania i wypłacania świadczeń pomocy materialnej;

6.7.1.5 kontakt ze studentami w sprawach studenckich, związanych z tokiem kształcenia;

6.7.1.6 wykonywanie przez Uczelnię obowiązków sprawozdawczych (np. POL-on) archiwalnych, statystycznych, rachunkowych, księgowych, w tym na podstawie przepisów: ustawy Prawo o szkolnictwie wyższym i nauce, ustawy z dnia 29 września 1994 r. o rachunkowości (Dz. U. Nr 121, poz. 591 ze zm.), ustawy z dnia 29 czerwca 1995 r. o statystyce publicznej (Dz. U. Nr 88, poz. 439 ze zm.), ustawa z dnia 14 lipca 1993 r. o narodowym zasobie archiwalnym i archiwach (t.j. Dz. U. 2018, poz. 217);

6.7.1.7 wykonywanie obowiązków rachunkowo-podatkowych oraz dotyczących rozliczeń finansowych, dla których niezbędne jest przetwarzanie danych osobowych w dokumentach finansowych i innych dokumentach potwierdzających wykonane operacje gospodarcze w oparciu o przepisy ustawy z dnia 29 września 1994 r. o rachunkowości (Dz. U. Nr 121, poz. 591 ze zm.), ustawy z dnia 11 marca 2004 r. o podatku od towarów i usług (Dz. U. Nr 54, poz. 535 ze zm.)., ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych (Dz. U. Nr 157, poz. 1240 ze zm.);

6.7.1.8 udostępnianie zasobów bibliotecznych studentom i pracownikom w oparciu o przepisy ustawy Prawo o szkolnictwie wyższym i nauce;

6.7.1.9 dokumentowanie procesu zatrudnienia w uczelniach realizowane w oparciu o przepisy Kodeksu Pracy, Prawo o szkolnictwie wyższym i nauce i przepisy wykonawcze, w tym także przetwarzanie danych pracowników w przypadku monitoringu wizyjnego.

6.7.2 Przetwarzanie w oparciu o wykonywanie zadań realizowanych w interesie publicznym (art. 6 ust. 1 lit. e RODO) może być podstawą przetwarzania danych w przypadkach:

6.7.2.1 realizacji projektów edukacyjno-informacyjnych dla studentów, podejmowanych w celu rozwoju ich kompetencji i umiejętności np. warsztaty, konferencje, doradztwo zawodowe,

6.7.2.2 nawiązywanie kontaktu z prelegentami i uczestnikami w celu zaproszenia na konferencję/seminarium/wydarzenie o profilu naukowym lub popularyzujące naukę.

6.7.2.3 stosowania monitoringu wizyjnego.

6.7.3 Przetwarzanie w oparciu o uzasadniony interes administratora (art. 6 ust. 1 lit. f RODO) znajdzie zastosowanie w następujących obszarach:

6.7.3.1 ochrona interesów administratora, w tym dochodzenie roszczeń, prowadzenie postępowań spornych, postępowań przed organami władzy publicznej, innych postępowań w celu dochodzenia roszczeń,

6.7.3.2 przetwarzanie danych osób reprezentujących kontrahentów.

6.7.4 Przetwarzanie w oparciu o żywotny interes osoby fizycznej (art. 6 ust. 1 lit. d RODO) powinno być uzupełniającą podstawą przetwarzania danych, przede wszystkim w przypadku sytuacji nadzwyczajnych, w których przetwarzanie nie może być oparte na innej podstawie, np. kontakt/podanie danych osoby w sprawach niecierpiących zwłoki, związanych z zagrożeniem życia lub zdrowia tej osoby, np. nagłe niebezpieczeństwo podczas Juwenaliów wymagające podania danych studenta.

6.7.5 Przetwarzanie w oparciu o zgodę osoby fizycznej (art. 6 ust. 1 lit. a RODO) powinno stanowić podstawę przetwarzania danych osobowych w Uczelniach w następujących obszarach:

6.7.5.1 dane osobowe kandydatów i absolwentów:

6.7.5.1.1 dane kontaktowe kandydatów niezrekrutowanych (adres e-mail, numer telefonu) w celu podtrzymywania kontaktu z uczelnią;

6.7.5.1.2 monitoring kariery zawodowej po ukończeniu studiów;

6.7.5.1.3 informowanie absolwentów o możliwości podejmowania dodatkowych aktywności edukacyjnych.

6.7.5.2 dane osobowe uczestników wydarzeń i programów mobilności naukowej:

6.7.5.2.1 uczestnictwo w konferencjach, sympozjach, seminariach;

6.7.5.2.2 uczestnictwo w programach mobilności naukowej przez kadrę przyjeżdżającą, o ile osoba nie jest stroną umowy;

6.7.5.2.3 uczestnictwo w programach mobilności naukowej przez kadrę przyjeżdżającą.

6.7.5.3 dane osobowe kandydatów do pracy w zakresie wykraczającym poza katalog podany w Kodeksie pracy,

6.7.5.4 dane wnioskodawców i członków rodziny przy świadczeniach socjalnych dla pracowników uczelni;

6.7.5.5 korzystanie z zasobów bibliotecznych przez: absolwentów, współpracowników i inne osoby.

6.7.6 Przetwarzanie w oparciu o umowę, której stroną jest osoba, której dane dotyczą (art. 6 ust. 1 lit. B RODO oraz – jednocześnie - obowiązek prawny Uczelni (art. 6 ust. 1 lit. c RODO) np. wynikający z ustawy z dnia 29 września 1994 r. o rachunkowości (Dz. U. Nr 121, poz. 591 ze zm.), znajduje zastosowanie w następujących procesach:

6.7.6.1 współpracy z nauczycielami akademickimi na podstawie umów cywilnoprawnych,

6.7.6.2 współpracy z osobami w oparciu o stosunek prawny wolontariatu,

6.7.6.3 realizacji studenckich programów mobilności,

6.7.6.4 zawierania umów z dostawcami będącymi osobami fizycznymi, w tym - osobami fizycznymi prowadzącymi jednoosobową działalność gospodarczą (umowa, przepis),

6.7.6.5 zawierania umów cywilnoprawnych z recenzentami w procesach wydawniczych oraz postępowaniach o nadanie stopni i tytułów naukowych,

6.7.6.6 zawierania umów o kształcenie w ramach tzw. innych form kształcenia (kursy dokształcające, szkoły letnie).

6.7.7 Przetwarzanie w oparciu o umowę, której stroną jest osoba, której dane dotyczą (art. 6 ust. 1 lit. B RODO) znajduje zastosowanie przy zawieraniu umów z zakresu prawa autorskiego w procesach wydawniczych, Umowa nie może być podstawą przetwarzania danych osoby fizycznej, jeżeli osoba,

której dane dotyczą nie jest stroną takiej umowy (np. w przypadku umów o mobilności naukowe, jeżeli stronami umowy są uczelnie). Uczelnia przetwarza dane kontaktowe osób fizycznych wskazanych w umowach, których stronami są osoby prawne na podstawie art. 6 ust. 1 lit. e/f RODO.

6.8 Do stosowania zasad określonych przez dokumenty *Polityki Bezpieczeństwa Informacji* zobowiązane są osoby przetwarzające dane osobowe w AP. Każda osoba, mająca dostęp do danych osobowych przetwarzanych w AP jest zobowiązana do zapoznania się z niniejszym dokumentem.

6.9 Obszarem przetwarzania danych osobowych są budynki, pomieszczenia, w których są przetwarzane dane osobowe (serwerownia, sekretariaty instytutów, pokoje administracji, portiernie, …).

6.10 Dostęp do pomieszczeń, w których przetwarzane są dane osobowe:

6.10.1 dostęp do budynków i pomieszczeń Uczelni, w których przetwarzane są dane osobowe podlega całodobowej kontroli dostępu;

6.10.2 kontrola dostępu polega na ewidencjonowaniu wszystkich przypadków pobierania i zwrotu kluczy do budynków i pomieszczeń. W ewidencji uwzględnia się: imię i nazwisko osoby pobierającej lub zdającej klucz, numer lub inne oznaczenie pomieszczenia lub budynku oraz godzinę pobrania lub zdania klucza, podpis osoby pobierającej i zdającej klucze;

6.10.3 klucze lub kody dostępu do budynków lub pomieszczeń, w których przetwarzane są dane osobowe wydawane mogą być wyłącznie pracownikom upoważnionym do przetwarzania danych osobowych lub innym pracownikom upoważnionym do dostępu do tych budynków, lub pomieszczeń na innych zasadach;

6.10.4 GUS zbiorów danych osobowych, w jednostkach organizacyjnych, w których przetwarzane są dane osobowe są zobowiązani do niezwłocznego przekazywania do Inspektora informacji o zmianie lub powstaniu nowej lokalizacji miejsc przetwarzania danych osobowych, jednocześnie informując o tym służby dozoru w odpowiednich budynkach;

6.10.5Uczelnia na potrzeby PBI w zakresie ochrony danych osobowych może wprowadzać inne formy monitorowania dostępu do obszarów przetwarzania danych osobowych;

6.10.6 w przypadku, gdy w pomieszczeniu znajduje się część ogólnodostępna oraz część, w której przetwarzane są dane osobowe – część, w której są przetwarzane dane osobowe powinna być wyraźnie oddzielona od ogólnodostępnej;

6.10.7 wydzielenie części pomieszczenia, w której przetwarza się dane osobowe może być w szczególności realizowane poprzez montaż barierek, lad lub odpowiednie ustawienie mebli biurowych, uniemożliwiające lub co najmniej ograniczające niekontrolowany dostęp osób niepowołanych do zbiorów danych osobowych przetwarzanych w danym pomieszczeniu;

6.10.8 w budynkach, pomieszczeniach i częściach pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe mają prawo przebywać wyłącznie osoby upoważnione do dostępu lub przetwarzania danych osobowych oraz osoby sprawujące nadzór i kontrolę nad bezpieczeństwem przetwarzania tych danych, za wyjątkiem przypadków, o których mowa w ppkt. 6.10.9 poniżej;

6.10.9 osoby nieupoważnione do przetwarzania danych osobowych mogą przebywać w budynkach, pomieszczeniach i częściach pomieszczeń, tworzących obszar Uczelni, w którym przetwarzane są dane osobowe - wyłącznie w obecności upoważnionego

pracownika lub w razie jego nieobecności, na podstawie upoważnienia wydanego przez LADO lub inną upoważnioną osobę;

6.10.10 opuszczenie pomieszczenia, w którym przetwarzane są dane osobowe, musi wiązać się z zastosowaniem dostępnych środków zabezpieczających używane aktualnie zbiory danych osobowych. W szczególności w razie planowanej, choćby chwilowej, nieobecności pracownika upoważnionego do przetwarzana danych osobowych, obowiązany jest on umieścić zbiory występujące w formach tradycyjnych w odpowiednio zabezpieczonym miejscu ich przechowywania oraz dokonać niezbędnych operacji w systemie informatycznym uniemożliwiającym dostęp do danych osobowych osobom niepowołanym;

6.10.11 opuszczenie przez pracownika przetwarzającego dane osobowe obszaru ich przetwarzania bez zabezpieczenia pomieszczenia oraz umiejscowionych w nim zbiorów danych jest niedopuszczalne i jako takie traktowane będzie jako naruszenie podstawowych obowiązków pracowniczych.

6.11 Wykaz budynków, pomieszczeń lub części pomieszczeń tworzących obszar przetwarzania danych osobowych, stanowi *załącznik nr 3 do PBI;*

6.12 Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych, opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi oraz sposób przepływu danych pomiędzy poszczególnymi systemami, stanowią *załącznik nr 4 do PBI;*

6.13 Podstawowe zbiory danych osobowych w AP, to zbiory zawierające dane: kandydatów na studia, studentów, doktorantów, absolwentów, kandydatów na pracowników, pracowników, byłych pracowników, gości DS., członków związków i organizacji, stron umów cywilnoprawnych, kontrahentów, uczestników studiów podyplomowych, uczestników kursów, szkoleń i konferencji, osób korzystających z Biblioteki Uczelnianej, osób przeprowadzających postępowania o uzyskanie w Uczelni stopnia naukowego;

6.14 W Uczelni dane osobowe przetwarzane są w zbiorach, jak poniżej:

6.14.1 **Zbiór PRACOWNIK –** w nim moduły: HMS/kadr, HMS/plac, HMS/usso, HMS/bfpl, HMS/uzus; przetwarzanie danych tekstowych i rachunkowych – programy: Microsoft Word i Microsoft Excel, pakiet Open Office;

6.14.2 **Zbiór STUDENT –** w nim moduły: HMS/dsys, eHMS/dsys, HMS/dees; przetwarzanie danych tekstowych i rachunkowych – programy: Microsoft Word i Microsoft Excel, pakiet Open Office;

6.14.3 **Zbiór REKRUTACJA –** w nim moduły: eHMS/irka; przetwarzanie danych tekstowych i rachunkowych – programy: Microsoft Word i Microsoft Excel, pakiet Open Office;

6.14.4 **Zbiór CZYTELNIK –** program PROLIB, w nim moduł WYPOŻYCZALNIA zawierający dane osobowe;

6.14.5 **Zbór Gość DS. –** program: Microsoft Word – stacje robocze;

6.14.6 **Zbiór Kontrahent -** program: Microsoft Word – stacje robocze.;

6.14.7 **Zbiór Monitoring wizyjny** – program Microsoft – stacja robocza;

6.14.8 **Zbiór doraźny –** tworzone wyłącznie ze względów technicznych, szkoleniowych, konkursowych lub w związku z dydaktyką na Uczelni itp.;

6.15 Wykaz z lokalizacją zbiorów, w tym modułów programowych *zawiera załącznik nr 9 do PBI.*

6.16 Należy zgłaszać do Inspektora wszelkie nowe powstałe zbiory danych, modyfikacje, aktualizacje, likwidacje według *załącznika nr 19 do niniejszej PBI*.

6.17 Opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi przepływy danych (załącznik nr 8 *do PBI*);

6.18 Wszystkie osoby, które przetwarzają dane osobowe w obszarze wymienionym w paragrafie 6.9, muszą posiadać pisemne upoważnienie do przetwarzania danych nadane przez **ADO lub wyznaczoną** osobę w imieniu ADO - (**Kierownik Sekcji Kadr i Spraw Socjalnych AP**) oraz podpisać oświadczenie o zachowaniu poufności tych danych. Wzór upoważnienia stanowi *załącznik nr 5 do niniejszej PBI*. Wzór oświadczenia o zachowaniu poufności stanowi *załącznik nr 7 do PBI;*

6.19 Upoważnienia do przetwarzania danych osobowych w systemie informatycznym wydawane są zgodnie z właściwą procedurą określoną w niniejszym dokumencie*;*

6.20 Upoważnienia, o których mowa w pkt. 6.19 , ważne są do dnia odwołania lub do chwili ustania zatrudnienia upoważnionego pracownika;

6.21 W zbiorach danych gromadzonych w systemie informatycznym zabrania się przetwarzania danych ujawniających:

6.21.1 pochodzenie rasowe lub etniczne;

6.21.2 poglądy polityczne;

6.21.3 przekonania religijne lub filozoficzne;

6.21.4 przynależność wyznaniową;

6.21.5 przynależność partyjną lub związkową;

6.21.6 dane genetyczne;

6.21.7 dane biometryczne;

6.21.8 nałogi;

6.21.9 preferencje seksualne, chyba że wymagają tego obowiązujące przepisy prawa lub osoba, której dane dotyczą, wyraziła na to pisemną zgodę.

6.22 Dane o skazaniach, w tym dane o niekaralności można przetwarzać wyłącznie pod nadzorem władz publicznych.

6.23 Do profilowania zabrania się używania danych wymienionych w pkt 6.21 niniejszego paragrafu, chyba, że osoba, której dane dotyczą wyraziła na to zgodę lub jest to podyktowane ważnym interesem publicznym.

6.24 O profilowaniu należy informować osobę, której ono dotyczy na etapie zbierania danych.

6.25 Dane osobowe mogą być wykorzystywane wyłącznie do celów, dla jakich były, są lub będą zbierane i przetwarzane. Po wykorzystaniu, dane osobowe powinny być przechowywane w formie uniemożliwiającej identyfikację osób, których dotyczą.

6.26 W przypadku konieczności udostępniania dokumentów i danych w nich zawartych, wśród których znajdują się dane osobowe niemające bezpośredniego związku z celem udostępnienia, należy bezwzględnie dokonać anonimizacji tych danych.

6.27 W przypadku, gdy dane osobowe osoby, od której zostały zebrane, są niekompletne, nieaktualne, nieprawdziwe, zostały zebrane z naruszeniem ustawy lub są zbędne do realizacji celu, dla którego zostały zebrane, ADO lub osoba przez niego upoważniona (LADO) jest zobowiązana do ich uzupełnienia, uaktualnienia, sprostowania lub usunięcia.

7. Powierzanie danych do przetwarzania.

7.1 Relacje uczelni i ich partnerów w przetwarzaniu danych osobowych.

7.1.1 **Uczelnia jako administrator -** w większości przypadków uczelnia jest administratorem danych. Oznacza to, że samodzielnie decyduje, w jakim celu i w jaki sposób przetwarza dane osobowe i ponosi za to odpowiedzialność. Wynika to z tego, że uczelnia ma obowiązek realizowania swoich własnych zadań, co nierozerwalnie wiąże się z przetwarzaniem danych osobowych.

7.1.2 **Relacja: uczelnia (administrator) i podmiot przetwarzający -** Uczelnia, jako administrator, może zlecić przetwarzanie danych innemu podmiotowi – np. świadczącemu usługi informatyczne – który staje się podmiotem przetwarzającym. Uczelnia powierza dane osobowe w przypadku korzystania z usług podwykonawców (wsparcie techniczne, inne usługi zewnętrzne związane z dostępem do danych). Uczelnia w takim przypadku powinna zawrzeć umowę, która musi zawierać postanowienia określone w art. 28 ust. 3 RODO. Podmiot przetwarzający nie ma, w przeciwieństwie do uczelni, kompetencji do decydowania o tym, jak przetwarzać dane osobowe. Może to robić tylko na zasadach określonych w umowie. Podmiot przetwarzający ma szereg obowiązków, m.in. poddania się kontroli uczelni – co wynika z odpowiedzialności uczelni za wybór podmiotu przetwarzającego.

Sytuacja odwrotna – gdy inny podmiot, będący administratorem, chce powierzyć przetwarzanie danych osobowych uczelni – która stałaby się podmiotem przetwarzającym – nie może być regułą w stosunkach uczelni z innymi podmiotami, w szczególności z sektora prywatnego. Przede wszystkim uczelnia nie działa, co do zasady, na zlecenie innych podmiotów (co jest charakterystyczne dla roli podmiotu przetwarzającego). Ponadto uczelnia legitymuje się podstawą prawną przetwarzania danych osobowych, która w większości przypadków wynika z przepisów prawa powszechnie obowiązującego. Nie da się pogodzić narzucenia uczelni roli podmiotu przetwarzającego z jej obowiązkami związanymi np. z zakresem przetwarzanych danych, czasem przechowywania, zasadami udostępniania danych innym podmiotom. Uczelnie, jako podmioty publiczne, działają na podstawie i w granicach przepisów prawa. Nie jest dopuszczalne modyfikowanie sposobu przetwarzania danych osobowych przez uczelnie – poprzez powierzenie im do przetwarzania danych na podstawie umowy cywilnoprawnej – bo de facto prowadzi to do modyfikowania sposobu wykonywania przez nie zadań i konieczność poddania się kontrolom przez podmioty prywatne, a także stosowanie się do ich zaleceń w zakresie ochrony danych osobowych.

7.1.3 **Relacja: uczelnia i inne uczelnie/partnerzy jako współadministratorzy –** współadministrowanie danymi polega na wspólnym ustalaniu celów i sposobów przetwarzania danych osobowych. Dotyczy to sytuacji, gdy współpraca z inną uczelnią lub partnerem jest tak ścisła, że wszystkie kluczowe decyzje są podejmowane wspólnie. Przykładem współadministrowania jest współorganizowanie konferencji naukowej. Zasady współadministrowania danymi powinny być określone w dwu- lub wielostronnej umowie, która określa zadania poszczególnych współadministratorów – w zakresie wywiązywania się przez nich z obowiązków wynikających z RODO.

7.1.4 **Relacja: uczelnia (administrator) i inny podmiot (administrator) -** w tej relacji kluczowe znaczenie ma to, że uczelnia (administrator – decydujący o celach i sposobach przetwarzania)

udostępnia dane osobowe innemu podmiotowi (administratorowi, decydującemu o celach i sposobach przetwarzania) – możliwa jest oczywiście sytuacja odwrotna – inny podmiot udostępnia dane uczelni. Tym, co odróżnia tę relację od innych jest to, że uczelnia i inny podmiot przetwarzają dane we własnych, odrębnych celach, zaś łączy je jedynie to, że udostępniają sobie dane osobowe. Udostępniając dane osobowe innej uczelni lub partnerowi uczelnia musi legitymować się podstawą prawną upoważniającą do takiego działania (najczęściej będzie to art. 6 ust. 1 lit. a lub lit. b RODO). Przykładem udostępnienia danych osobowych innemu administratorowi jest udostępnienie przez uczelnię danych jej studenta, biorącego udział w programie mobilności uczelni, do której wyjeżdża. W tym przypadku podstawą prawną udostępnienia jest konieczność wykonania umowy, której stroną jest student, doktorant. Udostępniając dane innemu podmiotowi uczelnia musi pamiętać o poinformowaniu o tym w klauzuli informacyjnej z art. 13 RODO. Otrzymując dane od inne podmiotu uczelnia musi pamiętać o spełnieniu obowiązku informacyjnego z art. 14 RODO – w tym wskazać źródło danych.

7.2 Powierzenie przetwarzanie innemu podmiotowi;

7.2.1 Do przetwarzania danych osobowych mogą być dopuszczeni jedynie pracownicy Akademii Pomorskiej oraz podmioty, którym powierzono przetwarzanie danych osobowych w związku z realizacją określonych celów i zadań (*prace doraźne o charakterze serwisowym lub innym usługom);*

7.2.2 Podmiot wymieniony w pkt 1 niniejszego paragrafu zobowiązany jest do podpisania z Akademią Pomorską umowy powierzenia przetwarzania danych osobowych. Wzór umowy stanowi *załącznik nr 11* do PBI;

7.2.3 Podmiot, któremu powierzono dane może przetwarzać je wyłącznie w zakresie przewidzianym w umowie;

7.2.4 Podmiot, o którym mowa w ust. 1 jest obowiązany przed rozpoczęciem przetwarzania danych podać środki zabezpieczające zbiór danych spełniające wymogi rozporządzenia 2016/679 oraz ustawy;

7.2.5 Umowa, o której mowa w ust. 1 powinna zapewnić AP możliwość kontroli zgodności przetwarzania danych z przepisami o ochronie danych osobowych w siedzibie podmiotu, będącym stroną umowy zarówno przed jak i w trakcie trwania umowy;

7.3 Udostępnienie innemu podmiotowi przetwarzanie danych;

7.3.1 Umowy zawierane przez Uczelnię z innymi podmiotami związane z dostępem do danych osobowych przetwarzanych w AP, muszą zawierać klauzule określające zakres ochrony danych osobowych zgodnie z PBI (*wzór umowy załącznik nr 12 do PBI)* w tym zobowiązanie do zachowania poufności. (*Wzór oświadczenia zawiera załącznik nr 7 do PBI)* i winny zawierać w szczególności:

7.3.1.1 cel i zakres udzielonych praw dostępu do danych osobowych przetwarzanych w AP;

7.3.1.2 prawa i obowiązki związane z udzielonym dostępem oraz okres ich obowiązywania;

7.3.1.3 oświadczenie o znajomości przepisów dotyczących ochrony danych osobowych;

7.3.1.4 zasady związane ze zmianą składu personelu świadczącego usługi;

7.3.1.5 tryb rozwiązywania kwestii spornych dotyczących bezpieczeństwa danych osobowych przetwarzanych w AP.

7.3.2 Udostępnianie danych osobowych innym podmiotom spoza Uczelni odbywa się według następującej procedury:

7.3.2.1 udostępnienie danych osobowych AP może nastąpić na pisemny, umotywowany wniosek innego podmiotu;

7.3.2.2 wniosek opiniuje odpowiedni LADO;

7.3.2.3 LADO przekazuje wniosek do Inspektora, który rejestruje zdarzenie i wydaje decyzję;

7.3.2.4 na wniosek odpowiada LADO zgodnie z decyzją Inspektor;

7.3.2.5 podstawa udzielenia dostępu do danych osobowych wynika z przepisów prawa oraz umowy zawartej pomiędzy AP, a innym podmiotem.

7.3.3 Zakres danych osobowych powierzanych, udostępniany przez Akademię Pomorską powinien być adekwatny do celu powierzenia, udostępnienia oraz udokumentowany w postaci wykazu podmiotów, którym powierzono dane osobowe, za każdym razem, gdy takie powierzenie nastąpi (*załącznik nr 14 do* PBI);

8. Zabezpieczenie przetwarzanych danych osobowych.

Przed rozpoczęciem przetwarzania danych osobowych, w Akademii Pomorskiej zastosowano środki zabezpieczające powierzone zbiory danych w postaci zabezpieczeń technicznych i organizacyjnych wymienionych poniżej:

8.1 Zabezpieczenia techniczne:

8.1.1 dokumenty zawierające dane osobowe w formie papierowej, upoważnione osoby przechowują w obszarze przetwarzania danych w pomieszczeniach zabezpieczonych drzwiami zamykanymi na klucz, w szafach zamykanych na klucz;

8.1.2 pomieszczenia, których przetwarzane są dane osobowe wyposażone są w przeciwwłamaniowy system alarmowy;

8.1.3 pomieszczenia, w których przetwarzane są dane osobowe są zabezpieczone przed skutkami pożaru;

8.1.4 dostęp do pomieszczeń, w których przetwarzane są dane osobowe kontrolowany jest przez system monitoringu;

8.1.5 do niszczenia niepotrzebnych dokumentów papierowych zawierających dane osobowe wykorzystuje się niszczarki;

8.1.6 dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła;

8.1.7 do ochrony danych osobowych przetwarzanych w komputerach stosuje się specjalne programy antywirusowe;

8.1.8 Akademia Pomorska dbając o bezpieczeństwo studentów, pracowników oraz mienia AP stosuje środki techniczne umożliwiając rejestrację obrazu – MONITORING (*załącznik nr 21 do PBI).*

8.2 Zabezpieczenia organizacyjne:

8.2.1 opracowanie i wdrożenie Polityki bezpieczeństwa informacji oraz Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych;

8.2.2 wyznaczenie inspektora ochrony danych;

8.2.3 dopuszczanie do przetwarzania danych osobowych wyłącznie osób posiadających ważne upoważnienia;

8.2.4 organizowanie cyklicznych szkoleń wewnętrznych dla pracowników z zakresu ochrony danych osobowych;

8.2.5 regularne wykonywanie kopii zapasowych zbiorów danych, zgodnie z przyjętą Instrukcją zarządzania systemem informatycznym służącym do przetwarzania danych osobowych;

8.2.6. przechowywanie kopii zapasowych w specjalnie do tego celu wyznaczonych i zabezpieczonych pomieszczeniach.

9. Odpowiedzialność.

9.1 Nieprzestrzeganie zasad ochrony danych osobowych grozi odpowiedzialnością cywilna wynikającą z art. 89 rozporządzenia 2016/679 ujęte w rozdziale 10 art. 89 – 93 ustawy, kary administracyjne art. 83 rozporządzenia 2016/679 zawarte w rozdziale 11 art. 94 - 100 ustawy oraz innych przepisów prawa powszechnie obowiązującego uwzględniających ww.

9.2 Odpowiedzialności karnej, zgodnie z ustawą podlega każdy pracownik, który:

9.2.1 Przetwarza dane osobowe, choć ich przetwarzanie nie jest dopuszczalne, albo do których przetwarzania nie jest uprawniony, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat dwóch.

9.2.2 Jeżeli czyn dotyczy danych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, danych genetycznych, biometrycznych, o stanie zdrowia, seksualności lub orientacji seksualnej, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat trzech;

9.2.3 Udaremniając lub utrudniając kontrolującemu prowadzenie kontroli przestrzegania przepisów o ochronie danych osobowych, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat dwóch.

9.3 Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu mogą być potraktowane, jako ciężkie naruszenie obowiązków pracowniczych, w szczególności przez osobę, która po stwierdzeniu naruszenia zabezpieczenia systemu informatycznego lub uzasadnionego domniemania takiego naruszenia nie powiadomiła o tym fakcie Inspektora.

10. Obowiązek informacyjny.

10.1 W przypadku zbierania danych osobowych od osoby, której one dotyczą, ADO jest obowiązany poinformować tę osobę podając:

10.1.1 dane administratora i dane kontaktowe;

10.1.2 dane kontaktowe inspektora ochrony danych osobowych;

10.1.3 cele przetwarzania danych osobowych, oraz podstawę prawną przetwarzania;

10.1.4 informację o odbiorcach danych osobowych;

10.1.5 okres, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteria ustalania tego okresu;

10.1.6 prawo do żądania od administratora dostępu do danych ich sprostowania, usunięcia lub ograniczenia przetwarzania lub o prawie do wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych;

10.1.7 prawo wniesienia skargi do organu nadzorczego;

10.1.8 podanie danych osobowych jest wymogiem ustawowym lub umownym lub warunkiem zawarcia umowy oraz czy osoba, której dane dotyczą, jest zobowiązana do ich podania i jakie są ewentualne konsekwencje niepodania danych;

10.1.9 gdy ma to zastosowanie – o zamiarze przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej;

10.2 W przypadku pozyskania danych osobowych z innego źródła, niż osoba, której dane dotyczą, ADO jest zobowiązany poinformować tę osobę podając:

10.2.1 dane administratora i dane kontaktowe;

10.2.2 dane kontaktowe inspektora ochrony danych osobowych;

10.2.3 cele przetwarzania danych osobowych, oraz podstawę prawną przetwarzania;

10.2.4 kategorii odnośnych danych osobowych;

10.2.5 informację o odbiorcach danych osobowych;

10.2.6 okres, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteria ustalania tego okresu;

10.2.7 prawo do żądania od administratora dostępu do danych ich sprostowania, usunięcia lub ograniczenia przetwarzania lub o prawie do wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych;

10.2.8 źródło pochodzenia danych osobowych;

10.2.9 prawo wniesienia skargi do organu nadzorczego;

10.2.10 gdy ma to zastosowanie – o zamiarze przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej;

10.3 Obowiązek poinformowania wymieniony w art.10.1 niniejszego paragrafu powinien być wykonany w momencie zbierania danych;

10.4 Obowiązek poinformowania wymieniony w art. 10.2 niniejszego dokumentu powinien zostać spełniony bezpośrednio po utrwaleniu zebranych danych, a więc po zapisaniu danych w sposób umożliwiający ich dalsze przetwarzanie.

11. INSPEKTOR OCHRONY DANYCH.

11.1 Inspektor ochrony danych (Inspektor) to pracownik Uczelni wyznaczony przez Administratora Danych Osobowych do zapewnienia przestrzegania przepisów ochrony danych osobowych na terenie Uczelni;

11.2 Inspektor wyznaczony jest zarządzeniem Rektora Nr. R.021.76.18 z dnia 24 sierpnia 2018r.;

11.3 Dokonano zawiadamia Prezesa Urzędu Ochrony Danych Osobowych o wyznaczeniu inspektora, wskazując imię, nazwisko, adres poczty elektronicznej lun numer telefonu inspektora;

11.4 Inspektor prowadzi rejestr czynności przetwarzanych danych na potrzeby realizacji celów i zadań Akademii Pomorskiej (*załącznik nr 16 do PBI)*. W rejestrze tym zamieszcza się następujące informacje:

11.4.1 nazwę oraz dane kontaktowe administratora oraz inspektora ochrony danych;

11.4.2 cele przetwarzania;

11.4.3 kategorie osób, których dane dotyczą, oraz kategorii danych osobowych;

11.4.4 kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w tym odbiorców w państwach trzecich lub w organizacjach międzynarodowych;

11.4.5 w stosownym przypadku informacje o stosowaniu profilowania;

11.4.6 w stosownym przypadku kategorie 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;

11.4.7 jeżeli jest to możliwe, planowane terminy usunięcia poszczególnych kategorii danych;

11.4.8 jeżeli jest to możliwe, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa.

11.5 Inspektor jest zobowiązany do przeprowadzania analizy ryzyk związanych z zagrożeniami związanymi z przetwarzaniem danych osobowych w systemie informatycznym oraz w systemie tradycyjnym (*załącznik nr 20 do PBI).*

11.6 Ponadto Inspektor prowadzi następujące wykazy:

11.6.1 wykaz osób, którym nadano upoważnienia do przetwarzania danych osobowych;

11.6.2 wykaz pomieszczeń, w których przetwarzane są dane osobowe, stanowiących obszar przetwarzania;

11.6.3 wykaz podmiotów i osób, którym udostępniono dane (*załącznik nr 14 do PBI*);

11.6.4 wykaz podmiotów, którym powierzono dane osobowe do przetwarzania.

11.7 Inspektor ochrony danych ma następujące zadania:

11.7.1 informowanie administratora, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy niniejszego rozporządzenia oraz innych przepisów Unii lub państw członkowskich o ochronie danych i doradzanie im w tej sprawie;

11.7.2 monitorowanie przestrzegania niniejszego rozporządzenia, innych przepisów Unii lub państw członkowskich o ochronie danych 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;

11.7.3 współpraca z organem nadzorczym Prezesem Urzędu Ochrony Danych Osobowych (PUODO);

11.7.4 pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w art. 36 rozporządzenia 2016/679, oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach.

11.7.5 Inspektor ochrony danych wypełnia swoje zadania z należytym uwzględnieniem ryzyka związanego z operacjami przetwarzania, mając na uwadze charakter, zakres, kontekst i cele przetwarzania.

12. WARUNKI KORZYSTANIA Z SYSTEMU INFORMATYCZNEGO.

12.1 Zgodnie z postanowieniami PBI, zabrania się Użytkownikowi systemu podejmowania jakichkolwiek czynności mających na celu naruszenie bezpieczeństwa przetwarzanych danych, w tym prób przełamania zabezpieczeń systemu;

12.2 Każdy Użytkownik jest zobowiązany do zapoznania się z zasadami korzystania z systemu informatycznego, opisanego w niniejszym dokumencie*;*

12.3 W celu zapobieżenia nieautoryzowanemu dostępowi do systemu informatycznego Użytkownik nie może udostępniać innej osobie swojego identyfikatora, hasła;

12.4 Zabronione jest korzystanie z systemu informatycznego z użyciem danych dostępowych innego Użytkownika.

12.5 Użytkownicy są zobowiązani do zachowania zasady bezpiecznego ustawienia monitora, czyli ustawienia w pozycji uniemożliwiającej podgląd osób nieuprawnionych*;*

12.6 Użytkownik zobowiązany jest do przestrzegania zasady czystego biurka - po zakończeniu pracy należy zabezpieczyć dokumenty z danymi osobowymi w szafach do tego przeznaczonych*;*

12.7 Użytkownik jest zobowiązany do przestrzegania zasady czystej drukarki/kopiarki - po zakończeniu pracy sprawdzić czy nie pozostawiono dokumentów, zbędne wydruki zniszczyć, wyłączyć drukarkę/kopiarkę.

13. Przetwarzanie danych osobowych z wykorzystaniem systemów teleinformatycznych.

13.1 Dane osobowe w AP są przetwarzane przy zastosowaniu systemów teleinformatycznych, w zbiorach danych oraz poza zbiorami;

13.2 Rektor zatwierdza poziom bezpieczeństwa systemów informatycznych do przetwarzania danych osobowych zgodnie z wzorem określonym *w załączniku nr 10 do PBI;*

13.3 Za zabezpieczenie systemów teleinformatycznych zgodnie z zatwierdzonym poziomem bezpieczeństwa odpowiadają właściwi ASI;

13.4 ASI stosują wszelkie dostępne im mechanizmy ochrony celem właściwego zabezpieczenia systemu do przetwarzania danych;

13.5 Systemy informatyczne służące do przetwarzania danych osobowych zabezpieczone są przed działaniami niepożądanymi na bieżąco aktualizowanymi przez Sekcję Informatyki systemami antywirusowymi;

13.6 Zbiory danych osobowych zlokalizowane są w przedmiotowych bazach danych umieszczonych na serwerach bazodanowych;

13.7 Dane osobowe w zbiorach są przetwarzane tylko w aplikacjach (programach) dostosowanych do merytorycznych potrzeb jednostek organizacyjnych Uczelni;

13.8 Przepływy danych pomiędzy poszczególnymi systemami teleinformatycznymi przetwarzającymi dane osobowe przedstawia w schemacie *załącznik nr 4 do PBI.*

14. POCZTA ELEKTRONICZNA, INTERNET W SYSTEMIE.

14.1 W systemie informatycznym wykorzystano funkcjonalność wysyłania powiadomień na adres e-mail podany w systemie;

14.2 Informacje zawierające dane osobowe przesyłane pocztą elektroniczną są szyfrowane.

14.3 Użytkownik zobowiązany jest do dbania o bezpieczeństwo konta mailowego, o którym mowa powyżej, w szczególności do:

14.3.1 używania silnego hasła dostępu;

14.3.2 nieotwierania załączników do poczty i linków pochodzących z nieznanych źródeł;

14.3.3 zachowania ostrożności podczas otwierania nieoczekiwanych załączników w korespondencji pochodzącej od znanych nadawców;

14.4 Użytkownik zobowiązany jest do korzystania z sieci Internet w sposób, który nie zagraża bezpieczeństwu danych gromadzonych i przetwarzanych w systemie.

15. POSTĘPOWANIE NA WYPADEK ZAGROŻENIA – NARUSZENIA BEZPIECZEŃSTWA DANYCH OSOBOWYCH.

15.1 Podział zagrożeń:

15.1.1 Zagrożenia losowe zewnętrzne (np. klęski żywiołowe, przerwy w zasilaniu), ich występowanie może prowadzić do utraty integralności danych, ich zniszczenia i uszkodzenia infrastruktury technicznej systemu, ciągłość systemu zostaje zakłócona – nie dochodzi do naruszenia poufności danych;

15.1.2 Zagrożenia losowe wewnętrzne (np. niezamierzone pomyłki operatorów, administratora, awarie sprzętowe, błędy oprogramowania), może dojść do zniszczenia danych, może zostać zakłócona ciągłość pracy systemu - może nastąpić naruszenie poufności danych;

15.1.3 Zagrożenia zamierzone, świadome i celowe - najpoważniejsze zagrożenia, naruszenia poufności danych, (zazwyczaj nie następuje uszkodzenie infrastruktury technicznej i zakłócenie ciągłości pracy), zagrożenia te możemy podzielić na:

15.1.3.1 Nieuprawniony dostęp do systemu z zewnątrz (włamanie do systemu);

15.1.3.2 Nieuprawniony dostęp do systemu z jego wnętrza;

15.1.3.3 Nieuprawniony przekaz danych;

15.1.3.4 Pogorszenie, jakości sprzętu i oprogramowania;

15.1.3.5 Bezpośrednie zagrożenie materialnych składników systemu.

15.2 Przypadki zakwalifikowane jako naruszenie lub uzasadnione podejrzenie naruszenia zabezpieczenia systemu informatycznego, w którym przetwarzane są dane osobowe to głównie:

15.2.1 Sytuacje losowe lub nieprzewidziane oddziaływanie czynników zewnętrznych na zasoby systemu jak np.: wybuch gazu, pożar, zalanie pomieszczeń, katastrofa budowlana, napad, działania terrorystyczne, niepożądana ingerencja ekipy remontowej itp.;

15.2.2 Niewłaściwe parametry środowiska, jak np. nadmierna wilgotność lub wysoka temperatura, oddziaływanie pola elektromagnetycznego, wstrząsy lub wibracje pochodzące od urządzeń przemysłowych;

15.2.3 Awaria sprzętu lub oprogramowania, które wyraźnie wskazują na umyślne działanie w kierunku naruszenia ochrony danych lub wręcz sabotaż, a także niewłaściwe działanie serwisu, a w tym sam fakt pozostawienia serwisantów bez nadzoru;

15.2.4 Pojawienie się odpowiedniego komunikatu alarmowego od tej części systemu, która zapewnia ochronę zasobów lub inny komunikat o podobnym znaczeniu;

15.2.5 Jakość danych w systemie lub inne odstępstwo od stanu oczekiwanego wskazujące na zakłócenia systemu lub inną nadzwyczajną i niepożądaną modyfikację w systemie;

15.2.6 Nastąpiło naruszenie lub próba naruszenia integralności systemu lub bazy danych w tym systemie;

15.2.7 Stwierdzono próbę lub modyfikację danych lub zmianę w strukturze danych bez odpowiedniego upoważnienia (autoryzacji);

15.2.8 Nastąpiła niedopuszczalna manipulacja danymi osobowymi w systemie;

15.2.9 Ujawniono osobom nieupoważnionym dane osobowe lub objęte tajemnicą procedury ochrony przetwarzania albo inne strzeżone elementy systemu zabezpieczeń;

15.2.10 Praca w systemie lub jego sieci komputerowej wykazuje nieprzypadkowe odstępstwa od założonego rytmu pracy wskazujące na przełamanie lub zaniechanie ochrony danych osobowych - np. praca przy komputerze lub w sieci osoby, która nie jest formalnie dopuszczona do jego obsługi, sygnał o uporczywym nieautoryzowanym logowaniu, itp.;

15.2.11 Ujawniono istnienie nieautoryzowanych kont dostępu do danych lub tzw. "bocznej furtki", itp.;

15.2.12 Podmieniono lub zniszczono nośniki z danymi osobowymi bez odpowiedniego upoważnienia lub w sposób niedozwolony skasowano lub kopiowano dane osobowe;

15.2.13 Rażąco naruszono dyscyplinę pracy w zakresie przestrzegania procedur bezpieczeństwa informacji (nie wylogowanie się przed opuszczeniem stanowiska pracy, pozostawienie danych osobowych w drukarce, na ksero, nie zamknięcie pomieszczenia z komputerem, nie wykonanie w określonym terminie kopii bezpieczeństwa, prace na danych osobowych w celach prywatnych, itp.).

15.2.14 Za naruszenie ochrony danych uważa się również stwierdzone nieprawidłowości w zakresie zabezpieczenia miejsc przechowywania danych, w tym także osobowych (otwarte szafy, biurka, regały, urządzenia archiwalne i inne) na nośnikach tradycyjnych tj. na papierze (wydrukach), kliszy, folii, zdjęciach, dyskietkach, pendrive czy przenośnych dyskach HD w formie niezabezpieczonej itp.

15.3 Każdy pracownik AP, w przypadku stwierdzenia zagrożenia lub naruszenia ochrony danych osobowych, zobowiązany jest poinformować Inspektora – kontakt – e-mail.- inspektor@apsl.edu.pl. *według załącznika nr 19 do PBI* - dostępny na stronie AP pod adresem www.si.apsl.edu.pl

15.4 W przypadku stwierdzenia wystąpienia zagrożenia, stwierdzenia incydentu – naruszenie bezpieczeństwa, Inspektor prowadzi postępowanie wyjaśniające, w toku, którego:

15.4.1 Ustala zakres i przyczyny zagrożenia oraz jego ewentualne skutki;

15.4.2 Inicjuje ewentualne działania dyscyplinarne;

15.4.3 Opisuje możliwe konsekwencje naruszenia ochrony danych;

15.4.4 Rekomenduje działania prewencyjne (zapobiegawcze) zmierzające do eliminacji (naprawy) naruszeń w przyszłości;

15.4.5 Dokumentuje prowadzone postępowania.

15.5 W przypadku, gdy naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o naruszeniu ochrony danych osobowych.

15.6 Naruszeń nie musimy zgłaszać osobom, których dane przetwarzamy, jeśli:

15.6.1 Zostały zastosowane odpowiednie środki techniczne i organizacyjne dla danych, których dotyczy naruszenie, takie jak szyfrowanie, aby uniemożliwić osobom nieuprawnionym odczytanie danych;

15.6.2 Użyto środków, które eliminują prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osób, których dane dotyczą;

15.6.3 Administrator musiałby dokonać niewspółmiernie dużego wysiłku by powiadomić osobę, której dane dotyczą o naruszeniu, wówczas wydawany jest publiczny komunikat lub inny podobny środek by poinformować osoby w skuteczny sposób.

15.7 Inspektor jest odpowiedzialny za nadzór nad poprawnością i terminowością wdrażanych działań korygujących lub zapobiegawczych. Po przeprowadzeniu działań korygujących lub zapobiegawczych, jest zobowiązany do oceny efektywności ich zastosowania i prowadzenia stosownej dokumentacji.

15.8 Integralną częścią *Polityki Bezpieczeństwa Informacji* są nw. dokumenty prowadzone przez Inspektora w przypadku stwierdzenia naruszenia bezpieczeństwa danych osobowych:

15.8.1 Dziennik naruszeń bezpieczeństwa danych – *załącznik nr 17* do PBI;

15.8.2 Protokół naruszeń bezpieczeństwa danych – *załącznik nr 18* do PBI.

16. Monitoring wizyjny

16.1 Uczelnia może stosować monitoring wizyjny w celu zapewnienia bezpieczeństwa osób i mienia na terenie uczelni i terenie wokół uczelni.

16.2 Podstawą prawną przetwarzania danych osobowych w związku ze stosowaniem monitoringu wizyjnego jest art. 6 ust. 1 lit. e RODO w związku z ustawą z dnia 20 lipca 2018 r. Prawo o szkolnictwie wyższym i nauce – wynikającym z niej obowiązkiem dbania o utrzymanie porządku i bezpieczeństwa na terenie uczelni.

16.3 Monitoring wizyjny nie obejmuje pomieszczeń sanitarnych, szatni przy obiektach sportowych, punktów medycznych.

16.4 Uczelnia wyznacza jednostkę lub osobę nadzorującą zgodność z prawem przetwarzanie danych w tym danych osobowych, w związku ze stosowaniem monitoringu wizyjnego.

16.5 Uczelnia określa zasady i tryb udostępniania nagrań z monitoringu wizyjnego.

16.6 Uczelnia określa czas przechowywania nagrań z monitoringu wizyjnego.

16.7 Jeśli w związku ze stosowaniem monitoringu wizyjnego uczelnia korzysta z usług innego podmiotu, powierza temu podmiotowi przetwarzanie danych osobowych na podstawie umowy, o której mowa art. 28 ust. 3 RODO.

16.8 Obowiązek informacyjny uczelnia spełnia poprzez wywieszenie klauzuli informacyjnej przy wejściu do budynku.

16.9 Przetwarzanie danych osobowych w związku ze stosowaniem monitoringu wizyjnego nie stanowi przetwarzania szczególnych kategorii danych osobowych, w szczególności danych dotyczących zdrowia, pochodzenia rasowego, etnicznego ani danych biometrycznych, o ile nie są stosowane specjalne metody techniczne, umożliwiającymi automatyczną, jednoznaczną identyfikację osoby fizycznej lub potwierdzenie jej tożsamości.

16.10 Ust. 10-9 nie naruszają art. 22^2 ustawy z dnia 26 czerwca 1974 r. Kodeks pracy, jeśli uczelnia stosuje monitoring, o którym mowa w tym przepisie.

16.11 W przypadku, o którym mowa w ust. 10, uczelnia przetwarza dane osobowe pracowników na podstawie art. 6 ust. 1 lit. c RODO.

17. Szkolenia.

17.1 Realizując politykę bezpieczeństwa w zakresie ochrony danych osobowych zapewnia się, cykl szkoleń przez Inspektora, zapoznawanie osób upoważnionych do dostępu lub przetwarzania danych osobowych z powszechnie obowiązującymi przepisami prawa, uregulowaniami wewnętrznymi, a także technikami i środkami ochrony tych danych stosowanymi w Uczelni, a także odpowiednio z ich zmianami.

17.2 Zapoznawanie osób upoważnionych do przetwarzania danych osobowych, o którym mowa w pkt.1 może odbywać się w szczególności poprzez:

17.2.1 Instruktaż na stanowisku pracy;

17.2.3 Szkolenie wewnętrzne realizowane na terenie Uczelni (także e-learning);

17.2.4 Szkolenie zewnętrzne.

17.3 W przypadku dostępu do danych osobowych przetwarzanych w systemie informatycznym, podstawowe szkolenie w zakresie procedur rozpoczęcia, zawieszenia i zakończenia pracy w systemie oraz mechanizmów zabezpieczenia stanowiska roboczego przeprowadza ASI.

18. INSTRUKCJA ZARZĄDZANIA SYSTEMAMI TELEINFORMATYCZNYMI SŁUŻĄCYMI DO PRZETWARZANIA DANYCH OSOBOWYCH.

18.1 Postanowienia ogólne.

18.1.1 Instrukcja zarządzania systemem teleinformatycznym służącym do przetwarzania danych osobowych w AP zwana dalej „Instrukcją", określa sposób zarządzania systemami teleinformatycznymi, służącymi do przetwarzania danych osobowych.

18.1.2 Instrukcja jest zgodna z opracowanym na Uczelni „Systemem Zarządzania Bezpieczeństwa Informacji AP oraz z procedurami, warunkami bezpieczeństwa w nim zawartymi (SZBI) opartych na analizie zagrożeń i ryzyku przy przetwarzaniu danych osobowych(*załącznik nr 20 do PBI).*

18.1.3 SZBI – System Zarządzania Bezpieczeństwem Informacji (dla systemów teleinformatycznych) – wprowadzony został zarządzeniem Rektora Nr R.021.72.19 z dnia 14 czerwca 2019 r.

18.2 Procedura nadawania/zmiany/odwołania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności.

18.2.1 Zasady nadawania uprawnień:

18.2.1.1 Każdy użytkownik systemu przed przystąpieniem do przetwarzania danych, zwłaszcza osobowych musi zapoznać się z:

18.2.1.1.1 Rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE;

18.2.1.1.2 Ustawą z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. Z 2019 poz. 1781);

18.2.1.1.3 Obowiązującą w AP Polityką Bezpieczeństwa Informacji danych osobowych;

18.2.1.1.4 Niniejszą instrukcją.

18.2.1.2 Jedynie prawidłowo wypełniony wniosek przełożonego o nadanie uprawnień (*załącznik nr 2 do PBI)* w systemie informatycznym Uczelni lub zmianę tych uprawnień jest podstawą rejestracji uprawnień w systemie;

18.2.1.3 Stosowany w Akademii Pomorskiej schemat uprawnień dostępu do zasobów informatycznych sieci LAN zakłada, iż użytkownicy uzyskują dostęp do sieci na pewnym, z góry zdefiniowanym poziomie;

18.2.2 Autoryzacja odbywa się na zasadzie autoryzowania sprzętu i jest w pełni automatyczna;

18.2.3 Niniejsza instrukcja przedstawia procesy związane z nadawaniem, zmianą i usuwaniem uprawnień dotyczących obsługi danych osobowych oraz innych newralgicznych systemów bazodanowych (np. e-learning, zasoby biblioteczne itp.).

18.3 Procedura nadawania uprawnień oraz ich ewidencjonowanie.

18.3.1 Kierownik (przełożony) jednostki organizacyjnej:

18.3.1.1 Nadaje upoważnienie do przetwarzania danych osobowych osobie, która w związku z wykonywanymi przez siebie obowiązkami będzie miała dostęp do danych osobowych;

18.3.1.2 Wypełnia i podpisuje wniosek nadania uprawnień dla osoby upoważnionej do przetwarzania danych osobowych (*załącznik nr 2 do PBI)*;

18.3.1.3 Przekazuje wypełniony dokument w postaci papierowej do ASI, w celu akceptacji;

18.3.1.4 W przypadku wniosku dotyczącego obsługi systemu z danymi osobowymi, ASI przekazuje go do Inspektora.

18.3.2 Inspektor sprawdza poprawność przesłanego wniosku oraz:

18.3.2.1 W przypadku braku uwag przekazuje go ze swoją adnotacją ASI, w celu nadania uprawnień użytkownikowi w systemie;

18.3.2.2 W przypadku uwag, np. gdy użytkownik nie został zapoznany z przepisami o ochronie danych osobowych, przekazuje dokument do kierownika jednostki organizacyjnej od którego dokument otrzymał. Na dokumencie dokonuje adnotacji, w której podaje przyczynę odmowy zatwierdzenia dokumentu. Kroki 1 i 2 powtarza się do czasu uzyskania akceptacji dokumentu przez Inspektora.

18.3.3. ASI odpowiednio, zgodnie z przekazanym dokumentem:

18.3.3.1 Rejestruje użytkownika w systemie i nadaje mu określone uprawnienia;

18.3.3.2 Generuje użytkownikowi tymczasowe hasło;

18.3.3.3 Informuje Inspektora o nadaniu uprawnień w celu aktualizacji ewidencji osób upoważnionych do przetwarzania danych osobowych w systemie;

18.3.4 Użytkownik uwierzytelnia się w systemie;

18.3.5 Użytkownik zmienia nadane mu przez ASI hasło i rozpoczyna pracę w aplikacji. Procedurę nadania uprawnień do przetwarzania danych osobowych w systemie należy stosować odpowiednio w przypadku zmiany uprawnień w systemie albo odebrania uprawnień w systemie;

18.4 Ewidencjonowanie uprawnień:

18.4.1 Inspektor w porozumieniem z ASI prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych w systemie informatycznym;

18.4.2 ewidencja osób upoważnionych może przyjmować formę elektroniczną, w takim wypadku należy jednak zapewnić ograniczenie dostępu do ewidencji, do kręgu osób upoważnionych;

18.4.3 ewidencja praw dostępu do sieci lokalnej jest prowadzona zgodnie z zasadami określonymi w odpowiedniej dokumentacji.

18.5 Stosowane metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem.

18.5.1 Identyfikatory i hasła są sposobem zagwarantowania rozliczalności, poufności i integralności danych osobowych przetwarzanych w systemach informatycznych. Służą do weryfikowania tożsamości użytkownika, uzyskania dostępu do określonych zasobów, kont uprzywilejowanych lub uruchomienia określonej funkcjonalności.

18.5.2 Identyfikatory i hasła użytkownik uzyskuje w procesie opisanym w paragrafie 17.3 niniejszej instrukcji.

18.5.3 Mając na uwadze zagwarantowanie wysokiego poziomu bezpieczeństwa przetwarzania danych osobowych oraz zagwarantowania użytkownikom pełnej rozliczalności wykonywanych przez nich operacji w systemach informatycznych, wszyscy użytkownicy przy uwierzytelnianiu do systemów informatycznych powinni stosować się do poniższych zasad:

18.5.3.1 Użytkownik systemu powinien posiadać unikalny identyfikator do swojego osobistego i wyłącznego użytku;

18.5.3.2 Hasła dostępu do systemów informatycznych powinny być tworzone przez użytkownika i stanowią tajemnicę służbową, znaną wyłącznie temu użytkownikowi;

18.5.3.3 Użytkownik ponosi pełną odpowiedzialność za utworzenie hasła dostępu oraz jego przechowywanie;

18.5.3.4 Hasła nie mogą być ujawniane lub przekazywane komukolwiek, bez względu na okoliczności;

18.5.3.5 Użytkownik nie powinien przechowywać haseł w widocznych miejscach, nie powinien umieszczać haseł w żadnych automatycznych procesach logowania (skryptach, makrach lub pod klawiszami funkcyjnymi).

18.5.4 Użytkownicy są odpowiedzialni za wszelkie działania w systemach informatycznych prowadzone z użyciem ich identyfikatora i hasła.

18.5.5 ASI są odpowiedzialni za okresowe sprawdzanie, usuwanie lub blokowanie zbędnych identyfikatorów użytkowników oraz kont w systemach za które są odpowiedzialni.

18.5.6 Administratorzy Systemu powinni przeprowadzać przegląd autoryzacji i uprawnień nie rzadziej niż co 6 miesięcy.

18.5.7 Administratorzy zakładają na stacjach roboczych specjalne konta (profile) służące do zarządzania daną stacją roboczą.

18.6 Wymogi dotyczące uwierzytelnienia.

18.6.1 Wszystkie konta dostępowe (identyfikatory) do systemów informatycznych powinny być chronione hasłem lub innym bezpiecznym, zaakceptowanym przez Inspektora sposobem uwierzytelniania;

18.6.2 Identyfikator oraz nadane uprawnienia powinny umożliwiać wykonywanie czynności wyłącznie zgodnych z zakresem powierzonych obowiązków;

18.6.3 Identyfikator użytkownika powinien być niepowtarzalny a po wyrejestrowaniu się z systemu informatycznego nie powinien być przydzielany innej osobie;

18.6.4 Identyfikator, który utracił ważność nie może być ponownie przydzielony innemu użytkownikowi;

18.6.5 Hasło początkowe, które jest przydzielane przez ASI, powinno umożliwiać użytkownikowi zarejestrowanie się w systemie tylko jeden raz i powinno być natychmiast zmienione przez użytkownika.

18.6.6 Użytkownicy powinny wybierać hasła dobrej jakości:

18.6.6.1 długości co najmniej 8 znaków;

18.6.6.2 które są łatwe do zapamiętania, a trudne do odgadnięcia;

18.6.6.3 nie są oparte na prostych skojarzeniach, łatwych do odgadnięcia lub wywnioskowania z informacji dotyczących właściciela konta (np. imię, nazwisko, data urodzenia itp.);

18.6.6.4 w których występuje przynajmniej jedna duża litera, jedna mała litera, jedna cyfra lub znak specjalny;

18.6.6.5 w których nie występują kolejne znaki, które nie są topologiczne (tzn. wynikające z układu klawiszy na klawiaturze, typu „qwer6., „zaq1xsw2CDE#. itp.).

18.6.7 Hasła nie mogą być takie same jak identyfikator użytkownika oraz nie mogą być zapisywane w systemach w postaci jawnej.

18.6.8 Hasła powinny być utrzymywane w tajemnicy również po upływie ich ważności.

18.6.9 Należy unikać ponownego lub cyklicznego używania starych haseł.

18.6.10 Rutynowe działania użytkownika nie powinny być prowadzone z wykorzystaniem kont uprzywilejowanych.

18.6.11 Udostępnienie hasła osobie postronnej należy traktować jako poważny incydent naruszenia ochrony danych osobowych.

18.7 Wymogi dotyczące zmiany haseł.

18.7.1 Użytkownik jest zobowiązany zmieniać hasło, w którego posiadaniu się znajduje;

18.7.2 Okresowo, zgodnie z wymaganiami dla danego systemu informatycznego (przed upływem terminu ważności hasła);

18.7.3 W przypadku ujawnienia lub podejrzenia ujawnienia hasła.

18.7.4 W przypadku braku dostępu do konta chronionego hasłem, w którego posiadaniu się znajduje, użytkownik zobowiązany jest wystąpić o zmianę hasła do właściwego ASI, w sytuacji:

18.7.4.1 Zapomnienia/zgubienia hasła;

18.7.4.2 Wygaśnięcia ważności hasła;

18.7.4.3 Zablokowania konta spowodowanego nieprawidłowym wprowadzeniem hasła;

18.7.4.4 Braku uprawnień/interfejsu umożliwiających samodzielną zmianę hasła.

18.7.5 Zmiana haseł użytkowników powinna być wymuszana przez system co 30 dni, w przypadku braku wymuszenia przez system, użytkownik sam jest zobowiązany do zmiany hasła co 30 dni.

18.8 Wymagania dotyczące sprzętu i oprogramowania.

18.8.1 Wygaszasz stacji roboczej powinien być skonfigurowany w taki sposób, aby aktywował się automatycznie po upływie 10 minut od ostatniego użycia stacji roboczej, uruchamiając blokadę stacji roboczej, wymuszającą ponowne zalogowanie;

18.8.2 Ekrany monitorów należy ustawić w taki sposób, by uniemożliwić osobom postronnym wgląd lub spisanie informacji aktualnie wyświetlanej na ekranie monitora;

18.8.3 Programy zainstalowane na stacjach roboczych stacjonarnych i na komputerach przenośnych obsługujących przetwarzanie danych osobowych muszą być użytkowane z zachowaniem praw autorskich i posiadać licencje;

18.8.4 Oprogramowanie może być używane tylko zgodnie z prawami licencji. Oprogramowanie typu Freewere, Shareware lub inne oprogramowanie dostarczane bez opłat jest uznawane jako nieautoryzowane, jeżeli nie otrzyma stosownej aprobaty Administratorów Systemu;

18.8.5 Przed zainstalowaniem nowego oprogramowania właściwy Administrator Systemu lub inna upoważniona osoba, zobowiązana jest sprawdzić jego działanie pod kątem bezpieczeństwa całego systemu;

18.8.6 Sieć teleinformatyczna wykorzystywana do przetwarzania danych osobowych powinna mieć zapewnione prawidłowe zasilanie energetyczne gwarantujące właściwe i zgodne z wymaganiami producenta działanie sprzętu informatycznego;

18.8.7 Serwer systemu przetwarzającego dane osobowe zasilany przez UPS o odpowiednich parametrach, pozwalających na podtrzymanie zasilania, przez co najmniej 15 minut oraz na wykonanie bezpiecznego wyłączenia serwera, tak, aby przed ostatecznym zanikiem zasilania zostały prawidłowo zakończone operacje rozpoczęte na zbiorze danych osobowych;

18.8.8 Infrastruktura techniczna związana z siecią teleinformatyczną i jej zasilaniem (rozdzielnie elektryczne, skrzynki z bezpiecznikami) powinna być zabezpieczona przed dostępem osób nieupoważnionych;

18.8.9 Gniazda zasilania sieci teleinformatycznej powinny być odpowiednio oznakowane, zabezpieczone przed włączeniem do nich innych odbiorników i wykonane w specjalnym standardzie;

18.8.10 Należy przechowywać wszystkie poprzednie wersje oprogramowania, jako środek utrzymania ciągłości działania;

18.8.11 Należy zapewnić rejestrowanie wszystkich błędów, związanych z problemami przetwarzania danych osobowych, zgłaszanych przez użytkowników lub programy systemowe;

18.8.12 Należy zapewnić ograniczenie dostępu do bibliotek źródłowych programów a dostęp i zmiany odnotowywać;

18.8.13. Należy chronić informacje zawarte w dziennikach zdarzeń systemów przed manipulacją i nieautoryzowanym dostępem;

18.8.14 Należy zapewnić synchronizację zegarów wszystkich stosowanych systemów służących do przetwarzania danych osobowych z uzgodnionym, dokładnym źródłem czasu;

18.8.15 Należy zapewnić, aby porty i usługi, które nie są wykorzystywane były zablokowane.

18.9 Procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu.

18.9.1 Przed przystąpieniem do pracy z systemem, użytkownik obowiązany jest dokonać sprawdzenia stanu urządzeń informatycznych oraz oględzin swojego stanowiska pracy, ze zwróceniem szczególnej uwagi, czy nie zaszły okoliczności wskazujące na naruszenie ochrony danych osobowych.

18.9.2 W przypadku stwierdzenia bądź podejrzenia, iż miało miejsce naruszenie ochrony danych osobowych, użytkownik systemu zobowiązany jest postępować zgodnie z procedurą opisaną w paragrafie 15 niniejszego dokumentu.

18.9.3 Procedura rozpoczęcia pracy w systemie IT.

18.9.3.1 Uruchomić komputer wchodzący w skład systemu informatycznego Uczelni, który jest podłączony fizycznie do sieci lokalnej lub wydzielonej i zalogować się podając identyfikator i hasło dostępu do odpowiedniego zasobu IT Uczelni;

18.9.3.2 Uruchomić wybraną aplikację (w szczególności aplikację bazodanową m.in. przetwarzającą dane osobowe);

18.9.3.3 Zalogować się do aplikacji za pomocą przydzielonego przez ASI loginu i hasła uwierzytelniającego.

18.9.4 Procedura zakończenia pracy w systemie IT.

18.9.4.1 W trakcie pracy, przy każdorazowym opuszczeniu stanowiska komputerowego, dopilnować, aby na ekranie nie były wyświetlane dane osobowe;

18.9.4.2 Przy opuszczaniu pokoju na dłuższy czas ustawić ręcznie blokadę klawiatury i wygaszacz ekranu.

18.9.5 Procedura zakończenia pracy w systemie IT.

18.9.5.1 Zamknąć aplikację;

18.9.5.2 Zamknąć system;

18.9.5.3 Wyłączyć monitor i ewentualnie drukarkę.

18.9.6 Nie wolno bez nadzoru pozostawiać po godzinach pracy włączonego sprzętu IT.

18.10 Procedury tworzenia kopii zapasowych zbiorów danych (bezpieczeństwa) oraz programów i narzędzi programowych służących do ich przetwarzania.

18.10.1 Kopie zapasowe zbiorów danych osobowych oraz programów i narzędzi programowych służących do ich przetwarzania powinny być wykonywane na bieżąco przez Administratorów Systemu Informatycznych;

18.10.2 Kopie zapasowe należy opisywać w sposób umożliwiający szybką i jednoznaczną identyfikację zawartych w nich danych;

18.10.3 Tworzenie, przechowywanie i likwidację kopii zapasowych powinny regulować szczegółowe instrukcje operacyjne dla poszczególnych systemów informatycznych, opracowywane przez ASI, z uwzględnieniem niniejszych postanowień;

18.10.4 Kopie zapasowe powinny być tworzone w bezpiecznym systemie archiwizacji, który powinien zapewniać ograniczony dostęp fizyczny do nośników oraz przyznanie uprawnień dostępu tylko wyznaczonemu imiennie ASI oraz Inspektora;

18.10.5 Dane z kopii zapasowych powinny być odtwarzane wyłącznie przez ASI;

18.10.6 Kopie zapasowe, które uległy uszkodzeniu powinny podlegać natychmiastowemu zniszczeniu. Niszczenia kopii zapasowych, na nośnikach magnetycznych dokonuje ASI lub inna upoważniona osoba;

18.10.7 Automatyczne dzienne kopie bezpieczeństwa winny być zapisywane na urządzeniach magazynujących znajdujących się w innym pomieszczeniu (innej serwerowni).

18.10.8 Centralnym punktem zapisu kopii bezpieczeństwa poszczególnych systemów informatycznych jest serwerownia przy ul. Westerplatte 64 którą zarządza Sekcja Informatyki. Urządzeniem magazynującym jest macierz dyskowa lub wysokowydajny FTP z dyskami w układzie RAID.

18.11 Przechowywanie nośników elektronicznych zawierających dane osobowe.

18.11.1 Dane osobowe mogą być przechowywane:

18.11.1.1 Na serwerach zlokalizowanych w obszarach wyznaczonych do przetwarzania danych osobowych;

18.11.1.2 Na wymiennych nośnikach elektronicznych;

18.11.1.3 Na zasobach sieciowych udostępnionych przez Administratora Systemu (FTP, NAS itp.),

18.11.2 Po wykorzystaniu dane osobowe w postaci elektronicznej należy niezwłocznie usunąć z nośnika elektronicznego w sposób uniemożliwiający ich ponowne odtworzenie;

18.11.3 Wykorzystanie wymiennych nośników elektronicznych (CD/DVD, pamięć USB, wymienna karta pamięci, dyskietka) powinno być ściśle kontrolowane i dozwolone wyłącznie dla upoważnionych użytkowników;

18.11.4 Wymienne nośniki elektroniczne, o ile nie są użytkowane, powinny być przechowywane w zamykanych szafkach;

18.11.5 Nośniki zawierające kopie zapasowe powinny być przechowywane w innym pomieszczeniu niż to, w którym umieszczony jest serwer przetwarzający dane osobowe;

18.11.6 Nośniki magnetyczne i optyczne z danymi osobowymi powinny być:

18.11.6.1 oznaczane i przechowywane w zamykanych szafach lub sejfach,

18.11.6.2 przechowywane maksymalnie przez okres wskazany dla danego rodzaju danych osobowych przez Administratora Bezpieczeństwa Informacji,

18.11.7 informację o maksymalnym okresie przechowywania nośników magnetycznych oraz optycznych, na których zapisane są dane osobowe przekazują GUS do Inspektora.

18.12 Sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania.

18.12.1 Ochrona systemu informatycznego przed działaniem szkodliwego oprogramowania:

18.12.1.1 Na każdej stacji roboczej w sieci oraz serwerze przetwarzającym dane osobowe powinno być zainstalowane oprogramowanie antywirusowe skanujące na bieżąco system informatyczny;

18.12.1.2 Oprogramowanie antywirusowe powinno być zainstalowane tak, aby użytkownik nie był w stanie wyłączyć lub pominąć etapu skanowania;

18.12.1.3 Kontrola antywirusowa powinna być przeprowadzana na wszystkich nośnikach magnetycznych i optycznych, służących zarówno do przetwarzania danych osobowych w systemie, jak i do celów instalacyjnych;

18.12.1.4 Należy stosować wersje programów antywirusowych z aktualną bazą sygnatur wirusów;

18.12.1.5 Nowe wersje oprogramowania antywirusowego oraz uaktualnienia bazy sygnatur wirusów instalują ASI niezwłocznie po ich otrzymaniu lub ściągnięciu, uprzednio weryfikując pochodzenie oprogramowania;

18.12.1.6 ASI mają prawo odłączyć od sieci stację roboczą, na której zostanie zlokalizowany wirus, jeśli uznają, że dalsze pozostawienie go w sieci zagraża innym stacjom roboczym.

18.13 Zasady komunikacji w sieci teleinformatycznej.

18.13.1 Przesyłanie danych osobowych drogą teletransmisji powinno odbywać się wyłącznie przy wykorzystaniu wymaganych zabezpieczeń logicznych chroniących przed nieuprawnionym dostępem, w szczególności takich jak ochrona kryptograficzna;

18.13.2 Pliki zawierające dane osobowe mogą się znajdować jedynie na serwerach, gdzie podlegają ochronie zapewnianej przez mechanizmy bezpieczeństwa systemu operacyjnego;

18.13.3 Wyłącznie w sytuacjach wyjątkowych dopuszcza się przetwarzanie danych osobowych w plikach (MS Word, MS Excel) na stacjach roboczych użytkowników, poza bazą danych, znajdującą się w określonym systemie teleinformatycznym Uczelni;

18.13.4 Zgodę na przetwarzanie danych w sytuacjach określonych w ust. 3 wydają LADO;

18.13.5 Inne technologie sieciowe takie jak sieci lokalne oparte na falach radiowych nie mogą być wykorzystywane do przekazu informacji, o ile połączenie nie jest szyfrowane. Takie połączenia mogą być używane jedynie dla wymiany poczty elektronicznej o ile wiadomo, że nie zawiera ona danych osobowych;

18.13.6 Wszystkie połączenia zewnętrzne do systemu teleinformatycznego powinny być monitorowane a logi połączeń archiwizowane w trybie ciągłym i bezterminowym;

18.13.7 System teleinformatyczny służący do przetwarzania danych osobowych ASI mają obowiązek chronić przed zagrożeniami pochodzącymi z sieci publicznej poprzez wdrożenie logicznych zabezpieczeń chroniących przed nieuprawnionym dostępem;

18.13.8 Zabezpieczenia logiczne, o których mowa w ust. 7 powyżej, obejmują:

18.13.8.1 Kontrolę przepływu informacji pomiędzy systemem teleinformatycznym a siecią publiczną,

18.13.8.2 Kontrolę działań inicjowanych z sieci publicznej i systemu informatycznego.

18.14 Zasady i sposób odnotowywania w systemach informacji o udostępnieniu danych osobowych.

18.14.1 Z uwagi na to, że przetwarzane dane osobowe w systemach informatycznych Uczelni nie są udostępniane podmiotom trzecim (za wyjątkiem wymienionych w punkcie 2), to nie istnieje potrzeba rejestracji udostępnień danych osobowych odbiorcom;

18.14.2 Odbiorcą danych jest każdy, komu udostępnia się dane osobowe, z wyłączeniem:

18.14.2.1 Osoby, której dane dotyczą;

18.14.2.2 Użytkownika systemu lub innej osoby upoważnionej do przetwarzania danych osobowych na Uczelni;

18.14.2.3 Przedstawiciela mającego siedzibę albo miejsce zamieszkania w państwie trzecim ;

18.14.2.4 Organów państwowych, którym dane są udostępniane w związku z prowadzonym postępowaniem (np. policja, prokuratura, itp.).

18.14.3 Systemy informatyczne Uczelni nie rejestrują źródła pochodzenia danych, ponieważ dane pochodzą bezpośrednio od osób, których te dane dotyczą (np. pracownik, student).

18.15 Rejestracja daty wprowadzenia danych do systemu informatycznego.

18.15.1 Systemy informatyczne rejestrują datę pierwszego wprowadzenia danych osobowych do systemu;

18.15.2 System rejestruje identyfikator użytkownika wprowadzającego dane do systemu, chyba, że dostęp do systemu i przetwarzanych w nim danych posiada wyłącznie jedna osoba;

18.15.3 System odnotowuje datę i identyfikator użytkownika podczas każdej zmiany danych w zarejestrowanych danych osobowych.

18.16 Procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych.

O przeprowadzanych przeglądach i konserwacjach systemu w każdym przypadku informowany jest Inspektor, który może być przy nich obecny.

18.16.1 Przeglądy i konserwacja urządzeń oraz nośników danych:

18.16.1.1 Przeglądy i konserwacja urządzeń wchodzących w skład systemu informatycznego powinny być wykonywane w terminach określonym przez producenta sprzętu;

18.16.1.2 Jeśli producent nie przewidział dla danego urządzenia potrzeby dokonywania przeglądów eksploatacyjnych, lub też nie określił ich częstotliwości, to o dokonaniu przeglądu oraz sposobie jego przeprowadzenia decydują ASI;

18.16.1.3 Nieprawidłowości ujawnione w trakcie przeglądów bądź konserwacji powinny być niezwłocznie usunięte, a ich przyczyny przeanalizowane. O fakcie ujawnienia nieprawidłowości należy zawiadomić Inspektora;

18.16.1.4 Za terminowość przeprowadzenia przeglądów i konserwacji oraz ich prawidłowy przebieg odpowiada ASI;

18.16.1.5 Jeżeli ASI nie dokonuje napraw osobiście, podmiot dokonujący naprawy zawiadamia o podjętych czynnościach ASI;

18.16.1.6 W przypadku przekazania sprzętu lub nośników informacji służących do przetwarzania danych osobowych podmiotowi trzeciemu, pozbawia się je zapisów danych osobowych w sposób, który uniemożliwi ich odtworzenie.

18.16.2 Przegląd programów i narzędzi programowych.

18.16.2.1 Przegląd programów i narzędzi programowych przeprowadzany jest w następujących przypadkach:

18.16.2.1.1 Zmiany wersji oprogramowania serwera plików,

18.16.2.1.2 Zmiany wersji oprogramowania stanowiska komputerowego użytkownika systemu,

18.16.2.1.3 Zmiany systemu operacyjnego serwera plików,

18.16.2.1.4 Zmiany systemu operacyjnego stanowiska komputerowego użytkownika systemu,

18.16.2.1.5 Wykonania zmian w projekcie systemu spowodowanych koniecznością naprawy lub modyfikacji systemu.

18.16.2.2 Postanowień punktu 1 nie stosuje, gdy zmiany oprogramowania stanowisk komputerowych bądź serwerów odbywają się w ramach rutynowej, odbywającej się

automatycznie lub według ustalonego harmonogramu, aktualizacji zabezpieczeń oprogramowania systemowego, biurowego itp.;

18.16.2.3 Przed dokonaniem zmian w systemie informatycznym należy dokonać przeglądu działania systemu w zmienionej konfiguracji w warunkach testowych na testowej bazie danych. Sprawdzenie powinno obejmować:

18.16.2.3.1 Poprawność logowania się do systemu w zależności od posiadanych uprawnień,

18.16.2.3.2 Poprawność działania wszystkich elementów aplikacji (menu, zestawienia, formularze, raporty).

18.16.2.4 Za prawidłowość przeprowadzenia przeglądów i konserwacji systemu odpowiada ASI.

18.16.2.5 Konserwację oprogramowania przeprowadza się po zgłoszeniu przez użytkownika systemu potrzeby wprowadzenia zmian pozwalających utrzymać funkcjonalność systemu w dynamicznie zmieniającym się środowisku pracy;

18.16.2.6 Przed dokonaniem zmian w systemie informatycznym należy dokonać przeglądu działania systemu w zmienionej konfiguracji w warunkach testowych na testowej bazie danych na podobnych zasadach jak ma to miejsce w przypadku przeglądu oprogramowania;

18.16.2.7 Konserwację przeprowadza serwisant systemu (na podstawie umowy serwisu wskazanego systemu informatycznego) - w obecności ASI;

18.16.2.8 Jeżeli serwisant dokonuje zmian w systemie informatycznym zdalnie za pośrednictwem np. sieci Internet, to wszystkie prace muszą być wykonane za wiedzą i pod nadzorem ASI.

19. POSTANOWIENIA KOŃCOWE.

19.1 W sprawach nieuregulowanych niniejszym dokumentem, znajdują zastosowanie przepisy ustawy o ochronie danych osobowych oraz rozporządzenia 2016/679.

19.2 ZAŁĄCZNIKI

Załącznik nr 1 - Zgłoszenie naruszenia bezpieczeństwa systemu informatycznego

Załącznik nr 2 – Wniosek nadania uprawnień dla użytkowników systemu teleinformatycznego

Załącznik nr 3 – Wykaz budynków i pomieszczę w których przetwarzane są dane osobowe

Załącznik nr 4 - Przepływ danych pomiędzy poszczególnymi systemami.

Załącznik nr 5 – Wzór upoważnienia

Załącznik nr 6 – Rejestr osób upoważnionych do przetwarzana danych osobowych

Załącznik nr 7 – Oświadczenie poufności

Załącznik nr 8 - Schemat organizacyjny struktury odpowiedzialności funkcjonalnej.

Załącznik nr 9 - Wykaz lokalizacji zbiorów, w tym modułów programowych zawierających dane osobowe.

Załącznik nr 10 - Poziom bezpieczeństwa.

Załącznik nr 11 - Wzór umowy powierzenia danych osobowych.

Załącznik nr 12 - Udostępnianie - przetwarzanie danych w imieniu administratora.

Załącznik nr 13 - Struktura zbiorów.

Załącznik nr 14 - Wykaz podmiotów, którym powierzono przetwarzanie danych

Załącznik nr 15 - Wykaz podmiotów, którym udostępniono przetwarzanie danych.

Załącznik nr 16 - Rejestr czynności przetwarzanych danych osobowych.

Załącznik nr 17 - Dziennik naruszeń bezpieczeństwa danych.

Załącznik nr 18 - Protokół naruszeń bezpieczeństwa danych

Załącznik nr 19 - Formularz informacyjny o zbiorze danych.

Załącznik nr 20 – Analiza ryzyka przy przetwarzaniu danych osobowych

Załącznik nr 21 – Monitoring wizyjny Uczelni

20. TABELA ZMIAN

Wersja dokumentu	Data publikacji	Opis zmian
1.0	**30 maja 2018**	**Dokument podstawowy w wersji 1.0**
2.0	**6 maja 2021**	**Nowelizacja do wersji 2.0**