Zarządzenie nr 97/2024
REKTORA
Państwowej Akademii Nauk Stosowanych
im. ks. Bronisława Markiewicza
w Jarosławiu
z dnia 22 lipca 2024 r.

w sprawie procedur dotyczących ochrony danych osobowych w Państwowej Akademii Nauk Stosowanych im. ks. Bronisława Markiewicza w Jarosławiu

Na podstawie art. 23 ust. 1 ustawy z dnia 20 lipca 2018 r. – Prawo o szkolnictwie wyższym i nauce (Dz.U. z 2023 r. poz. 742 z późn. zm.) zarządzam, co następuje:

§1

1. Wprowadza się wewnętrzne procedury dotyczące ochrony danych osobowych w Państwowej Akademii Nauk Stosowanych im. ks. Bronisława Markiewicza w Jarosławiu, które stanowią załączniki do zarządzenia.
2. Procedury podlegają bieżącej weryfikacji przez kierowników jednostek organizacyjnych. W przypadku stwierdzenia nieprawidłowości kierownicy zgłaszają je niezwłocznie do Inspektora Ochrony Danych w celu uaktualniania.
3. Wszyscy pracownicy i osoby współpracujące z PANS w Jarosławiu zobowiązani są do zapoznania się z procedurami oraz ich stosowania.

§2

Traci moc Zarządzenie nr 66/2019 Rektora PWSTE w Jarosławiu z dnia 18 czerwca 2019 r. w sprawie wprowadzenia procedur dotyczących ochrony danych osobowych w Państwowej Wyższej Szkole Techniczno-Ekonomicznej im. ks. Bronisława Markiewicza w Jarosławiu.

§3

Zarządzenie wchodzi w życie z dniem podpisania.

z upoważnienia Rektora PANS w Jarosławiu
Prorektor ds. dydaktycznych
dr Dorota Dejniak

Sporządził
.....

Zatwierdzam pod względem formalno-prawnym
RADCA PRAWNY
Jerzy Ryńkiewicz
Nr rej. Rz/P/47
.....

Zatwierdzam pod względem merytorycznym
KANCLERZ
mgr inż. Mariusz Dudek
.....

+48 16 624 46 20
uczelnia@pansjar.edu.pl
Państwowa Akademia Nauk Stosowanych
im. ks. Bronisława Markiewicza w Jarosławiu
ul. Czarnieckiego 16
37-500 Jarosław

Polityka Ochrony Danych Osobowych w Państwowej Akademii Nauk Stosowanych im. ks. Bronisława Markiewicza w Jarosławiu

Wstęp

Państwowa Akademia Nauk Stosowanych im. ks. Bronisława Markiewicza w Jarosławiu jest Administratorem Danych Osobowych, a czynności z zakresu ochrony danych osobowych wykonuje Rektor PANS w Jarosławiu. Jest On zobowiązany do podejmowania wszelkich możliwych działań koniecznych do zapobiegania zagrożeniom związanym z przetwarzaniem danych osobowych.

Polityka Ochrony Danych Osobowych jest dokumentem opisującym zasady ochrony danych osobowych stosowanych przez Administratora w celu spełnienia wymagań Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE oraz ustawy z 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2019 r. poz. 1781).

Celem Polityki Ochrony Danych Osobowych 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.

Spis treści

Rozdział 1

Postanowienia ogólne

§1

Na użytek niniejszego dokumentu:

1. Polityka – „Polityka Ochrony Danych Osobowych w Państwowej Akademii Nauk Stosowanych im. ks. Bronisława Markiewicza w Jarosławiu";
2. dane osobowe – informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej (osoba możliwa do zidentyfikowania to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny – w szczególności numer PESEL albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne);
3. zbiór danych – uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie;
4. Administrator – osoba fizyczna lub prawa, organ publiczny, jednostka organizacyjna lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych;
5. Podmiot przetwarzający – osoba fizyczna lub prawna, organ publiczny, jednostka organizacyjna lub inny podmiot, który w imieniu administratora przetwarza dane osobowe;
6. Inspektor Ochrony Danych (IOD) - to osoba formalnie wyznaczona przez Administratora w celu informowania i doradzania Administratorowi/Podmiotowi przetwarzającemu/pracownikom w zakresie obowiązującego prawa o ochronie danych i niniejszej Polityki oraz w celu monitorowania ich przestrzegania oraz działania, jako punkt kontaktowy dla osób przetwarzanych i organu nadzorczego;
7. przetwarzanie – operacja lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taka jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łącznie, ograniczanie, usuwanie lub niszczenie;
8. odbiorca – każda osoba fizyczna lub prawna, organ publiczny, jednostka 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 UE lub prawem państwa członkowskiego, nie są uznawane za odbiorców; przetwarzanie tych danych przez te organy publiczne musi być zgodne z przepisami o ochronie danych osobowych mającymi zastosowanie do celów przetwarzania;
9. zgoda osoby, której dane dotyczą – dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie pisemnego oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych;
10. naruszenie ochrony danych osobowych (incydent) – 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.

§2

Polityka określa:

a) zasady na podstawie, których opiera się przetwarzanie danych osobowych oraz sposób uzyskiwania upoważnień oraz nadawania uprawnień do przetwarzania danych osobowych;

b) procedurę przeprowadzania analizy ryzyka oraz instrukcję postępowania w przypadku wystąpienia incydentu;
c) wykaz zbiorów danych osobowych ze wskazaniem podstaw prawnych przetwarzania, aktywów, celi przetwarzania, rodzajów i zakresów danych oraz odbiorców, opisu operacji przetwarzania, czasu przechowywania;
d) wykaz budynków, pomieszczeń lub części pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe;
e) wykaz zabezpieczeń stosowanych w celu ochrony danych osobowych;
f) Regulamin Ochrony Danych Osobowych;
g) Politykę kluczy;
h) sposób zapoznawania pracowników z nowelizacją przepisów (szkolenie wewnętrzne pracowników).

Rozdział 2

Inwentaryzacja danych. Zasady przetwarzania danych osobowych. Odpowiedzialność. Obowiązek informacyjny.

§3

1. Dane osobowe wymagające ochrony zostały wykazane w załączniku do niniejszej Polityki (Załącznik nr 1 – Wykaz zbiorów danych osobowych).
2. Wykaz obejmuje zbiory ze stwierdzonym potencjalnym ryzykiem naruszenia praw lub wolności osób fizycznych.
3. Każdy ze zbiorów jest opisany w sposób umożliwiający przeprowadzenie analizy ryzyka.
4. Opis zbiorów obejmuje takie informacje, jak:
   a) nazwę zbioru;
   b) opis celów przetwarzania;
   c) charakter, zakres, kontekst, dokumentowane dane osobowe;
   d) odbiorcy;
   e) funkcjonalny opis operacji przetwarzania;
   f) aktywa służące do przetwarzania danych osobowych;
   g) informacje o konieczności wpisu do rejestru czynności przetwarzania;
   h) informacja o konieczności przeprowadzania oceny skutków dla zbioru.

§4

1. Administrator oraz podmiot przetwarzający zapewniają, że dane osobowe przetwarzane są zgodnie z poniższymi regułami:
   a) zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą (zgodność z prawem, rzetelność i przejrzystość);
   b) zbierane są w konkretnych, wyraźnych i prawnie uzasadnionych celach (ograniczenie celu);
   c) adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane (minimalizacja danych);
   d) prawidłowe i w razie potrzeby uaktualniane (prawidłowość);
   e) przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane, z wyjątkami wskazanymi w rozporządzeniu (ograniczenie przechowywania);
   f) w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych (integralność i poufność);
   g) wobec osób, których dane osobowe są przetwarzane wykonano tzw. obowiązek informacyjny – prawo dostępu do danych, prawo przenoszenia, sprostowania, usunięcia, ograniczenia przetwarzania, sprzeciwu.

2. Administrator prowadzi rejestr czynności przetwarzania. Rejestr czynności stanowi równocześnie wykaz zbiorów danych osobowych Administratora (Załącznik nr 1).
3. Podmiot przetwarzający prowadzi rejestr kategorii czynności przetwarzania.

§5

1. Do stosowania zasad określonych przez dokumenty Polityki zobowiązani są wszyscy pracownicy PANS w Jarosławiu, niezależnie od podstawy zatrudnienia, osoby wykonujące umowy cywilnoprawne, którzy w ramach obowiązków służbowych przetwarzają dane osobowe oraz podmioty którym zlecono wykonywanie określonych czynności na podstawie stosownych umów.
2. Każda osoba mająca dostęp do danych osobowych przetwarzanych w PANS w Jarosławiu jest zobowiązana do zapoznania się z niniejszym dokumentem.

§6

1. Administrator/podmiot przetwarzający odpowiada za nadawanie oraz anulowanie upoważnień do przetwarzania danych osobowych w zbiorach papierowych, systemach informatycznych.
2. Podmiot przetwarzający oraz każda osoba działająca z upoważnienia Administratora lub podmiotu przetwarzającego i mająca dostęp do danych osobowych przetwarza je wyłącznie na polecenia Administratora, chyba, że wymaga tego przepis prawa.
3. Upoważnienia nadawane są do zbiorów na wniosek przełożonych (kierowników/dyrektorów jednostek organizacyjnych). Kierownicy jednostek organizacyjnych określają zakres kompetencji przetwarzania danych osobowych.
4. Upoważnienia określają zakres operacji na danych.
5. Upoważnienia mogą być wyjątkowo nadawane w formie poleceń, np. upoważnienie do przeprowadzenia kontroli, audytów, wykonania czynności służbowych.
6. Inspektor Ochrony Danych prowadzi ewidencję osób upoważnionych, w celu sprawowania kontroli nad prawidłowym dostępem do danych osób upoważnionych. Ewidencja stanowi załącznik do niniejszej Polityki (Załącznik nr 2 –wzór Ewidencji osób upoważnionych. Ewidencja prowadzona jest w formie elektronicznej).

§7

1. Uprawnienia do przetwarzania danych osobowych w systemie informatycznym nadawane są na wniosek przełożonych (kierowników/dyrektorów jednostek organizacyjnych) osób, które mają przetwarzać dane.
2. Kierownicy jednostek organizacyjnych działów określają systemy informatyczne, do których dostęp mają pracownicy zarządzanych przez nich jednostek oraz zakres kompetencji.
3. Uprawnienie, o którym mowa w pkt. 1 jest anulowane z chwilą zaprzestania przetwarzania danych osobowych przez osobę, której uprawnienie zostało nadane bądź z ustaniem zatrudnienia.
4. Nadanie bądź anulowanie uprawnień, o którym mowa w niniejszym paragrafie odbywa się na podstawie wniosku kierującego daną jednostką organizacyjną, składanego w formie elektronicznej za pośrednictwem systemu EOD do Kanclerza PANS w Jarosławiu.

§8

1. Administrator pozyskując dane osobowe od osoby, której dotyczą jest zobowiązany podać jej następujące informacje:
   a) swoją tożsamość i dane kontaktowe;
   b) dane kontaktowe Inspektora Ochrony Danych;
   c) cele przetwarzania danych oraz podstawę prawną przetwarzania;
   d) jeżeli przetwarzanie danych osobowych związane jest z realizacją prawnie uzasadnionych interesów realizowanych przez Administratora lub przez stronę trzecią – należy wskazać prawnie uzasadnione interesy;
   e) informację o odbiorcach danych osobowych lub o kategoriach odbiorców;

f) w przypadkach, gdy ma to zastosowanie – informacje o zamiarze przekazania danych do państwa trzeciego lub organizacji międzynarodowej;

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

h) informacje o prawie do żądania od Administratora dostępu do danych osobowych dotyczących osoby, której dane dotyczą, ich sprostowania, usunięcia lub ograniczenia przetwarzania lub o prawie do wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych;

i) informacje o prawie do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem (reguła ta ma zastosowanie do przetwarzania danych na podstawie zgody wyrażonej w jednym lub większej liczbie celów oraz przetwarzania danych wrażliwych na podstawie zgody osoby, której dane dotyczą);

j) informację o prawie wniesienia skargi do organu nadzorczego;

k) informację czy podanie danych jest wymogiem ustawowym lub umownym lub warunkiem zwarcia umowy oraz czy osoba, której dane dotyczą, jest zobowiązana do ich podania i jakie są ewentualne konsekwencje niepodania danych;

l) informacje o zautomatyzowanym podejmowaniu decyzji.

2. W przypadku, gdy Administrator pozyskuje dane osobowe z innego źródła niż osoba, której dane dotyczą, Administrator jest zobowiązany podać tej osobie wszystkie informację wymienione w pkt. 1 a dodatkowo: podać informację o źródle pochodzenia danych osobowych.

3. Informacje, o których mowa w pkt. 2 Administrator podaje w rozsądnym terminie po pozyskaniu danych, najpóźniej w ciągu miesiąca mając na uwadze konkretne okoliczności przetwarzania danych osobowych. W przypadku, gdy dane osobowe mają być stosowane do komunikacji z osobą, której dane dotyczą administrator przekazuje dane najpóźniej przy pierwszej takiej komunikacji. Jeżeli planuje się ujawnić dane osobowe innemu odbiorcy najpóźniej przy pierwszym ich ujawnieniu.

§9

1. Dane osobowe mogą być wykorzystywane wyłącznie do celów, dla jakich były, są lub będą zbierane i przetwarzane, przez okres nie dłuższy niż jest to niezbędne do celów, dla których dane te są przetwarzane. Dane osobowe mogą być przechowywane przez okres dłuższy, jeżeli będą przetwarzane wyłącznie do celów archiwalnych w interesie publicznym, do celów naukowych lub historycznych lub do celów statystycznych.

2. Dane osobowe powinny być przechowywane w formie uniemożliwiającej identyfikację osób, których dotyczą.

3. Osoba, której dane dotyczą ma prawo żądać od Administratora sprostowania dotyczących jej danych, które są nieprawidłowe.

4. Osoba, której dane dotyczą ma prawo żądać od Administratora niezwłocznego usunięcia dotyczących jej danych osobowych, a Administrator ma obowiązek bez zbędnej zwłoki usunąć dane, jeśli zachodzi jedna z przesłanek:

a) dane osobowe nie są już niezbędne dla celów, dla jakich zostały zebrane;

b) osoba, której dane dotyczą cofnęła zgodę, na której opiera się przetwarzanie i nie ma innej podstawy prawnej przetwarzania;

c) osoba, której dane dotyczą wnosi sprzeciw na mocy przepisów prawa i nie występują nadrzędne prawnie uzasadnione podstawy przetwarzania;

d) dane osobowe były przetwarzane niezgodnie z prawem;

e) dane osobowe muszą zostać usunięte w celu wywiązania się z obowiązku prawnego;

f) dane osobowe zostały zebrane w związku z oferowaniem usług społeczeństwa informacyjnego.

5. Osoba, której dane dotyczą ma prawo żądać ograniczenia przetwarzania w następujących przypadkach:

a) osoba, której dane dotyczą kwestionuje ich prawidłowość;

b) przetwarzanie jest niezgodne z prawem, a osoba, której dane dotyczą sprzeciwia się usunięciu danych;

c) Administrator nie potrzebuje już danych osobowych do celów przetwarzania, ale są one potrzebne osobie, której dane dotyczą do ustalenia, dochodzenia lub obrony roszczeń;

d) osoba, której dane dotyczą wniosła sprzeciw wobec przetwarzania.

6. Osoba, której dane dotyczą, ma prawo otrzymać w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego dane osobowe jej dotyczące, które dostarczyła administratorowi, oraz ma prawo przesłać te dane osobowe innemu administratorowi bez przeszkód ze strony administratora, któremu dostarczono te dane osobowe.
7. Osoba, której dane dotyczą, ma prawo do tego, by nie podlegać decyzji, która opiera się wyłącznie na zautomatyzowanym przetwarzaniu, w tym profilowaniu, i wywołuje wobec tej osoby skutki prawne lub w podobny sposób istotnie na nią wpływa.

Rozdział 3

Procedura analizy ryzyka/ocena skutków

§10

1. Administrator jest odpowiedzialny za określenie listy zagrożeń naruszenia poufności, dostępności i integralności, które mogą wystąpić podczas przetwarzania danych osobowych.
2. Zagrożenia powinny być identyfikowane w odniesieniu do uprzednio zinwentaryzowanych zbiorów (kategorii osób), aktywów oraz procesów przetwarzania.
3. Procedura opisuje sposób przeprowadzenia analizy ryzyka w celu zabezpieczenia danych osobowych adekwatnie do zidentyfikowanych zagrożeń.
4. Przyjęto, że analiza ryzyka przeprowadzana jest dla zbioru danych osobowych lub grupy zbiorów charakteryzujących się podobieństwem celów i sposobów przetwarzania.
5. W przypadku konieczności przeprowadzenia oceny skutków (jeżeli rodzaj przetwarzania, ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych), wymagane jest wykonanie następujących czynności:

a) Systematyczny opis planowanych operacji przetwarzania i celów przetwarzania (Załącznik nr 1 – Wykaz zbiorów danych osobowych);

b) Ocenę czy operacje przetwarzania są niezbędne oraz proporcjonalne w stosunków do celów (Załącznik nr 1 – Wykaz zbiorów danych osobowych);

c) Ocenę ryzyka (Załącznik nr 3 – Procedura analizy ryzyka);

d) Środki planowane w celu zaradzenia ryzyku, przedstawione w postaci planu postępowania z ryzykiem (Załącznik nr 3 – Procedura analizy ryzyka).

§11

1. Administrator określa Prawdopodobieństwo (**P**) wystąpienia poszczególnych zagrożeń w zbiorze (dla kategorii osób) lub w procesie przetwarzania.
2. Proponowaną skalę prawdopodobieństwa prezentuje Tabela A.
3. Administrator określa Skutki (**S**) wystąpienia incydentów (materializacji zagrożeń), uwzględniając straty finansowe, utratę reputacji, sankcje/skutki karne.
4. Proponowaną Skalę skutków prezentuje Tabela B.
5. Administrator wylicza Ryzyka (R) dla wszystkich zagrożeń i ich skutków w/g formuły: **R = P * S**

Tabela A PRAWDOPODOBIEŃSTWO WYSTĄPIENIA ZAGROŻENIA	**SKALA (WAGA)**
zagrożenie niskie	1

zagrożenie średnie	2
zagrożenie wysokie	3

Tabela B SKUTKI WYSTĄPIENIA ZAGROŻENIA	**SKALA (WAGA)**
małe (do 10000 PLN, incydent prasowy lokalny)	1
średnie (10000-100000 PLN, incydent prasowy ogólnopolski)	2
duże (od 100000 PLN, naruszenie prawa)	3

3.1 Porównanie wyliczonych ryzyk ze skalą i określenie dalszego postępowania z ryzykiem

1. Administrator porównuje wyliczone ryzyka ze skalą i podejmuje decyzje dotyczące dalszego postępowania z ryzykiem
2. Proponowaną skalę Ryzyka prezentuje Tabela C

Tabela C POZIOM RYZYKA	**WARTOŚĆ [R = P*S]**
ryzyko pomijalne i akceptowalne (akceptujemy)	1-2
ryzyko jest opcjonalne (akceptujemy albo obniżamy)	3-6
ryzyko jest nieakceptowalne (musimy obniżyć)	9

3.2 Reakcja na wartość ryzyka

1. Akceptacja ryzyka – zabezpieczenia są właściwe – brak potrzeby stosowania dodatkowych zabezpieczeń
2. Działania obniżające ryzyko, które może zastosować Administrator:
    a. Przeniesienie –przerzucenie ryzyka (outsourcing, ubezpieczenie)
    b. Unikanie – eliminacja działań powodujących ryzyko
3. Redukcja – zastosowanie zabezpieczeń w celu obniżenia ryzyka
4. Analizę ryzyka przeprowadza się w specjalnym szablonie, która stanowi załącznik nr 3 do niniejszej Polityki.

3.3 Ponowna analiza ryzyka

Ponowna analiza ryzyka przeprowadzana jest cyklicznie lub po znaczących zmianach w przetwarzaniu danych (np. przetwarzanie nowych zbiorów, nowych procesów przetwarzania, zmiany prawne).

Rozdział 4

Postępowanie na wypadek zagrożenia bezpieczeństwa danych osobowych. Instrukcja postępowania z incydentami.

§12

Procedura definiuje katalog podatności i incydentów zagrażających bezpieczeństwu danych osobowych oraz opisuje sposób reagowania na nie. Jej celem jest minimalizacja skutków wystąpienia incydentów bezpieczeństwa oraz ograniczenie ryzyka powstania zagrożeń i występowania incydentów w przyszłości.

1. Każda osoba upoważniona do przetwarzania danych osobowych zobowiązana jest do powiadamiania o stwierdzeniu podatności lub wystąpieniu incydentu bezpośredniego przełożonego (lub jeśli jest powołany – Inspektora Ochrony Danych).
2. Do typowych podatności bezpieczeństwa danych osobowych należą:
    a. niewłaściwe zabezpieczenie fizyczne pomieszczeń, urządzeń i dokumentów,
    b. niewłaściwe zabezpieczenie sprzętu IT, oprogramowania przed wyciekiem, kradzieżą i utratą danych osobowych,
    c. nieprzestrzeganie zasad ochrony danych osobowych przez pracowników (np. niestosowanie zasady czystego biurka / ekranu, ochrony haseł, niezamykanie pomieszczeń, szaf, biurek).
3. Do typowych incydentów bezpieczeństwa danych osobowych należą:
    a. zdarzenia losowe zewnętrzne (pożar obiektu/pomieszczenia, zalanie wodą, utrata zasilania, utrata łączności),
    b. zdarzenia losowe wewnętrzne (awarie serwera, komputerów, twardych dysków, oprogramowania, pomyłki informatyków, użytkowników, utrata / zagubienie danych),
    c. umyślne incydenty (włamanie do systemu informatycznego lub pomieszczeń, kradzież danych/sprzętu, wyciek informacji, ujawnienie danych osobom nieupoważnionym, świadome zniszczenie dokumentów/danych, działanie wirusów i innego szkodliwego oprogramowania).
4. W przypadku stwierdzenia wystąpienia incydentu, Administrator (bądź IOD) prowadzi postępowanie wyjaśniające w toku, którego:
    a. ustala zakres i przyczyny incydentu oraz jego ewentualne skutki,
    b. inicjuje ewentualne działania dyscyplinarne,
    c. działa na rzecz przywrócenia działań organizacji po wystąpieniu incydentu,
    d. rekomenduje działania prewencyjne (zapobiegawcze) zmierzające do eliminacji podobnych incydentów w przyszłości lub zmniejszenia strat w momencie ich zaistnienia.
5. Administrator dokumentuje powyższe wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze (Załącznik nr 4 – Formularz rejestracji incydentu),
6. Zabrania się świadomego lub nieumyślnego wywoływania incydentów przez osoby upoważnione do przetwarzania danych.
7. W przypadku naruszenia ochrony danych osobowych skutkującego ryzykiem naruszenia praw lub wolności osób fizycznych, Administrator bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – zgłasza je organowi nadzorczemu.

Rozdział 5

Regulamin Ochrony Danych Osobowych, polityka kluczy.

§13

1. Regulamin ma na celu zapewnienie wiedzy osobom przetwarzającym dane osobowe odnośnie zasad przetwarzania tych danych zgodnie z przepisami prawa (Załącznik nr 5 – Regulamin Ochrony Danych Osobowych w PANS w Jarosławiu).
2. Po zapoznaniu się z zasadami ochrony danych osobowych, osoby zobowiązane są do potwierdzenia znajomości tych zasad i deklaracji ich stosowania (Załącznik nr 6 – Oświadczenie o poufności).
3. Polityka kluczy ma na celu techniczne zapewnienie bezpieczeństwa danych osobowych. Polityka kluczy stanowi załącznik do niniejszej Polityki – Załącznik nr 7.

Rozdział 6

Szkolenia/ audyt

§14

1. Każda osoba, przed dopuszczeniem do pracy z danymi osobowymi powinna być poddana przeszkoleniu i zapozna z obowiązującymi przepisami prawa.
2. Za przeprowadzenie szkolenia odpowiada IOD.
3. W przypadku przeprowadzenia szkolenia wewnętrznego z zasad ochrony danych osobowych wskazane jest udokumentowanie odbycia tego szkolenia.
4. Po przeprowadzeniu szkolenia z zasad ochrony danych osobowych, uczestnicy są zobowiązani do potwierdzenia znajomości tych zasad i deklaracji ich stosowania.
5. Kierownik jednostki organizacyjnej obowiązany jest poinformować IOD o zatrudnieniu nowego pracownika i ustalić z IOD termin szkolenia z zakresu ochrony danych osobowych.
6. Zgodnie z art. 32 RODO Administrator powinien regularnie testować, mierzyć i oceniać skuteczność środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania. W tym celu Administrator stosuje procedurę audytów (Załącznik nr 8 – Procedura audytów).

Rozdział 7

Środki organizacyjne i techniczne zabezpieczające dane osobowe

§15

1. Administrator prowadzi uproszczony wykaz zabezpieczeń, które stosuje w celu ochrony danych osobowych (Załącznik nr 9 – Wykaz zabezpieczeń).
2. Administrator opracował dokument – Instrukcja zarządzania systemami informatycznymi –wykaz zabezpieczeń w PANS w Jarosławiu.
3. Wykaz powinien być aktualizowany, jeśli zajdzie taka potrzeba po przeprowadzeniu analizy ryzyka/oceny skutków.

§16

1. Zgodnie z art. 32 RODO, Administrator powinien zapewnić zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego.
2. Procedury przywracania dostępności danych osobowych i dostępu do nich zostały opracowane, jako załącznik – Załącznik nr 10 – Plan ciągłości działania.

Rozdział 8

Wykaz pomieszczeń wchodzących w skład przetwarzania danych osobowych PANS w Jarosławiu

§17

Wykaz pomieszczeń należących do PANS w Jarosławiu, w których dokonuje się operacji na danych osobowych, z uwzględnieniem pomieszczeń szczególnie chronionych stanowi załącznik do niniejszej Polityki – Załącznik nr 11 – Wykaz pomieszczeń.

Spis treści

Opis kategorii osób (zbioru) w formie rejestru czynności przetwarzania	Aktywa	Proces przetwarzania / opis funkcjonalny

1. Opis kategorii osób (nazwa zbioru) Kandydaci do pracy **1.a Opis kategorii danych osobowych** Dane identyfikacyjne (imię i nazwisko), data urodzenia, dane kontaktowe wskazane przez ubiegającego się o pracę, informacje dotyczące wykształcenia, kwalifikacji zawodowych, przebiegu dotychczasowego zatrudnienia, inne dane dobrowolnie podane przez ubiegającego się o zatrudnienie bądź wynikające z przepisów prawa **2. Cele przetwarzania** Rekrutacja pracowników **3. Kategorie odbiorców** Podmioty uprawnione na podstawie przepisów prawa **4. Kategorie odbiorców w państwach trzecich** lub w organizacjach międzynarodowych (i ich nazwy) – nie dotyczy **5. Planowane terminy usunięcia poszczególnych kategorii danych** w przypadku bieżącej rekrutację – czas przechowywania do 4 miesięcy po zakończeniu rekrutacji, w przypadku udzielonej zgody kandydatów na przyszłe rekrutacje – czas przechowywania określono na 2 lata **6. Opis technicznych i organizacyjnych środków bezpieczeństwa** Stosowane są techniczne i organizacyjne środki mające na celu zapewnienie poufności, integralności, dostępności, obowiązuje Polityka Ochrony Danych Osobowych oraz Instrukcja Zarządzania Systemami informatycznymi wykaz zabezpieczeń – RODO **7. Podstawa prawna przetwarzania** Art.6 ust. 1 lit. c RODO - wykonanie obowiązku prawnego ciążącego na administratorze (na podst. m.in.: ustawa z 26 czerwca 1974r. Kodeksu pracy) Art.6, ust 1, lit. a RODO (na podst. zgody osoby) – dodatkowe informacje udostępnione poza wymaganiami określonymi przez prawo; zgoda na przyszłe rekrutacje, wizerunek **8. Konieczność przeprowadzenia oceny skutków dla zbioru:** nie	**1. Informacje (dokumentacja papierowa)** CV, kwestionariusz osobowy, oświadczenia składane przez kandydata do pracy, dodatkowe informacje dołączone przez kandydata **2. Programy i systemy operacyjne** e-mail: poczta.pwste.edu.pl, **3. Infrastruktura IT** Serwer, macierz dyskowa, dyski sieciowe, wewnętrzna sieć, urządzenia sieciowe, stacje robocze **4. Infrastruktura** Pomieszczenia działu Spraw Pracowniczych Kancelarii,pomieszczenia kierowników/dziekanów, sekretariaty **5. Pracownicy i współpracownicy** Pracownicy działu Spraw Pracowniczych, Pracownik Kancelarii, Kierownicy Działów, członkowie komisji konkursowych, dziekani wydziałów, pracownicy sekretariatów **6. Outsourcing**	1.Odbieranie zgłoszeń przesłanych pocztą tradycyjną. 2. Odbieranie zgłoszeń złożonych osobiście i przekazanie do Działu Spraw Pracowniczych/ odpowiedniego sekretariatu. 3. Odbieranie zgłoszeń przesłanych pocztą elektroniczną. 4. Przekazanie CV dla członków komisji konkursowych (papierowo) celem wyboru kandydata. 5. Usunięcie CV osób nieprzyjętych do pracy po odpowiednim czasie/ zachowanie dokumentów osób przyjętych do pracy bądź w przypadku zgody przechowywanie przez określony okres i następnie usunięcie danych.
1. Opis kategorii osób (nazwa zbioru) Pracownicy, wykonawcy umów zlecenia/umów o dzieło, byli pracownicy **1.a Opis kategorii danych osobowych** Dane identyfikacyjne (imię i nazwisko), data urodzenia, dane adresowe, kontaktowe, wykształcenie, kwalifikacje zawodowe, przebieg dotychczasowego zatrudnienia, PESEL (w przypadku jego braku rodzaj i numer dokumentu potwierdzającego tożsamość), inne dane osobowe pracownika, informacje dotyczące zdolności do pracy, a także dane osobowe dzieci pracownika i innych członków jego najbliższej rodziny, (jeżeli jest to konieczne ze względu na przysługujące uprawnienia), numer rachunku bankowego, dane dotyczące wypadków przy pracy, dane dotyczące przyznanych premii/nagród, dokumentacja BHP, dane dotyczące stosunku do służby wojskowej na wypadek ogłoszenia mobilizacji i ogłoszenia wojny **2. Cele przetwarzania** Zatrudnianie pracowników, przebieg zatrudnienia, udzielanie świadczeń, opłacanie składek, wypłata wynagrodzenia, nagród, premii, przeprowadzanie szkoleń BHP, dokumentacje powypadkowe w przypadku wypadków przy pracy, obowiązek sprawozdawczy, informacje na temat karalności **3. Kategorie odbiorców** Medycyna pracy, ZUS, US, POLON, banki w zakresie dokonywanie przelewów wynagrodzeń, inne podmioty uprawnione na podstawie przepisów prawa **4. Kategorie odbiorców w państwach trzecich** lub w organizacjach międzynarodowych (i ich nazwy) – nie dotyczy **5. Planowane terminy usunięcia poszczególnych kategorii danych** Dane osób zatrudnionych w formie etatów - 50 lat, dane wykonawców umów cywilnoprawnych – 50 lat. Osoby zatrudnione po 01.01.2019 r. –	**1. Informacje (dokumentacja papierowa)** Akta osobowe, Dokumentacja BHP, **2. Programy i systemy operacyjne** Płatnik, Windows, pliki z danymi pracowników, EOD, email – poczta.pwste.edu.pl, ESET AntiVirus, Simple, RCP, POLON, USOS, Egeria **3. Infrastruktura IT** Serwer, macierz dyskowa, dyski sieciowe, wewnętrzna sieć, urządzenia sieciowe, stacje robocze **4. Infrastruktura** Pomieszczenia Działu Spraw Pracowniczych, Pomieszczenia Kwestury, Pomieszczenie Działu Kształcenia, serwerownia, archiwum, **5. Pracownicy i współpracownicy** Pracownicy Działu Spraw Pracowniczych, Pracownicy Kwestury, Informatycy, Pracownicy Działu Kształcenia, członkowie Komisji Socjalnej, pracownicy Archiwum, specjalista ds. BHP i P.POŻ **6. Outsourcing** Supra Brokers – umowa powierzenia Umowa powierzenia przetwarzania danych z osobą zajmującą się sprawami pracowników na Słowacji Program Płatnik – produkt udostępniony przez ZUS Umowa powierzenia danych z firmą	1. Prowadzenie akt osobowych i innej dokumentacji zatrudnieniowej. 2. Wprowadzenie danych do systemu kadrowo-płacowego. 3. Obsługa Zakładowego Funduszu świadczeń socjalnych. 4. Rozliczanie pracowników z ZUS oraz z US, wypłaty wynagrodzeń, organizacja wyjazdów służbowych, ubezpieczenia społecznego, ubezpieczenia chorobowego. 5. Prowadzenie ewidencji rozliczeń pracowników dydaktycznych, ustalanie listy zajęć i realizowanych godzin dydaktycznych. 6. Zatwierdzanie rachunków wystawionych przez wykonawców umów cywilnoprawnych. 7. Wprowadzania danych pracowników dydaktycznych do systemu MNiSW (POLON). 8. Archiwizacja danych byłych pracowników.

10 lat **6. Opis technicznych i organizacyjnych środków bezpieczeństwa** Stosowane są techniczne i organizacyjne środki mające na celu zapewnienie poufności, integralności, dostępności, obowiązuje Polityka Ochrony Danych Osobowych oraz Instrukcja Zarządzania Systemami informatycznymi – wykaz zabezpieczeń RODO **7. Podstawa prawna przetwarzania** Art.6, ust 1, lit. a RODO - odrębna zgoda - upublicznienie wizerunku pracownika za zgodą; zgoda na przetwarzanie innych danych dobrowolnych Art.6 ust. 1 lit. c RODO - wykonanie obowiązku prawnego ciążącego na administratorze (na podst. m.in.: ustawa z 26 czerwca 1974r. Kodeksu pracy, ustawa z 13 października 1998r. o systemie ubezpieczeń społecznych, ustawy z 20 lipca 2018 r. Prawo o szkolnictwie wyższym i nauce) Art. 6 ust. 1 lit. b RODO – wykonanie umowy, której stroną jest osoba, której dane dotyczą **8. Konieczność przeprowadzenia oceny skutków dla zbioru:** nie	WebChili Umowa powierzenia danych z firmą AutoID	
1. Opis kategorii osób (nazwa zbioru) Osoby uprawnione do korzystania z Zakładowego Funduszu Socjalnego **1.a Opis kategorii danych osobowych** Dane identyfikacyjne, dane o dochodach, o stanie rodziny, oświadczenia o sytuacji rodzinnej, zdrowotnej, oświadczenia o zdarzeniach uprawniających do udzielenia świadczenia z ZFŚS, oświadczenia o wysokości dochodów przypadających na członka rodziny **2. Cele przetwarzania** Przyznanie pomocy materialnej z Zakładowego Funduszu Świadczeń Socjalnych **3. Kategorie odbiorców** Banki w zakresie przelewów, podmioty uprawnione na podstawie przepisów prawa **4. Kategorie odbiorców w państwach trzecich** lub w organizacjach międzynarodowych (i ich nazwy) – nie dotyczy **5. Planowane terminy usunięcia poszczególnych kategorii danych** Przechowywane przez okres nie dłuższy niż jest to niezbędne do przyznania świadczenia oraz przez okres dochodzenia do nich praw lub roszczeń (5 lat) **6. Opis technicznych i organizacyjnych środków bezpieczeństwa** Stosowane są techniczne i organizacyjne środki mające na celu zapewnienie poufności, integralności, dostępności, obowiązuje Polityka Ochrony Danych Osobowych oraz Instrukcja Zarządzania Systemami informatycznymi – wykaz zabezpieczeń RODO **7. Podstawa prawna przetwarzania** Art.6, ust 1, lit. c RODO – wykonanie obowiązku ciążącego na Administratorze (m.in. ustawa z dnia 04 marca 1994 r. o zakładowym funduszu świadczeń socjalnych, ustawa z 21 lutego 2019 r. o zmianie niektórych ustaw w związku z zapewnieniem stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE)2016/679 z dnia 27.04.2016 r.) Art. 9 ust. 2 lit. b RODO – przetwarzanie jest niezbędne do wypełnienia obowiązków i wykonania szczególnych praw przez administratora lub osobę, której dane dotyczą w dziedzinie prawa pracy, zabezpieczenia społecznego i ochrony socjalnej **8. Konieczność przeprowadzenia oceny skutków dla zbioru:** nie	**1. Informacje (dokumentacja papierowa)** Dokumentacja ZFŚS (złożone wnioski, oświadczenia, zaświadczenia) **2. Programy i systemy operacyjne** Egeria, Płatnik, Windows, pliki z danymi pracowników, EOD, email – poczta.pwste.edu.pl, ESET antivirus, Simple **3. Infrastruktura IT** Serwer, macierz dyskowa, dyski sieciowe, wewnętrzna sieć, urządzenia sieciowe, stacje robocze **4. Infrastruktura** Pomieszczenia Działu Spraw Pracowniczych, Pomieszczenia Kwestury, Pomieszczenie Biblioteki, pokój Kanclerza, sekretariaty Kanclerza, Rektora **5. Pracownicy i współpracownicy** Pracownicy Działu Spraw Pracowniczych, Pracownicy Kwestury, Kwestor, Kanclerz, członkowie Komisji ZFŚS **6. Outsourcing** Umowa powierzenia danych osobowych zawarta z firmą Benefit Systems Spółka Akcyjna Umowy powierzenia danych z firmami turystycznymi Umowy powierzenia danych z firmami ubezpieczeniowymi w celu zawarcia polis ubezpieczeniowych	1. Przyjmowanie wniosków/oświadczeń. 2. Rozpatrywanie spraw. 3. Akceptowanie wniosków przez Kwestor/Kanclerza. 4. Przyznawanie świadczeń. 5. Zawieranie umów z pracownikami. 6. Prowadzenie dokumentacji. 7. Weryfikacja dokumentacji. 8. Usuwanie dokumentacji/ przekazywanie do Archiwum po określonym czasie.

1. Opis kategorii osób (nazwa zbioru) Zbiór teleadresowy **1.a Opis kategorii danych osobowych** Dane identyfikacyjne, dane adresowe tj. imię, nazwisko, nr tel., adres email **2. Cele przetwarzania** Obsługa sekretariatów, kontakt z pracownikami, studentami oraz innymi osobami **3. Kategorie odbiorców** Nie dotyczy **4. Kategorie odbiorców w państwach trzecich** lub w organizacjach międzynarodowych (i ich nazwy) – nie dotyczy **5. Planowane terminy usunięcia poszczególnych kategorii dany** 5 lat **6. Opis technicznych i organizacyjnych środków bezpieczeństwa** Stosowane są techniczne i organizacyjne środki mające na celu zapewnienie poufności, integralności, dostępności, obowiązuje Polityka Ochrony Danych Osobowych oraz Instrukcja Zarządzania Systemami informatycznymi – Wykaz zabezpieczeń RODO **7. Podstawa prawna przetwarzania** Art.6, ust 1 lit. f RODO– przetwarzanie niezbędne do realizacji celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora **8. Konieczność przeprowadzenia oceny skutków dla zbioru:** nie	**1. Informacje (dokumentacja papierowa)** Dane w formie papierowej **2. Programy i systemy operacyjne** Dane w formie elektronicznej –pliki na komputerze **3. Infrastruktura IT** Serwer, macierz dyskowa, dyski sieciowe, wewnętrzna sieć, urządzenia sieciowe, stacje robocze **4. Infrastruktura** Sekretariaty, Kancelaria, pomieszczenia poszczególnych działów **5. Pracownicy i współpracownicy** Pracownicy sekretariatu, kancelarii, poszczególnych działów **6. Outsourcing** brak	1. Wykonywanie połączeń telefonicznych, wysyłanie maili służbowych. 2.Usuwanie danych.
1. Opis kategorii osób (nazwa zbioru) Promocja PWSTE w Jarosławiu **1.a Opis kategorii danych osobowych** Dane identyfikacyjne, dane adresowe(kontaktowe), dane wizerunkowe, **2. Cele przetwarzania** Budowanie pozytywnego wizerunku Administratora w przestrzeni publicznej **3. Kategorie odbiorców** nie dotyczy **4. Kategorie odbiorców w państwach trzecich** lub w organizacjach międzynarodowych (i ich nazwy) – nie dotyczy **5. Planowane terminy usunięcia poszczególnych kategorii danych** do momentu wycofania zgody bądź odpowiednio do celów, dla których dane zostały pozyskane **6. Opis technicznych i organizacyjnych środków bezpieczeństwa** Stosowane są techniczne i organizacyjne środki mające na celu zapewnienie poufności, integralności, dostępności, obowiązuje Polityka Ochrony Danych Osobowych oraz Instrukcja Zarządzania Systemami informatycznymi – wykaz zabezpieczeń RODO **7. Podstawa prawna przetwarzania** art. 6, ust. 1 lit. a RODO – publikacja wizerunku na podstawie zgody, wykorzystywanie danych osobowych umieszczonych na portalach społecznościowych, art. 6 ust. 1 lit. f RODO usprawiedliwiony interes Administratora **8. Konieczność przeprowadzenia oceny skutków dla zbioru:** nie	**1. Informacje (dokumentacja papierowa)** Dane w formie papierowej oraz elektronicznej **2. Programy i systemy operacyjne** Windows, EOD, MS Office, poczta – pwste.edu.pl, **3. Infrastruktura IT** Stacja robocza **4. Infrastruktura** pomieszczenia Biura Rektora, **5. Pracownicy i współpracownicy** pracownicy Biura Rektora, pracownicy wydziałów **6. Outsourcing** Umowa powierzenia z firmą drukującą, Umowa powierzenia z firmami świadczącymi usługi marketingowe/reklamowe Umowy powierzenia danych z firmami wykonującymi fotografie	1. Wykonywanie zdjęć promocyjnych z wydarzeń realizowanych przez PWSTE w Jarosławiu. 2.Podejmowanie działań promocyjnych (klipy promocyjne, wysyłka emaili promocyjnych). 3. Udzielanie odpowiedzi na portalach społecznościowych. 4. Usuwanie danych.
1. Opis kategorii osób (nazwa zbioru) Kontrahenci: dostawcy/wykonawcy • Zbiór dostawców/wykonawców znajdujący się w Dziale Administracyjno-Gospodarczym, • Zbiór dostawców/wykonawców znajdujący się w Dziale Telekomunikacji i Automatyki • Zbiór dostawców/wykonawców znajdujący się w Dziale Inwestycyjno-Technicznym **1.a Opis kategorii danych osobowych** Dane identyfikacyjne, dane adresowe tj. imię, nazwisko, nr tel., adres email, nr konta bankowego, dane dotyczące działalności,	**1. Informacje (dokumentacja papierowa)** Zamówienia, faktury od dostawców, umowy, rachunki **2. Programy i systemy operacyjne** Windows, EOD, MS Office, poczta – pwste.edu.pl, Simple ERP **3. Infrastruktura IT** Serwer, macierz dyskowa, NAS, dyski sieciowe, wewnętrzna sieć, router, switche, stacje robocze, **4. Infrastruktura** Pomieszczenia Działu Administracyjno-	1.Nawiązywanie kontaktów biznesowych. 2. Umowa z dostawcą/ Zamówienie towaru, usługi (przesłanie do dostawcy mailem). 3. Przyjęcie faktury i WZ – mailem lub papierowo. 4. Wprowadzenie danych do systemu Simple. 5. Księgowanie. 6. Realizacja płatności za

2. Cele przetwarzania Realizacja umów na dostawę towarów lub usług świadczonych przez osoby fizyczne prowadzące działalność gospodarczą, utrzymywanie i wykonywanie relacji biznesowych **3. Kategorie odbiorców** Banki w zakresie przelewów, podmioty uprawnione na podstawie przepisów prawa, **4. Kategorie odbiorców w państwach trzecich** lub w organizacjach międzynarodowych (i ich nazwy) – nie dotyczy **5. Planowane terminy usunięcia poszczególnych kategorii danych** 6 lat **6. Opis technicznych i organizacyjnych środków bezpieczeństwa** Stosowane są techniczne i organizacyjne środki mające na celu zapewnienie poufności, integralności, dostępności, obowiązuje Polityka Ochrony Danych Osobowych oraz Instrukcja Zarządzania Systemami informatycznymi **7. Podstawa prawna przetwarzania** art. 6 ust. 1 lit. c RODO wykonanie obowiązku prawnego ciążącego na administratorze (m.in. ustawa z 29 stycznia 2004 r. Prawo zamówień publicznych) art. 6 ust. 1 lit. b RODO – wykonanie umowy, której stroną jest osoba, której dane dotyczą **8. Konieczność przeprowadzenia oceny skutków dla zbioru:** nie	Gospodarczego, Telekomunikacji i Automatyki, Inwestycyjno-Technicznego, Kwestury, serwerownia, **5. Pracownicy i współpracownicy** Pracownicy Działu Administracyjno-Gospodarczego, Telekomunikacji i Automatyki, Inwestycyjno-Gospodarczego, Kwestury, Działu Informatyki, Kwestor, Kanclerz **6. Outsourcing**	faktury. 7. Archiwizacja faktur, umów.
1. Opis kategorii osób (nazwa zbioru) Rejestr korespondencyjny **1a. Opis kategorii danych osobowych** Dane identyfikacyjne, dane adresowe tj. imię, nazwisko, adres zamieszkania **2. Cele przetwarzania** Zarządzanie korespondencją przychodzącą i wychodzącą **3. Kategorie odbiorców** Poczta Polska **4. Kategorie odbiorców w państwach trzecich** lub w organizacjach międzynarodowych (i ich nazwy) – nie dotyczy **5. Planowane terminy usunięcia poszczególnych kategorii danych** Zgodnie z instrukcją kancelaryjną **6. Opis technicznych i organizacyjnych środków bezpieczeństwa** Stosowane są techniczne i organizacyjne środki mające na celu zapewnienie poufności, integralności, dostępności, obowiązuje Polityka Ochrony Danych Osobowych oraz Instrukcja Zarządzania Systemami informatycznymi – Wykaz zabezpieczeń RODO **7. Podstawa prawna przetwarzania** Art.6 ust 1 lit. c RODO – wykonanie obowiązku prawnego ciążącego na administratorze (Ustawa z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego, Ustawa z 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach) Art. 6 ust. 1 lit. f RODO – przetwarzanie jest niezbędne do realizacji celów wynikających z prawnie uzasadnionych interesów realizowanych przez Administratora **8. Konieczność przeprowadzenia oceny skutków dla zbioru:** nie	**1. Informacje (dokumentacja papierowa)** Książka korespondencyjna **2. Programy i systemy operacyjne** Rejestr w formie papierowej **3. Infrastruktura IT** Serwer, macierz dyskowa, NAS, dyski sieciowe, wewnętrzna sieć, router, switche, stacje robocze, **4. Infrastruktura** Sekretariaty, Kancelaria, pracownicy poszczególnych działów **5. Pracownicy i współpracownicy** Pracownicy sekretariatów, Kancelarii (Biura Rektora), poszczególnych działów/wydziałów, **6. Outsourcing** brak	1. Rejestracja papierowa korespondencji wysyłanej i otrzymywanej. 2. Archiwizacja.
1. Opis kategorii osób (nazwa zbioru) Czytelnicy biblioteki **1.a Opis kategorii danych osobowych** Dane identyfikacyjne, dane adresowe tj. imię, nazwisko, nr tel., adres email, miejsce zamieszkania, PESEL, nr dowodu osobistego bądź innego dokumentu potwierdzającego tożsamość, nr legitymacji/tytuł naukowy, kategoria zawodowa, imię ojca (jako dana dobrowolna) **2. Cele przetwarzania** Umożliwienie korzystania z zasobów bibliotecznych **3. Kategorie odbiorców** podmioty uprawnione na podstawie przepisów prawa	**1. Informacje (dokumentacja papierowa)** Dokumentacja niezbędna do utworzenia konta bibliotecznego oraz dokumentacja wypożyczeni **2. Programy i systemy operacyjne** Windows, EOD, MS Office, poczta – pwste.edu.pl, Sowa **3. Infrastruktura IT** Serwer, macierz dyskowa, NAS, dyski sieciowe, wewnętrzna sieć, router, switche, stacje robocze,	1. Rejestracja czytelnika. 2. Wprowadzenie danych czytelnika do systemy SowaSQL. 3. Obsługa czytelników, wypożyczanie pozycji bibliotecznych, podpijanie kart obiegowych. 4. Usuwanie danych nieaktywnych czytelników. 5. Przekazywanie do firm

4. Kategorie odbiorców w państwach trzecich lub w organizacjach międzynarodowych (i ich nazwy) – nie dotyczy **5. Planowane terminy usunięcia poszczególnych kategorii danych** Dane studentów po zakończeniu studiów, dane pracowników po rozwiązaniu umowy, dane osób z zewnątrz zgodnie z postanowieniami Regulaminu udostępniania zbiorów bibliotecznych **6. Opis technicznych i organizacyjnych środków bezpieczeństwa** Stosowane są techniczne i organizacyjne środki mające na celu zapewnienie poufności, integralności, dostępności, obowiązuje Polityka Ochrony Danych Osobowych oraz Instrukcja Zarządzania Systemami informatycznymi – Wykaz zabezpieczeń RODO **7. Podstawa prawna przetwarzania** Art.6 ust 1, lit. c RODO - wykonanie obowiązku ciążącego na administratorze (m.in. ustawa z 27 czerwca 1997 r. o bibliotekach) art. 6, ust. 1 lit. a RODO – dane dobrowolne przetwarzane na podstawie zgody **8. Konieczność przeprowadzenia oceny skutków dla zbioru:** nie	**4. Infrastruktura** Pomieszczenia Biblioteki, serwerownia, pomieszczenia Kwestury **5. Pracownicy i współpracownicy** Pracownicy Biblioteki, Działu Informatyki, Kwestury **6. Outsourcing** Sokrates – umowa powierzenia	windykacyjnych w przypadku powstania zadłużenia.
1. Opis kategorii osób (nazwa zbioru) Rejestr wejść i wyjść **1a. Opis kategorii danych osobowych** Dane identyfikacyjne (imię i nazwisko) pracowników **2. Cele przetwarzania** Nadzór nad obecnością pracowników na terenie uczelni w czasie pracy **3. Kategorie odbiorców** Nie dotyczy **4. Kategorie odbiorców w państwach trzecich** lub w organizacjach międzynarodowych (i ich nazwy) – nie dotyczy **5. Planowane terminy usunięcia poszczególnych kategorii danych** Zgodnie z przepisami prawa **6. Opis technicznych i organizacyjnych środków bezpieczeństwa** Stosowane są techniczne i organizacyjne środki mające na celu zapewnienie poufności, integralności, dostępności, obowiązuje Polityka Ochrony Danych Osobowych **7. Podstawa prawna przetwarzania** Art.6, ust 1, lit. c RODO– wykonanie obowiązku prawnego ciążącego na administratorze (Ustawa z 26 czerwca 1974r. Kodeks pracy, wewnętrzny regulamin organizacyjny) **8. Konieczność przeprowadzenia oceny skutków dla zbioru:** nie	**1. Informacje (dokumentacja papierowa)** Księga wejść, ewidencja czasu pracy **2. Programy i systemy operacyjne** Nie dotyczy **3. Infrastruktura IT** Nie dotyczy **4. Infrastruktura** Portiernia, pomieszczenie Działu Spraw Pracowniczych, pomieszczenia poszczególnych kierowników, upoważnionych pracowników **5. Pracownicy i współpracownicy** Pracownicy Działu Administracyjno-Gospodarczego, pracownicy Działu Spraw Pracowniczych, Kanclerz, Kwestor, upoważnieni pracownicy w poszczególnych działach **6. Outsourcing**	1. Rejestracja papierowa pracowników rozpoczynających pracę w danym dniu oraz opuszczających miejsce pracy w godzinach pracy. 2. Archiwizacja.
1. Opis kategorii osób (nazwa zbioru) Monitoring **1a. Opis kategorii danych osobowych** Dane wizerunkowe osób przebywających na uczelni (studentów, pracowników, osób spoza uczelni) **2. Cele przetwarzania** Zabezpieczenie obiektu i mienia, zachowanie w tajemnicy informacji, których ujawnienie mogłoby narazić Uczelnię na szkodę) **3. Kategorie odbiorców** Podmioty uprawnione na podstawie przepisów prawa **4. Kategorie odbiorców w państwach trzecich** lub w organizacjach międzynarodowych (i ich nazwy) – nie dotyczy **5. Planowane terminy usunięcia poszczególnych kategorii danych** do 1 miesiąca **6. Opis technicznych i organizacyjnych środków bezpieczeństwa** Stosowane są techniczne i organizacyjne środki mające na celu zapewnienie poufności, integralności, dostępności, obowiązuje Polityka Ochrony Danych Osobowych oraz Instrukcja Zarządzania Systemami informatycznymi – wykaz zabezpieczeń RODO **7. Podstawa prawna przetwarzania** Art.6, ust 1, lit. c RODO – wykonanie obowiązku prawnego ciążącego na administratorze(ustawa z 26 czerwca 1974r. Kodeks pracy) **8. Konieczność przeprowadzenia oceny skutków dla zbioru:**	**1. Informacje (dokumentacja papierowa)** brak **2. Programy i systemy operacyjne** Rejestratory, programy zapewniające obsługę systemu **3. Infrastruktura IT** Serwer, wewnętrzna sieć, stacje robocze, kamery, okablowanie, wewnętrzne programy **4. Infrastruktura** Portiernia, serwerownia, stanowiska monitoringu, Pomieszczenie Działu Telekomunikacji i Automatyki **5. Pracownicy i współpracownicy** Pracownicy Działu Administracyjno-Gospodarczego, Działu Telekomunikacji i Automatyki, Kanclerz **6. Outsourcing**	1. Bieżąca kontrola obrazu. 2. Zabezpieczenie nagrań. 3. Konserwacja i naprawa sprzętu nagrywającego. 4. Udostępnianie nagrań uprawnionym podmiotom. 5. Usuwanie nagrań.

nie		
1. Opis kategorii osób (nazwa zbioru) Zbiór przetargów **1.a Opis kategorii danych osobowych** Osoby kontaktowe ze strony oferenta, imię, nazwisko, dane korespondencyjne w przypadku osób fizycznych **2. Cele przetwarzania** Realizacja zamówień publicznych **3. Kategorie odbiorców** Nie dotyczy **4. Kategorie odbiorców w państwach trzecich** lub w organizacjach międzynarodowych (i ich nazwy) – nie dotyczy **5. Planowane terminy usunięcia poszczególnych kategorii danych** Zgodnie z instrukcją kancelaryjną **6. Opis technicznych i organizacyjnych środków bezpieczeństwa** Stosowane są techniczne i organizacyjne środki mające na celu zapewnienie poufności, integralności, dostępności, obowiązuje Polityka Ochrony Danych Osobowych oraz Instrukcja Zarządzania Systemami informatycznymi – wykaz zabezpieczeń RODO **7. Podstawa prawna przetwarzania** Art.6, ust 1, lit. c RODO – wypełnienie prawnego obowiązku ciążącego na administratorze (ustawa z 29 stycznia 2004r. Prawo zamówień publicznych) **8. Konieczność przeprowadzenia oceny skutków dla zbioru:** nie	**1. Informacje (dokumentacja papierowa)** Dokumentacja oferentów **2. Programy i systemy operacyjne** Windows, EOD, ESET antivirus, poczta – pwste.edu.pl, **3. Infrastruktura IT** Serwer, macierz dyskowa, NAS, dyski sieciowe, wewnętrzna sieć, router, switche, stacje robocze, **4. Infrastruktura** Pomieszczenia Działu Administracyjno-Gospodarczego, **5. Pracownicy i współpracownicy** Pracownicy Dział Administracyjno-Gospodarczego, pracownicy Działu Informatyki, **6. Outsourcing**	1. Zbieranie ofert od oferentów. 2. Wybór oferenta. 3. Ogłoszenie zwycięzcy konkursu. 4. Publikacja danych podmiotu. 5. Zawieranie umów. 6. Archiwizacja
1. Opis kategorii osób (nazwa zbioru) Kandydaci na studia **1.a Opis kategorii danych osobowych** Dane identyfikacyjne kandydatów: imię, nazwisko, data urodzenia, nr dowodu osobistego, adres zamieszkania, adres do korespondencji, dane o wykształceniu, ankieta osobowa, adres e-mail, nr telefonu **2. Cele przetwarzania** Rekrutacja na studia **3. Kategorie odbiorców** Podmioty uprawnione na podstawie przepisów prawa **4. Kategorie odbiorców w państwach trzecich** lub w organizacjach międzynarodowych (i ich nazwy) – nie dotyczy **5. Planowane terminy usunięcia poszczególnych kategorii danych** Dane studentów, którzy nie zostali przyjęci na studia usuwane są po 6 miesiącach, dane kandydatów na studia po zakończeniu postępowania i przyjęciu na studia zostają przeniesione do zbioru studentów **6. opis technicznych i organizacyjnych środków bezpieczeństwa** Stosowane są techniczne i organizacyjne środki mające na celu zapewnienie poufności, integralności, dostępności, obowiązuje Polityka Ochrony Danych Osobowych oraz Instrukcja Zarządzania Systemami informatycznymi – Wykaz zabezpieczeń RODO **7. Podstawa prawna przetwarzania** Art.6, ust 1, lit. a RODO – zgoda na przetwarzanie danych Art. 6 ust. 1 lit. c – realizowanie prawnego obowiązku ciążącego na administratorze (m.in.: Ustawa z dnia 20 lipca 2018 r. Prawo o szkolnictwie wyższym i nauce, Rozporządzenie Ministra Nauki i Szkolnictwa Wyższego z dnia 27 września 2018 r. w sprawie studiów)	**1. Informacje** Wnioski składane w formie elektronicznej oraz w formie papierowej **2. Programy i systemy operacyjne** Program „IRK”, **3. Infrastruktura IT** Serwer, macierz dyskowa, NAS, dyski sieciowe, wewnętrzna sieć, router, switche, stacje robocze, **4. Infrastruktura** Pomieszczenie Działu Obsługi Studentów, Działu Informatyki **5. Pracownicy i współpracownicy** Pracownicy Działu Obsługi Studentów, Informatycy, członkowie Komisji Rekrutacyjnej, pracownicy Kwestury, Kwestor **6. Outsourcing** Umowa o współpracy zawarta z Uniwersytetem Warszawskim	1. Zapewnienie prawidłowego funkcjonowania systemu elektronicznego do składania wniosków. 2. Ogłoszenie wstępnie przyjętych na studia. 3. Składanie wniosków w wersji papierowej. 4. Wybór kandydatów. 5. Usuwanie danych studentów, którzy nie zostali przyjęci na studia. 6. Zwrot opłaty rekrutacyjnej w przypadku nieotwarcia kierunku.
1. Opis kategorii osób (nazwa zbioru) Studenci (w tym byli studenci) **1.a Opis kategorii danych osobowych** Dane studentów: dane identyfikacyjne, kontaktowe, data rozpoczęcia i zakończenia nauki, świadectwo dojrzałości, wyniki egzaminów, karty okresowe osiągnięć studenta, oświadczenia o stanie rodziny, stanie zdrowia, dochodach – w przypadku studentów starających się o świadczenia socjalne dokumenty o przyznaniu studentowi pomocy materialnej, dane studentów, którzy ukończyli studia i stali się absolwentami, dane dotyczące zatrudnieniu lub umowy o pracę do celów	**1. Informacje (dokumentacja papierowa)** Teczki studenckie **2. Programy i systemy operacyjne** USOS, poczta – pwste.edu.pl, EOD, Egeria-Uczelnia (Nextech), POLON, Program do Elektronicznej Legitymacji Studenckiej, APR system, Microsoft Teams **3. Infrastruktura IT** Serwer, macierz dyskowa, NAS, dyski sieciowe, wewnętrzna sieć, router, switche, stacje robocze,	1. Założenie ewidencji studentów. 2. Prowadzenie dokumentacji studenckiej. 3. Wydawanie zaświadczeń 4. Udzielanie pomocy materialnej. 5. Wypłacanie stypendiów 6. Organizacja praktyk studenckich.

zwolnienia z odbycia obowiązkowych praktyk, numer albumu **2. Cele przetwarzania** Świadczenie usług edukacyjnych (studiowanie), prowadzenie dokumentacji studenckiej, świadczenie pomocy materialnej studentom, załatwianie spraw studenckich **3. Kategorie odbiorców** ZUS, KRUS, podmioty uprawnione na podstawie przepisów szczególnych, Ministerstwo Nauki i Szkolnictwa Wyższego, banki w zakresie przelewów, Medycyna Pracy, **4. Kategorie odbiorców w państwach trzecich** lub w organizacjach międzynarodowych (i ich nazwy) – nie dotyczy **5. Planowane terminy usunięcia poszczególnych kategorii danych** 50 lat **6. Opis technicznych i organizacyjnych środków bezpieczeństwa** Stosowane są techniczne i organizacyjne środki mające na celu zapewnienie poufności, integralności, dostępności, obowiązuje Polityka Ochrony Danych Osobowych oraz Instrukcja Zarządzania Systemami informatycznymi – Wykaz zabezpieczeń RODO **7. Podstawa prawna przetwarzania** Art.6, ust 1, lit. a – Zgoda studenta na przetwarzanie danych osobowych Art.6, ust 1 lit. c RODO – wypełnienie obowiązków prawnych ciążących na administratorze (m.in. ustawa z dnia 20 lipca 2018 r. Prawo o szkolnictwie wyższym i nauce, Rozporządzenie Ministra Nauki i Szkolnictwa Wyższego z dnia 27 września 2018 r. w sprawie studiów) Art. 6 ust. 1 lit. b RODO – realizacja umowy, której storną jest osoba, której dane dotyczą Art. 9 ust. 2 lit. b RODO- wykonywanie obowiązków i szczególnych praw w dziedzinie ochrony socjalnej **8. Konieczność przeprowadzenia oceny skutków dla zbioru:** tak	**4. Infrastruktura** Pomieszczenie Działu Obsługi Studentów, Działu Informatyki, Kwestury, Sekretariatu Prorektora, Rektora, Działu Spraw Pracowniczych, wydziałów, Archiwum **5. Pracownicy i współpracownicy** Pracownicy Działu Obsługi Studentów, Działu Informatyki, członkowie komisji socjalnych ds. studentów, Kwestury, Działu Spraw Pracowniczych, Archiwum, pracownicy dydaktyczni, Kwestor, koordynatorzy praktyk studenckich **6.Outsourcing**	7. Archiwizacja.
1. Opis kategorii osób (nazwa zbioru) Uczestnicy studiów podyplomowych **1.a Opis kategorii danych osobowych** Dane uczestników: dane identyfikacyjne, kontaktowe, data rozpoczęcia i zakończenia nauki,świadectwo dojrzałości, wyniki egzaminów, karty okresowe osiągnięć studenta, dokumenty o przyznaniu studentowi pomocy materialnej **2. Cele przetwarzania** Świadczenie usług edukacyjnych (studiowanie), prowadzenie dokumentacji, załatwianie spraw związanych z odbywaniem studiów podyplomowych **3. Kategorie odbiorców** ZUS, KRUS, podmioty uprawnione na podstawie przepisów szczególnych, **4. Kategorie odbiorców w państwach trzecich** lub w organizacjach międzynarodowych (i ich nazwy) – nie dotyczy **5. Planowane terminy usunięcia poszczególnych kategorii danych** 50 lat **6. Opis technicznych i organizacyjnych środków bezpieczeństwa** Stosowane są techniczne i organizacyjne środki mające na celu zapewnienie poufności, integralności, dostępności, obowiązuje Polityka Ochrony Danych Osobowych oraz Instrukcja Zarządzania Systemami informatycznymi – wykaz zabezpieczeń RODO **7. Podstawa prawna przetwarzania** Art.6, ust 1, lit. c RODO- wykonanie obowiązku prawnego ciążącego na administratorze (m.in.: Ustawa z dnia 20 lipca 2018 r. Prawo o szkolnictwie wyższym i nauce; Rozporządzenie Ministra Nauki i Szkolnictwa Wyższego z dnia 27 września 2018 r. w sprawie dokumentacji przebiegu studiów), Art. 6 ust. 1 lit. b RODO – realizacja umow, której stroną jest osoba, której dane dotyczą, Art.6, ust 1 lit. a RODO – zgoda osoby na przetwarzanie danych	**1. Informacje (dokumentacja papierowa)** Teczki słuchaczy studiów podyplomowych **2. Programy i systemy operacyjne** USOS, poczta – pwste.edu.pl, EOD, Egeria-Uczelnia (Nextech), POLON, **3. Infrastruktura IT** Serwer, macierz dyskowa, NAS, dyski sieciowe, wewnętrzna sieć, router, switche, stacje robocze, **4. Infrastruktura** Pomieszczenie Działu Obsługi Studentów, Działu Informatyki, Kwestury, **5. Pracownicy i współpracownicy** Pracownicy Działu Obsługi Studentów, Działu Informatyki, Kwestury, Kwestor, kierownicy studiów podyplomowych zatrudnieni do prowadzenia studiów podyplomowych, pracownicy dydaktyczni **6. Outsourcing**	1. Złożenie kompletu dokumentów w formie papierowej. 2.Założenie ewidencji słuchaczy. 3. Prowadzenie dokumentacji uczestników studiów podyplomowych. 4. wydawanie zaświadczeń. 5. Archiwizacja.

dobrowolnych **8. Konieczność przeprowadzenia oceny skutków dla zbioru:** nie		
1. Opis kategorii osób (nazwa zbioru) Zbiór umów: • Zbiór umów najmu w Dziale Administracyjno-Gospodarczym • Zbiór umów najmu w Dziale Inwestycyjno-Technicznym • Zbiór umów zawieranych ze studentami do celów wyjazdowych **1.a Opis kategorii danych osobowych** Dane osobowe, dane kontaktowe osób, z którymi zawarto umowy, w zależności od rodzaju umowy: numer PESEL, adres zamieszkania, numer dokumentu potwierdzającego tożsamość, numer konta bankowego **2. Cele przetwarzania** Bieżąca realizacja umowy **3. Kategorie odbiorców** m.in. banki w zakresie przelewów, inne podmioty uprawnione na podstawie przepisów prawa **4. Kategorie odbiorców w państwach trzecich** lub w organizacjach międzynarodowych (i ich nazwy) – nie dotyczy **5. Planowane terminy usunięcia poszczególnych kategorii danych** Zgodnie z instrukcją kancelaryjną **6. Opis technicznych i organizacyjnych środków bezpieczeństwa** Stosowane są techniczne i organizacyjne środki mające na celu zapewnienie poufności, integralności, dostępności, obowiązuje Polityka Ochrony Danych Osobowych oraz Instrukcja Zarządzania Systemami informatycznymi – wykaz zabezpieczeń RODO **7. Podstawa prawna przetwarzania** Art.6 ust 1, lit. c RODO – wykonanie obowiązku prawnego ciążącego na administratorze (Ustawa z 23 kwietnia 1964r. Kodeks cywilny) Art. 6 ust. 1 lit. b RODO – wykonanie umowy, której stroną jest osoba, której dane dotyczą **8. Konieczność przeprowadzenia oceny skutków dla zbioru:** nie	**1. Informacje (dokumentacja papierowa)** Dokumentacja najemców **2. Programy i systemy operacyjne** Windows, EOD, ESET antivirus, poczta – pwste.edu.pl, Centos5 **3. Infrastruktura IT** Serwer, macierz dyskowa, NAS, dyski sieciowe, wewnętrzna sieć, router, switche, stacje robocze, **4. Infrastruktura** Pomieszczenia Działu Administracyjno-Gospodarczego**,** pomieszczenie Działu Inwestycyjno-Techniczny, Kwestury **5. Pracownicy i współpracownicy** Kanclerz, Kwestor, Pracownicy Działu Administracyjno-Gospodarczego, Pracownicy Działu Inwestycyjno-Technicznego, Kwestury **6. Outsourcing**	1. Sporządzanie umów. 2. Prowadzenie ewidencji umów. 3. Rozliczanie płatności (księgowanie). 4. Wprowadzanie faktur do systemu EOD. 5. Archiwizacja. 6. Usuwanie danych.
1. Opis kategorii osób (nazwa zbioru) Zbiór danych osób uczestniczących w konferencjach organizowanych przez PANS w Jarosławiu **1.a Opis kategorii danych osobowych** dane kontaktowe osób, które brały udział w konferencjach (imię, nazwisko, adres do korespondencji, adres mailowy, numer telefonu, nr konta bankowego w przypadku odpłatnych konferencji) **2. Cele przetwarzania** Kontakt z uczestnikami konferencji, zapraszanie na kolejne edycje konferencji/wydarzeń **3. Kategorie odbiorców** Nie dotyczy **4. Kategorie odbiorców w państwach trzecich** lub w organizacjach międzynarodowych (i ich nazwy) – nie dotyczy **5. Planowane terminy usunięcia poszczególnych kategorii danych** **6. Opis technicznych i organizacyjnych środków bezpieczeństwa** Stosowane są techniczne i organizacyjne środki mające na celu zapewnienie poufności, integralności, dostępności, obowiązuje Polityka Ochrony Danych Osobowych oraz Instrukcja Zarządzania Systemami	**1. Informacje (dokumentacja papierowa)** Dane kontaktowe w formie plików na komputerze/zbiorów papierowych **2. Programy i systemy operacyjne** Windows, EOD, ESET antivirus, poczta – pwste.edu.pl, **3. Infrastruktura IT** Serwer, macierz dyskowa, NAS, dyski sieciowe, wewnętrzna sieć, router, switche, stacje robocze, **4. Infrastruktura** Pomieszczenia sekretariatów instytutów, biblioteki **5. Pracownicy i współpracownicy** Pracownicy Sekretariatów instytutów, pracownicy biblioteki, sekretarze konferencji, członkowie komitetów organizacyjnych **6. Outsourcing**	1. Prowadzenie zbioru danych kontaktowych. 2. Wysyłanie zaproszeń na konferencje. 3. Przyjmowanie materiałów pokonferencyjnych. 4. Wydawanie zaświadczeń/certyfikatów. 5. Wykonywanie fotografii. 6. Archiwizacja. 7. Usuwanie danych.

informatycznymi – Wykaz zabezpieczeń RODO **7. Podstawa prawna przetwarzania** Art.6 ust 1 lit. a RODO – na podstawie zgody na przetwarzanie danych osobowych w celach kontaktowych, informowanie o przyszłych konferencjach Art. 6 ust. 1 lit. f RODO – usprawiedliwiony interes Administratora **8. Konieczność przeprowadzenia oceny skutków dla zbioru:** nie		
1. Opis kategorii osób (nazwa zbioru) Zbiór danych recenzentów/autorów/redaktorów publikacji wydawanych przez PANS w Jarosławiu **1.a Opis kategorii danych osobowych** dane kontaktowe recenzentów, autorów, redaktorów publikacji (imię, nazwisko, adres do korespondencji, adres mailowy, numer telefonu), dane zawarte w rachunku konieczne do wypłaty wynagrodzenia i wypełnienia obowiązków prawnych **2. Cele przetwarzania** Kontakt z redaktorami, recenzentami, autorami; sporządzenie umów z recenzentami; autorami, wypłata wynagrodzenia **3. Kategorie odbiorców** Nie dotyczy **4. Kategorie odbiorców w państwach trzecich** lub w organizacjach międzynarodowych (i ich nazwy) – nie dotyczy **5. Planowane terminy usunięcia poszczególnych kategorii danych** Zgodnie z wewnętrzną procedurą **6. Opis technicznych i organizacyjnych środków bezpieczeństwa** Stosowane są techniczne i organizacyjne środki mające na celu zapewnienie poufności, integralności, dostępności, obowiązuje Polityka Ochrony Danych Osobowych oraz Instrukcja Zarządzania Systemami informatycznymi – Wykaz zabezpieczeń RODO **7. Podstawa prawna przetwarzania** Art.6, ust 1, lit. a RODO – na podstawie zgody na przetwarzanie danych w celach kontaktowych Art.6 ust. 1 lit. b RODO– wykonanie umowy, której stroną jest osoba, której dane dotyczą, **8. Konieczność przeprowadzenia oceny skutków dla zbioru:** nie	**1. Informacje (dokumentacja papierowa)** Dane kontaktowe w formie plików na komputerze/zbiorów papierowych **2. Programy i systemy operacyjne** Windows, Ubuntu 22, EOD, ESET antivirus, poczta – pwste.edu.pl, system OJS/PKP (czasopisma.pwste.edu.pl) **3. Infrastruktura IT** Serwer, macierz dyskowa, NAS, dyski sieciowe, wewnętrzna sieć, router, switche, stacje robocze, **4. Infrastruktura** Pomieszczenia sekretariatów wydziałów, Działu Kształcenia, Biblioteki, Kwestury **5. Pracownicy i współpracownicy** Pracownicy Sekretariatów wydziałów, pracownicy Biblioteki, pracownicy Działu Kształcenia, pracownicy Działu Spraw Pracowniczych, Kwestury, Kanclerz, Kwestor **6. Outsourcing**	1. Sporządzanie umów z recenzentami. 3. Sporządzanie umów licencyjnych z autorami. 4. Zgłaszanie do ZUS. 5. Wypłata wynagrodzeń. 6. Archiwizacja.
1. Opis kategorii osób (nazwa zbioru) Uniwersytet Dzieci **1.a Opis kategorii danych osobowych** Dane dzieci biorących udział w Uniwersytecie Dziecięcym – imię, nazwisko, wizerunek **2. Cele przetwarzania** Promowanie działalności, budowanie pozytywnego wizerunku Administratora w przestrzeni publicznej **3. Kategorie odbiorców** Nie dotyczy **4. Kategorie odbiorców w państwach trzecich** lub w organizacjach międzynarodowych (i ich nazwy) – nie dotyczy **5. Planowane terminy usunięcia poszczególnych kategorii danych** Po zakończeniu semestru zajęć **6. Opis technicznych i organizacyjnych środków bezpieczeństwa** Stosowane są techniczne i organizacyjne środki mające na celu zapewnienie poufności, integralności, dostępności, obowiązuje Polityka Ochrony Danych Osobowych oraz Instrukcja Zarządzania Systemami informatycznymi – Wykaz zabezpieczeń RODO **7. Podstawa prawna przetwarzania** Art.6, ust 1 lit. a RODO – na podstawie zgody rodzica/opiekuna dziecka, który bierze udział w zajęciach organizowanych w ramach Uniwersytetu Dzieci **8. Konieczność przeprowadzenia oceny skutków dla zbioru:** nie	**1. Informacje (dokumentacja papierowa)** Dane kontaktowe w formie plików na komputerze **2. Programy i systemy operacyjne** Windows, EOD, ESET antivirus, poczta – pwste.edu.pl, **3. Infrastruktura IT** Serwer, macierz dyskowa, NAS, dyski sieciowe, wewnętrzna sieć, router, switche, stacje robocze, **4. Infrastruktura** Pomieszczenia Działu Informatyki, osób biorących udział w programie **5. Pracownicy i współpracownicy** Pracownicy Działu Informatyki, osoby borące udział w programie (pracownicy dydaktyczni) **6. Outsourcing**	1. Fotografowanie dzieci, przeprowadzanie fotoreportaży. 2. Umieszczanie wizerunku dzieci w mediach, materiałach promocyjnych. 3. Usuwanie danych.
1. Opis kategorii osób (nazwa zbioru)	**1. Informacje (dokumentacja papierowa)**	1. Zabezpieczenie informacji

Zbiór informacji niejawnych **1.a Opis kategorii danych osobowych** Dane dotyczące informacji niejawnych, spraw obronnych uczelni **2. Cele przetwarzania** Zabezpieczenie informacji niejawnych uczelni, sprawy obronne **3. Kategorie odbiorców** Nie dotyczy **4. Kategorie odbiorców w państwach trzecich** lub w organizacjach międzynarodowych (i ich nazwy) – nie dotyczy **5. Planowane terminy usunięcia poszczególnych kategorii danych** 10 lat **6. Opis technicznych i organizacyjnych środków bezpieczeństwa** Stosowane są techniczne i organizacyjne środki mające na celu zapewnienie poufności, integralności, dostępności, obowiązuje Polityka Ochrony Danych Osobowych oraz Instrukcja Zarządzania Systemami informatycznymi – Wykaz zabezpieczeń RODO **7. Podstawa prawna przetwarzania** Art.6, ust 1, lit. c RODO wykonanie obowiązku prawnego ciążącego na administratorze (ustawa z 5 sierpnia 2010 r. o ochronie informacji niejawnych) **8. Konieczność przeprowadzenia oceny skutków dla zbioru:** nie	Imię. Nazwisko, wiek, płeć **2. Programy i systemy operacyjne** Windows, EOD, ESET antivirus, poczta – pwste.edu.pl, **3. Infrastruktura IT** Serwer, macierz dyskowa, NAS, dyski sieciowe, wewnętrzna sieć, router, switche, stacje robocze, **4. Infrastruktura** Pomieszczenia Kancelarii Materiałów Niejawnych i Spraw Obronnych, pomieszczenia Archiwum, sekretariatów Kanclerza i Rektora **5. Pracownicy i współpracownicy** Pracownicy Kancelarii Materiałów Niejawnych i Spraw Obronnych, pracownicy Archiwum, Kanclerz **6. Outsourcing**	niejawnych uczelni. 2. Sporządzanie dokumentacji. 3. Przekazywanie uprawnionym organom.
1. Opis kategorii osób (nazwa zbioru) Zbiór danych osób uczestniczących w szkoleniach/kursach/warsztatach organizowanych przez wydziały **1.a Opis kategorii danych osobowych** Dane osobowe, kontaktowe, wizerunkowe, nr konta bankowego w przypadku płatnych szkoleń/kursów/warsztatów **2. Cele przetwarzania** Prowadzenie szkoleń/kursów/warsztatów **3. Kategorie odbiorców** Nie dotyczy **4. Kategorie odbiorców w państwach trzecich** lub w organizacjach międzynarodowych (i ich nazwy) – nie dotyczy **5. Planowane terminy usunięcia poszczególnych kategorii danych** 5 lat **6. Opis technicznych i organizacyjnych środków bezpieczeństwa** Stosowane są techniczne i organizacyjne środki mające na celu zapewnienie poufności, integralności, dostępności, obowiązuje Polityka Ochrony Danych Osobowych oraz Instrukcja Zarządzania Systemami informatycznymi – Wykaz zabezpieczeń RODO **7. Podstawa prawna przetwarzania** Art.6 ust 1 lit. a RODO – zgoda osoby, której dane dotyczą, jako odrębnej zgody na zarejestrowanie w kursie/szkoleniu; na przesyłaniu informacji o kolejnych edycjach; zgody na wykonanie fotografii Art. 6 ust. 1 lit. c RODO – wykonywanie obowiązków ciążących na Administratorze Art. 6 ust. 1 lit. b RODO – wykonywanie umowy **8. Konieczność przeprowadzenia oceny skutków dla zbioru:** nie	**1. Informacje (dokumentacja papierowa)** Imię, nazwisko, dane kontaktowe **2. Programy i systemy operacyjne** Windows, EOD, ESET antivirus, poczta – pwste.edu.pl, Microsoft Teams **3. Infrastruktura IT** Serwer, macierz dyskowa, NAS, dyski sieciowe, wewnętrzna sieć, router, switche, stacje robocze, **4. Infrastruktura** Pomieszczenia instytutów **5. Pracownicy i współpracownicy** Pracownicy instytutów prowadzących kursy/szkolenia/warsztaty, koordynatorzy, organizatorzy kursów/szkoleń/warsztatów **6. Outsourcing**	1. Zbieranie wniosków 2. Sporządzanie dokumentacji. 3. Wydawanie zaświadczeń o odbyciu kursu/szkolenia/warsztatów. 4. wykonywanie fotografii. 5. Przesyłanie informacji o kolejnych edycjach kursów/szkoleń/ 5. Usuwanie danych.
1. Opis kategorii osób (nazwa zbioru) Osoby korzystające z pokojów hotelowych Uczelni **1.a Opis kategorii danych osobowych** Dane osób korzystających z pokojów hotelowych m.in. imię, nazwisko, adres zamieszkania, nr konta bankowego **2. Cele przetwarzania** Wynajem pokojów gościnnych **3. Kategorie odbiorców** Nie dotyczy **4. Kategorie odbiorców w państwach trzecich** lub w organizacjach międzynarodowych (i ich nazwy) – nie dotyczy **5. Planowane terminy usunięcia poszczególnych kategorii danych** 5 lat	**1. Informacje (dokumentacja papierowa)** Imię, nazwisko, adres zamieszkania, nr konta bankowego **2. Programy i systemy operacyjne** Windows, EOD, ESET antivirus, poczta – pwste.edu.pl, **3. Infrastruktura IT** Serwer, macierz dyskowa, NAS, dyski sieciowe, wewnętrzna sieć, router, switche, stacje robocze, **4. Infrastruktura** Pomieszczenia Portierni, Działu Inwestycyjno-Technicznego, Kwestury	1. Meldowanie osób korzystających z pokojów, sporządzanie umów. 2. Pobieranie opłat od osób korzystających z pokojów hotelowych. 3. Prowadzenie ewidencji korzystających z pokojów w formie książki meldunkowej. 4. Wykonywanie obowiązków finansowych. 5. Usuwanie danych.

6. Opis technicznych i organizacyjnych środków bezpieczeństwa Stosowane są techniczne i organizacyjne środki mające na celu zapewnienie poufności, integralności, dostępności, obowiązuje Polityka Ochrony Danych Osobowych oraz Instrukcja Zarządzania Systemami informatycznymi – Wykaz zabezpieczeń RODO **7. Podstawa prawna przetwarzania** Art.6 ust 1 lit. a RODO – zgoda osoby, której dane dotyczą jako odrębnej zgody Art. 6 ust. 1 lit. b RODO – wykonanie umowy, której stroną jest osoba, której dane dotyczą Art. 6 ust. 1 lit. f RODO – usprawiedliwiony interes Administratora **8. Konieczność przeprowadzenia oceny skutków dla zbioru:** nie	**5. Pracownicy i współpracownicy** Pracownicy Portierni, Działu Inwestycyjno-Technicznego, Kwestury, Kwestor, Kanclerz **6. Outsourcing**	
1. Opis kategorii osób (nazwa zbioru) Rejestr skarg i wniosków **1.a Opis kategorii danych osobowych** Imię, nazwisko, adres zamieszkania, dane kontaktowe **2. Cele przetwarzania** Rozpatrywanie złożonych skarg i wniosków **3. Kategorie odbiorców** Podmioty uprawnione na podstawie przepisów prawa **4. Kategorie odbiorców w państwach trzecich** lub w organizacjach międzynarodowych (i ich nazwy) – nie dotyczy **5. Planowane terminy usunięcia poszczególnych kategorii danych** Zgodnie z przepisami prawa **6. Opis technicznych i organizacyjnych środków bezpieczeństwa** Stosowane są techniczne i organizacyjne środki mające na celu zapewnienie poufności, integralności, dostępności, obowiązuje Polityka Ochrony Danych Osobowych oraz Instrukcja Zarządzania Systemami informatycznymi – Wykaz zabezpieczeń RODO **7. Podstawa prawna przetwarzania** Art.6 ust 1 lit. c RODO – wypełnienie obowiązku prawnego ciążącego na Administratorze **8. Konieczność przeprowadzenia oceny skutków dla zbioru:** nie	**1. Informacje (dokumentacja papierowa)** Imię, nazwisko, adres zamieszkania, dane kontaktowe **2. Programy i systemy operacyjne** Windows, EOD, ESET antivirus, poczta – pwste.edu.pl, **3. Infrastruktura IT** Serwer, macierz dyskowa, NAS, dyski sieciowe, wewnętrzna sieć, router, switche, stacje robocze, **4. Infrastruktura** Pomieszczenia Działu Informatyki, sekretariaty, pomieszczenia Kanclerza, dyrektorów, prorektorów **5. Pracownicy i współpracownicy** Pracownicy sekretariatów, Kanclerz, Prorektorzy, dyrektorzy **6. Outsourcing**	1. Przyjmowanie skarg i wniosków. 2. Przekazywanie według kompetencji. 3. Rozpatrywanie skarg i wniosków. 4. Archiwizowanie. 5. Usuwanie danych.
1. Opis kategorii osób (nazwa zbioru) Rejestr wniosków o udostępnienie informacji publicznej **1.a Opis kategorii danych osobowych** Imię, nazwisko, adres zamieszkania, dane kontaktowe **2. Cele przetwarzania** Rozpatrywanie wniosków o udostępnienie informacji publicznej **3. Kategorie odbiorców** Podmioty uprawnione na podstawie przepisów prawa **4. Kategorie odbiorców w państwach trzecich** lub w organizacjach międzynarodowych (i ich nazwy) – nie dotyczy **5. Planowane terminy usunięcia poszczególnych kategorii danych** Zgodnie z przepisami prawa **6. Opis technicznych i organizacyjnych środków bezpieczeństwa** Stosowane są techniczne i organizacyjne środki mające na celu zapewnienie poufności, integralności, dostępności, obowiązuje Polityka Ochrony Danych Osobowych oraz Instrukcja Zarządzania Systemami informatycznymi – Wykaz zabezpieczeń RODO **7. Podstawa prawna przetwarzania** Art.6 ust 1 lit. c RODO – wypełnienie obowiązku prawnego ciążącego na Administratorze (m.in. ustawa z 06.09.2001 r. – o dostępie do informacji publicznej) **8. Konieczność przeprowadzenia oceny skutków dla zbioru:** nie	**1. Informacje (dokumentacja papierowa)** Imię, nazwisko, adres zamieszkania, dane kontaktowe **2. Programy i systemy operacyjne** Windows, EOD, ESET antivirus, poczta – pwste.edu.pl, **3. Infrastruktura IT** Serwer, macierz dyskowa, NAS, dyski sieciowe, wewnętrzna sieć, router, switche, stacje robocze, **4. Infrastruktura** Pomieszczenia Działu Informatyki, sekretariaty, pomieszczenia Kanclerza, dziekanów, prorektorów **5. Pracownicy i współpracownicy** Pracownicy sekretariatów, Kanclerz, Prorektorzy, dziekani **6. Outsourcing**	1. Przyjmowanie wniosków. 2. Przekazywanie według kompetencji. 3. Rozpatrywanie wniosków. 4. Usuwanie.
1. Opis kategorii osób (nazwa zbioru) Rejestr legitymacji pracowniczych **1.a Opis kategorii danych osobowych** Imię, nazwisko, zdjęcie pracownika (wizerunek) **2. Cele przetwarzania**	**1. Informacje (dokumentacja papierowa)** Imię, nazwisko, PESEL, zdjęcie osoby **2. Programy i systemy operacyjne** Windows, EOD, ESET antivirus, poczta – pwste.edu.pl, USOS, AccoNet	1. Wydawanie legitymacji pracowniczych na wniosek pracownika. 2. Nadawanie uprawnień do obsługi ksero, zasobów

Wydawanie legitymacji pracowniczych umożliwiających korzystanie z urządzeń wielofunkcyjnych, wjazd na teren uczelni, umożliwienie z korzystania depozytora kluczy, zbiorów bibliotecznych **3. Kategorie odbiorców** Podmioty uprawnione na podstawie przepisów prawa **4. Kategorie odbiorców w państwach trzecich** lub w organizacjach międzynarodowych (i ich nazwy) – nie dotyczy **5. Planowane terminy usunięcia poszczególnych kategorii danych** Zgodnie z przepisami prawa **6. Opis technicznych i organizacyjnych środków bezpieczeństwa** Stosowane są techniczne i organizacyjne środki mające na celu zapewnienie poufności, integralności, dostępności, obowiązuje Polityka Ochrony Danych Osobowych oraz Instrukcja Zarządzania Systemami informatycznymi – Wykaz zabezpieczeń RODO **7. Podstawa prawna przetwarzania** Art.6 ust 1 lit. a RODO – przetwarzanie na podstawie zgody, jako odrębnej zgody na przetwarzanie wizerunku w celu wyrobienie legitymacji pracowniczej art. 6 ust. 1 lit. f RODO – przetwarzanie w ramach usprawiedliwionego interesu Administratora **8. Konieczność przeprowadzenia oceny skutków dla zbioru:** nie	**3. Infrastruktura IT** Serwer, macierz dyskowa, NAS, dyski sieciowe, wewnętrzna sieć, router, switche, stacje robocze, **4. Infrastruktura** Pomieszczenia Działu Informatyki, Działu Spraw Pracowniczych, Działu Automatyki i Telekomunikacji, Biblioteki, Działu Obsługi Studentów **5. Pracownicy i współpracownicy** Pracownicy Działu Spraw Pracowniczych, Działu Informatyki, Działu Automatyki i Telekomunikacji, Działu Obsługi Studentów **6. Outsourcing**	bibliotecznych, szlabanu na teren Uczelni. 3. Rejestr wydanych legitymacji. 4. Usuwanie danych.
1. Opis kategorii osób (nazwa zbioru) Rejestr kart dostępu dla osób korzystających z infrastruktury uczelni oraz wykonawców umów cywilnoprawnych **1.a Opis kategorii danych osobowych** Imię, nazwisko, numer konta bankowego w przypadku opłat dokonywanych online **2. Cele przetwarzania** Wydawanie kart dostępu (kart wjazdowych) dla korzystających z infrastruktury uczelni **3. Kategorie odbiorców** Podmioty uprawnione na podstawie przepisów prawa **4. Kategorie odbiorców w państwach trzecich** lub w organizacjach międzynarodowych (i ich nazwy) – nie dotyczy **5. Planowane terminy usunięcia poszczególnych kategorii danych** Zgodnie z przepisami prawa **6. Opis technicznych i organizacyjnych środków bezpieczeństwa** Stosowane są techniczne i organizacyjne środki mające na celu zapewnienie poufności, integralności, dostępności, obowiązuje Polityka Ochrony Danych Osobowych oraz Instrukcja Zarządzania Systemami informatycznymi – Wykaz zabezpieczeń RODO **7. Podstawa prawna przetwarzania** Art.6 ust 1 lit. a RODO – przetwarzanie na podstawie zgody, jako odrębnej zgody na przetwarzanie wizerunku w celu wyrobienie legitymacji pracowniczej art. 6 ust. 1 lit. f RODO – przetwarzanie w ramach usprawiedliwionego interesu Administratora **8. Konieczność przeprowadzenia oceny skutków dla zbioru:** nie	**1. Informacje (dokumentacja papierowa)** Imię, nazwisko, numer konta bankowego **2. Programy i systemy operacyjne** Windows, EOD, ESET antivirus, poczta – pwste.edu.pl, aplikacja Call Ex, AccoNet **3. Infrastruktura IT** Serwer, macierz dyskowa, NAS, dyski sieciowe, wewnętrzna sieć, router, switche, stacje robocze, **4. Infrastruktura** Pomieszczenia Działu Informatyki, pokój Kanclerza, Działu Automatyki i Telekomunikacji **5. Pracownicy i współpracownicy** Kanclerz, Pracownicy Działu Automatyki i Telekomunikacji, Działu Informatyki **6. Outsourcing**	1. Przyjmowanie wniosków o wydanie kart dostępu oraz opłat. 2. Wydawanie kart dostępu. 3. Rejestr wydawanych kart dostępu. 4. Usuwanie nieaktywnych kart.
1. Opis kategorii osób (nazwa zbioru) Członkowie Rady Uczelni **1.a Opis kategorii danych osobowych** Imię, nazwisko, numer konta bankowego, dane niezbędne do zgłoszenia do ZUS, numer telefonu, adres e-mail, oświadczenia lustracyjne **2. Cele przetwarzania** Powołanie i funkcjonowanie Rady Uczelni **3. Kategorie odbiorców** Podmioty uprawnione na podstawie przepisów prawa **4. Kategorie odbiorców w państwach trzecich** lub w organizacjach międzynarodowych (i ich nazwy) – nie dotyczy **5. Planowane terminy usunięcia poszczególnych kategorii danych** Zgodnie z przepisami prawa	**1. Informacje (dokumentacja papierowa)** Imię, nazwisko, numer konta bankowego, dane niezbędne do zgłoszenia do ZUS, numer telefonu, adres e-mail, Simple ERP **2. Programy i systemy operacyjne** Windows, EOD, ESET antivirus, poczta – pwste.edu.pl, Microsoft Teams **3. Infrastruktura IT** Serwer, macierz dyskowa, NAS, dyski sieciowe, wewnętrzna sieć, router, switche, stacje robocze, **4. Infrastruktura** Pomieszczenia Działu Spraw Pracowniczych,	1. Sporządzania dokumentacji. 2. Wypłata wynagrodzenia. 3. Archiwizowanie.

6. Opis technicznych i organizacyjnych środków bezpieczeństwa Stosowane są techniczne i organizacyjne środki mające na celu zapewnienie poufności, integralności, dostępności, obowiązuje Polityka Ochrony Danych Osobowych oraz Instrukcja Zarządzania Systemami informatycznymi – Wykaz zabezpieczeń RODO **7. Podstawa prawna przetwarzania** Art.6 ust 1 lit. c RODO – wypełnienie obowiązków prawnych ciążących na Administratorze **8. Konieczność przeprowadzenia oceny skutków dla zbioru:** nie	Kwestury **5. Pracownicy i współpracownicy** Pracownicy Działu Spraw Pracowniczych, Kwestury, Kwestor **6. Outsourcing**	
1. Opis kategorii osób (nazwa zbioru) Studenci biorący udział w programie Legia Akademicka **1.a Opis kategorii danych osobowych** Imię, nazwisko, imię ojca, data i miejsce urodzenia, PESEL, adres pobytu stałego, adres do korespondencji, telefon kontaktowy, nazwa uczelni, kierunek studiów, aktualny rok studiów, planowany rok ukończenia studiów, kategoria zdolności do czynnej służby wojskowej, informacja o karalności za przestępstwo umyślne, numer albumu **2. Cele przetwarzania** Realizacja programu Legia Akademicka, dokonanie zgłoszenia do odbycia przeszkolenia wojskowego **3. Kategorie odbiorców** Podmioty uprawnione na podstawie przepisów prawa **4. Kategorie odbiorców w państwach trzecich** lub w organizacjach międzynarodowych (i ich nazwy) – nie dotyczy **5. Planowane terminy usunięcia poszczególnych kategorii danych** Zgodnie z przepisami prawa **6. Opis technicznych i organizacyjnych środków bezpieczeństwa** Stosowane są techniczne i organizacyjne środki mające na celu zapewnienie poufności, integralności, dostępności, obowiązuje Polityka Ochrony Danych Osobowych oraz Instrukcja Zarządzania Systemami informatycznymi – Wykaz zabezpieczeń RODO **7. Podstawa prawna przetwarzania** Art.6 ust 1 lit. a RODO –zgoda osoby, której dane dotyczą, art. 6 ust. 1 lit. c RODO - wypełnienie obowiązku prawnego, *art. 6 ust. 1 lit. e RODO – wykonanie zadania realizowanego w intersie publicznym* **8. Konieczność przeprowadzenia oceny skutków dla zbioru:** nie	**1. Informacje (dokumentacja papierowa)** Imię, nazwisko, imię ojca, data i miejsce urodzenia, PESEL, adres pobytu stałego, adres do korespondencji, telefon kontaktowy, nazwa uczelni, kierunek studiów, aktualny rok studiów, planowany rok ukończenia studiów, kategoria zdolności do czynnej służby wojskowej, informacja o karalności za przestępstwo umyślne, numer albumu **2. Programy i systemy operacyjne** Windows, EOD, ESET antivirus, poczta – pwste.edu.pl, **3. Infrastruktura IT** Serwer, macierz dyskowa, NAS, dyski sieciowe, wewnętrzna sieć, router, switche, stacje robocze, **4. Infrastruktura** Pomieszczenia sekretariatu Wydziału Ekonomii i Zarządzania, sekretariat Prorektora **5. Pracownicy i współpracownicy** Pracownicy Wydziału Ekonomii i Zarządzania, Prorektor ds. studenckich , pracownicy sekretariatu prorektora, koordynator programu **6. Outsourcing**	1. Zbieranie wniosków studentów. 2. Przekazywanie wniosków do odpowiedniego WSZW oraz podmiotów uprawnionych. 3. Prowadzenie dokumentacji. 4. Archiwizowanie danych.
1. Opis kategorii osób (nazwa zbioru) Osoby korzystające z Podkarpackiego Centrum Badań, Diagnozy i Terapii PANS w Jarosławiu **1.a Opis kategorii danych osobowych** Imię, nazwisko, wiek, dane kontaktowe **2. Cele przetwarzania** Udzielanie wsparcia i pomocy psychologicznej **3. Kategorie odbiorców** Podmioty uprawnione na podstawie przepisów prawa **4. Kategorie odbiorców w państwach trzecich** lub w organizacjach międzynarodowych (i ich nazwy) – nie dotyczy **5. Planowane terminy usunięcia poszczególnych kategorii danych** Po rozpoznaniu i zdiagnozowaniu problemu **6. Opis technicznych i organizacyjnych środków bezpieczeństwa** Stosowane są techniczne i organizacyjne środki mające na celu zapewnienie poufności, integralności, dostępności, obowiązuje Polityka Ochrony Danych Osobowych oraz Instrukcja Zarządzania Systemami informatycznymi – Wykaz zabezpieczeń RODO **7. Podstawa prawna przetwarzania** Art.6 ust 1 lit. a RODO –zgoda osoby, której dane dotyczą **8. Konieczność przeprowadzenia oceny skutków dla zbioru:** nie	**1. Informacje (dokumentacja papierowa)** Imię, nazwisko, dane kontaktowe **2. Programy i systemy operacyjne** Windows, EOD, ESET antivirus, poczta – pwste.edu.pl, **3. Infrastruktura IT** Serwer, macierz dyskowa, NAS, dyski sieciowe, wewnętrzna sieć, router, switche, stacje robocze, **4. Infrastruktura** Pomieszczenia Instytutu Humanistycznego **5. Pracownicy i współpracownicy** Pracownicy Instytutu Humanistycznego, Koordynator Centrum **6. Outsourcing**	1. Prowadzenie zbioru danych kontaktowych z korzystających z PCBDiT. 2. Konsultacja psychologiczna. 3. Usuwanie danych.

Załącznik nr 2 do Polityki Ochrony Danych
PANS w Jarosławiu

L.p.	Imię i nazwisko	Stanowisko/komórka organizacyjna	Nazwa zbioru	Zakres	Data nadania upoważnienia	Data ustania upoważnienia
1.						
2.						
3.						
4.						
5.						

Arkusz analizy ryzyka

P-Prawdopodobieństwo incydentu (skala od 1 do 3), S-Skutki wystąpienia incydentu (skala od 1 do 3), R-Ryzyko wystąpienia incydentu (skala od 1 do 9), Formuła: R=P*S

Zagrożenie	Opis zagrożenia	P	S	R	Zabezpieczenie
Phishing, cybersquatting (podrabianie stron)	• Mail z prośbą o zalogowanie się (pod pretekstem weryfikacji danych lub informowanie o próbie włamania na konto) do „podróbki" strony, np. bankowej, lub pseudo konta gmail i w rezultacie przejęcie hasła. • Zachęcanie do zalogowania się do podrobionej strony o „wiarygodnym" adresie www. Zamiast logować się do www.mbank.pl logowanie byłoby w www.rnbank.pl	3	3	9	**Procedura:** • Szkolenia personelu • Regulamin ODO **Zabezpieczenie:** • Systemy antywirusowy i antyspamowy • Sewery proxy i bramki filtrujące • Modyfiakacje reguł filtrowanie treści wiadomości pocztowej, by blokować znane frazy • Blokowanie adresów poczty
Nakłanianie do wykonania czynności	• Mail z dyspozycją podjęcia określonej czynności • Fax/mail z fakturą od rzekomego „dostawcy" z informacją o zmianie numeru konta bankowego do opłacenia faktur	2	3	6	**Procedura:** • Szkolenia personelu • Regulamin ODO • Wewnętrzny regulamin działu księgowego dotyczący zasad akceptacji i modyfikacji przelewów
Instalacja szkodliwego oprogramowania / działanie szkodliwego oprogramowania	Szkodliwe oprogramowanie (backdoory, exploity, exploitpaki, keyloggery). *Najczęściej instalowane są poprzez otwarcie „zainfekowanego" załącznika z maila lub poprzez kliknięcie na zarażoną stronę. Maile takie zachęcają do otwarcia załącznika lub kliknięcia na hiperlink. W efekcie możemy zarazić nasz komputer lub wiele komputerów w sieci* *Działające szkodliwe oprogramowanie może wywołać różnorodne skutki:* • *Przejęcie konta pocztowego do wysyłki spamu* • *Użycie przejętych komputerów do kopania kryptowalut* • *Użycie przejętych komputerów do ataków DOS* • *Użycie przejętych komputerów do śledzenia haseł użytkowników celem uzyskania dostępu do systemów i plików* • *Użycie przejętych komputerów do uzyskania pełnego dostępu do wewnętrznej sieci i kopiowania danych i baz danych (kradzież)*	2	3	6	**Procedura:** • Szkolenia personelu • Regulamin ODO **Zabezpieczenie:** • Systemy antywirusowy i antyspamowy • Sewery proxy i bramki filtrujące

	Szkodliwe oprogramowanie: *Wirusy i trojany – instalują się często z nielegalnym oprogramowaniem. Zawierają ukrytą funkcjonalność, działają na szkodę użytkownika.* *Backdoory - Instalują się z maili lub z hiperlinków w mailach. Po uruchomieniu umożliwiają intruzowi ponowny dostęp i stałą kontrolę nad komputerem. Taki komputer-zombie może być użyty do wszelkich zachcianek intruza.* *Keyloggery - Programy przechwytujące hasła wpisywane na klawiaturze przez użytkownika i oddające je intruzowi.* *Exploity / exploitpaki - Oprogramowanie wykorzystujące znane luki w systemach. Uruchomiony pozwala na przejęcie systemu przez intruza.*				
Podrzucone nośniki danych	Atakujący pozostawia w biurze lub w dziale księgowości specjalnie przygotowany pendrive z zainstalowanym samouruchamiającym się szkodliwym programem. W wielu przypadkach pracownicy sprawdzają jego zawartość wkładając go do portu USB. W wyniku tego uruchamiają nieświadomie szkodliwe oprogramowanie (backdoory, exploity, exploitpaki, keyloggery).	1	3	3	**Procedura:** • Szkolenia personelu • Regulamin ODO **Zabezpieczenie:** • Blokada portów USB na stacjach roboczych • Dopuszczenie do użycia wyłącznie zakwalifikowanych pendrive
Ataki telefoniczne	• Intruz podający się za „naszego informatyka” prosi o podanie hasła pod pretekstem sprawdzania lub naprawy naszego systemu informatycznego • Intruz przedstawia się jako „serwisant Orange lub Netii” naprawiający usterkę i prosi o wejście na określoną stronę internetową w ramach testowania łącza internetowego • Intruz przedstawia się jako inżynier Microsoftu lub programista dostawcy oprogramowania. Podsyła „aktualizację” lub prosi o udostępnienie pulpitu	1	3	3	**Procedura:** • Szkolenia personelu • Regulamin ODO
Łamanie haseł	Łamanie haseł metodami słownikowymi i siłowymi (brute force) : • do baz danych • do serwera • do aplikacji www • do poczty • do windows na stacjach roboczych • do routera • do firewalla	1	2	2	**Procedura:** • Metody i środki uwierzytelnienia (polityka haseł) • Szkolenia personelu **Zabezpieczenia:** • Testy penetracyjne
Łatwo dostępne, łatwe lub standardowe hasła	• Ujawnianie haseł • Nieprawidłowe przechowywanie (karteczki, pliki) • Stosowanie domyślnych haseł producenta	1	3	3	**Procedura:** • Metody i środki uwierzytelnienia (polityka haseł) • Szkolenia personelu **Zabezpieczenia:**

	• Stosowanie słownikowych lub popularnych haseł, np. Grazynka1, qwerty, 12345678
	• Stosowanie jednego hasła do wielu (często wszystkich) systemów
					• długość hasła - 12 znaków
					• mechanizmy blokujące używanie takich haseł w serwisisach do zmiany hasłamechanizm wymuszenia zmiany hasła
					• uwierzytelnianie do
					  ○ aplikacji,
					  ○ stacji roboczych
					  ○ dysku sieciowego
					  ○ sieci
					  ○ poczty
					• Testy penetracyjne

Ataki na sprzęt - Włamania do urządzeń nieaktualizowanych	Ataki na urządzenia sieciowe oraz inne, które działają dzięki umieszczonemu na nich oprogramowaniu (firmware / strowniki) Zagrożenie dla nast. elementów: • routery • switche • access pointy • firewall • macierz • dysk NAS • drukarki i skanery *Brak aktualizacji tego oprogramowania skutkuje podatnością na włamania, kradzież danych, zakłócanie pracy.*	2	1	2	**Procedura:** • Procedura zabezpieczenia systemu informatycznego **Zabezpieczenia:** • Testy penetracyjne • Sondy IPS/IDS
Ataki na sprzęt - Włamania do urządzeń nieodpowiednio skonfigurowanych	Ataki na błędnie skonfigurowany sprzęt lub sprzęt działający z ustawieniami fabrycznymi. Zagrożenie dla nast. elementów: • routery • switche • access pointy • firewall • macierz • dyski NAS • drukarki i skanery *Błędy konfiguracyjne popełniane przez administratorów mogą ułatwiać hackerom włamanie się do sieci lub urządzenia. Powodem jest najczęściej brak profesjonalnej wiedzy u osób konfigurujących urządzenia. Przykładem jest np. pozostawienie domyślnych haseł lub dostępu do strony konfiguracyjnej routera z poziomu Internetu.*	1	2	2	**Procedura:** • Procedura zabezpieczenia systemu informatycznego **Zabezpieczenia:** • Zmiana domyślnych haseł na urządzeniach • Zmiana domyślnej nazwy konta administratora w urządzeniu • Testy penetracyjne
Ataki na sprzęt - Włamania z użyciem	Atakujący wpina się do urządzeń IT przez ich niezabezpieczone porty konfiguracyjne (USB, Ethernet lub COM - szeregowe)	1	3	3	**Procedura:** • Procedura zabezpieczenia systemu informatycznego

niezabezpieczonych interfejsów lokalnych	Zagrożenie dla nast. elementów: • routery • switche • firewalle • macierze • serwery • drukarki i skanery *Administratorzy często pozostawiają te porty niezabezpieczone, co powoduje ryzyko wpięcia się do powyższych urządzeń i ich skonfigurowania przez hakera.*				**Zabezpieczenia:** • Dostęp do portów fizycznych (gniazd - np. szeregowy, USB, Ethernet) zabezpieczono hasłem, aby przypadkowa osoba, która podłączy do nich swój komputer nie mogła zmienić konfiguracji. • Umieszczenie krytycznych elementów infrastruktury w zamykanych na klucz szafach serwerowych • Kontrola dostępu do pomieszczeń serwerowni i punktów dystrybucyjnych sieci • Testy penetracyjne
Ataki na sprzęt - Włamania za pośrednictwem niepotrzebnych usług (np. telnet na routerze)	Atakujący wykorzystuje do włamania usługi sieciowe, których działanie w danym środowisku nie jest wymagane Zagrożenie dla nast. Usług: • DHCP • DNS • SSH • http • telnet • FTP • SMTP • SNMP *Urządzenia sieciowe posiadają często włączone wszystkie możliwe usługi sieciowe (DHCP, DNS, SSH, HTTP, telnet, FTP), mimo iż nie wszystkie z nich są potrzebne w danym środowisku. Każda z tych usług jest obsługiwana przez oprogramowanie, które może zawierać błędy.*	1	3	3	**Procedura:** • Procedura wykonywania przeglądów i konserwacji • Procedura zabezpieczenia systemu informatycznego **Zabezpieczenia:** • Wyłączenie niepotrzebnych serwisów (ogranicza ilość dziur i możliwość przechwycenia / podsłuchania ruchu lub haseł.) • Włączone tylko te usługi, które są niezbędne do działania danego środowiska • Monitorowanie aktywnych usług • Skanery podatności (stosowany jest system wykrywania słabości i zagrożeń) • Security Information and Event Managment (analityczny system do wykrywania zagrożeń • Testy penetracyjne • Udostępnianie na serwerze tylko niezbędnych usług (portów)
Ataki na oprogramowanie - Wykorzystanie znanych dziur w nieaktualizowanym oprogramowaniu	Atak z wykorzystaniem znanych dziur w niezaktualizowanym oprogramowaniu Zagrożenie dla programów • Systemy operacyjne na stacjach roboczych • Systemy serwerowe • Przeglądarki www • Wordpress, Drupal, <inne silniki webowe>, <sklepy internetowe>, • Dedykowany CMS • Adobe • Flash • Java • (podaj inne aplikacje niewymienione) *Istniejące błędy oprogramowania pozwalające na przełamanie zabezpieczeń są upubliczniane po tym, jak producent*	1	3	3	**Procedura:** • Procedura zabezpieczenia systemu informatycznego • Procedura wykonywania przeglądów i konserwacji **Zabezpieczenia:** • Stosowane jest darmowe/komercyjne oprogramowanie do inwentaryzacji zainstalowanego oprogramowania na stacjach roboczych (serwerach) oraz do kontroli procesu aktualizacji (patche / łatki) • Aktualizacja oprogramowania zgodnie z zaleceniami producentów oraz opinią rynkową co do bezpieczeństwa i stabilności nowych wersji (np. aktualizacje, service pack-i, łatki) • Skanery podatności (stosowany jest system wykrywania słabości i zagrożeń) • Security Information and Event Managment (analityczny system do wykrywania zagrożeń) • Sondy IPS/IDS • Testy penetracyjne • Cykliczne aktualizowanie systemów operacyjnych i oprogramowanie

	oprogramowania przygotuje odpowiednią łatę lub aktualizację. Jeżeli nie zainstalujemy tych aktualizacji, narażamy się na atak, np. zdalny dostęp do systemu lub wykonanie złośliwego kodu (instalacja backdoora, exploita, ransomeware)				
Podsłuch	• podsłuch danych przesłanych drogą mailową • podsłuch danych podczas korzystania z aplikacji webowych • podsłuch podczas korzystania z formularzy kontaktowych • podsłuch podczas zdalnego dostępu do sieci wewnętrznej przez Internet	1	3	3	**Procedura:** • Procedura zabezpieczenia systemu informatycznego **Zabezpieczenia:** • szyfrowanie poczty wysyłanej (SSL) • szyfrowanie połączeń internetowych SSL/VPN • szyfrowanie plików (7zip) wysyłanych mailowo • Ograniczenie fizycznego dostępu do miejsc, gdzie znajdują się nienadzorowane gniazdka sieciowe (np. sale konferencyjne, korytarze) • Dezaktywacja nieużywanych gniazd sieciowych przez wypięcie przewodu lub wyłączenie portu na switchu • Testy penetracyjne
Ataki na oprogramowanie - Włamania z wykorzystaniem luk typu zero day	Zero-day to błędy w oprogramowaniu, do których autor nie przygotował jeszcze poprawek / aktualizacji. Informacje o nich są sprzedawane i wykorzystywane przez intruzów.	1	3	3	**Procedura:** • Procedura zabezpieczenia systemu informatycznego **Zabezpieczenia:** • Oprogramowanie antywirusowe • Sondy IPS/IDS • Testy penetracyjne • Systemem klasy EDR (Sentinel)
Ataki na oprogramowanie - Włamania z wykorzystaniem najczęstszych błędów programistycznych	*Programiści pisząc programowanie często popełniają te same, znane błędy.* *Przykładowo: możliwość wpisania ujemnej liczby sztuk w formularzu zamówienia, możliwość odgadnięcia numeru zamówienia innego klienta i wpisanie go w pasku adresu przeglądarki w celu wyświetlenia szczegółów.*	1	3	3	**Procedura:** • Procedura zabezpieczenia systemu informatycznego **Zabezpieczenia:** • Sondy IPS/IDS • Testy penetracyjne
Włamania z wykorzystaniem API (interfejsów programistycznych)	*Niektóre aplikacje pozwalają na zdalne zarządzanie nimi przez specjalnie zaprojektowane funkcje/usługi sieciowe. Np. baza danych może pozwalać na podłączenie się do niej administratorowi w celu wykonania prac naprawczych lub backupu. Dostęp ten odbywa się przy użyciu domyślnych loginów i haseł, co stanowi zagrożenie.*	1	3	3	**Procedura:** • Procedura zabezpieczenia systemu informatycznego **Zabezpieczenia:** • Zmiana domyślnych loginów i haseł • Wyłączenie zdalnego dostępu, gdy nie jest wymagany • Testy penetracyjne
Ataki na oprogramowanie - Namierzanie wersji testowych (np. strona www)	*Niektóre aplikacje posiadają swoje kopie utrzymywane do celów testowych. Są one często gorzej zabezpieczone i łatwiej jest się do nich włamać, a mogą zawierać również krytyczne dane ze środowiska produkcyjnego. Przykładem może być kopia serwera wykonana w celu przetestowania nowej wersji aplikacji. Często udaje się je namierzyć wpisując np. zamiast adresu www.strona.pl adres test.strona.pl .*	2	1	2	**Procedura:** • Procedura zabezpieczenia systemu informatycznego **Zabezpieczenia:** • Zmiana domyślnych loginów i haseł • Stosowanie tych samych zasad bezpieczeństwa, co do systemów produkcyjnych • Testy penetracyjne

Skanowanie sieci i usług	*Udostępniane w Internecie serwery, urządzenia sieciowe i aplikacje oraz serwisy www mogą być namierzane przez intruzów poprzez skanowanie adresów IP. Polega to na próbach łączenia się z wszystkimi znanymi usługami w celu sprawdzenia, które z nich są dostępne w naszej sieci i w jakiej wersji. Dzięki temu możliwe jest znalezienie usług nieaktualnych i zawierających błędy.*	1	2	2	**Procedura:** • Procedura zabezpieczenia systemu informatycznego **Zabezpieczenia:** • Firewalle • Sondy IPS/IDS • Wyłączanie niepotrzebnych usług na urządzeniach sieciowych i serwerach
Włamanie do sieci poprzez WIFI	Uzyskanie dostępu do sieci wewnętrznej poprzez włamanie się do sieci bezprzewodowej	1	2	2	**Z Procedura:** • Procedura zabezpieczenia systemu informatycznego **abezpieczenia:** • Odseparowanie wifi dla gości/klientów od sieci wewnętrznej • Stosowanie odpowiednich standardów szyfrowania • Stosowanie haseł dostępowych

Włamanie z sieci zewnętrznej do sieci wewnętrznej	Włamania z zewnątrz poprzez nieodpowiednio zabezpieczone i skonfigurowane punkty styku z Internetem oraz udostępnione w Internecie serwery i aplikacje.	1	3	3	**Procedura:**
					• Procedura zabezpieczenia systemu informatycznego
					Zabezpieczenia:
					• Sewery proxy i bramki filtrujące
					  o skan niebezpiecznej zawartości
					• Firewall / NG Firewall / UTM do ochrony dostępu do sieci komputerowej
					  o firewall sprzętowy
					  o firewall programowy
					• system IDS/IPS do ochrony dostępu do sieci komputerowej
					• Skanery podatności (stosowany jest system wykrywania słabości i zagrożeń)
					• Testy penetracyjne

Nieuprawniony dostęp do sieci z użyciem hakerskiego urządzenia	Możliwość wpięcia hakerskiego urządzenia do łatwo dostępnych urządzeń sieciowych wewnątrzorganizacyjnych, celem uzyskania dostępu do sieci przez to urządzenie z zewnątrz. Możliwość uruchomienia tzw. wrogiego access pointa w celu przechwycenia klientów sieci bezprzewodowej. Zagrożenie dla nast. elementów: • gniazdka sieciowe w korytarzach, w sali konferencyjnej • skanery, drukarki na korytarzach • switche w miejscach dostępnych	1	3	3	**Procedura:** • Procedura zabezpieczenia systemu informatycznego **Zabezpieczenia:** • Okablowanie i elementy sieci są fizycznie zabezpieczone przed ingerencją osób postronnych • Blokada portów USB na stacjach roboczych • Dezaktywacja nieużywanych gniazd sieciowych poprzez wypięcie przewodu lub wyłączenie portu na switchu
Atak ransomeware	Ransomeware - Program do szyfrowania plików. Instaluje się z maili lub z hiperlinków w mailach lub poprzez odwiedziny zainfekowanej strony. Są też znane przypadki infekcji poprzez sieć lokalną. Odszyfrowanie wymaga zapłaty np. 500 USD. Bardzo groźny	3	3	9	**Procedura:** • Procedura zabezpieczenia systemu informatycznego • Procedura tworzenia kopii zapasowych • **Procedura:** • Szkolenia personelu • Regulamin ODO **Zabezpieczenia:** • Systemy antywirusowy i antyspamowy

					• Kopie bezpieczeństwa kluczowych danych zabezpieczone przed szyfrowaniem przez ransomeware
					• Sewery proxy i bramki filtrujące
					  o blokada ruchu na podstawie bazy reputacji
					  o blokada dostępu do określonych stron

ATAKI MAN-IN-THE-MIDDLE	Zmuszenie komputerów w sieci lokalnej do komunikowania się za pośrednictwem komputera intruza. Umożliwia przechwytywanie i podsłuchiwanie ruchu w sieci.	1	3	3	**Procedura:** • Procedura zabezpieczenia systemu informatycznego **Zabezpieczenia:** • Systemy antywirusowe • Sondy IPS/IDS • Systemy SIEM • Testy penetracyjne
Eskalacja uprawnień	• Zwiększenie uprawnień użytkownika przez wykorzystanie błędów programistycznych • Przejęcie uprawnień użytkownika zaawansowanego • Przejęcie uprawnień administratora • Przejęcie uprawnień systemowych • Przejęcie innych poświadczeń (certyfikaty elektroniczne, pliki cookies z identyfikatorami sesji)	2	2	4	**Procedura:** • Procedura nadawania uprawnień do przetwarzania danych osobowych • Procedura wykonywania przeglądów i konserwacji **Zabezpieczenia:** • Systemy SIEM • Regularny przegląd logów i uprawnień • Monitorowanie logowania na konta administracyjne • Testy penetracyjne
Atak DOS / DDOS	Atak na system komputerowy lub usługę sieciową w celu uniemożliwienia działania. Atak dotyczy głownie stron i aplikacji www. Np. wypełnienie i wysłanie kilka milionów razy formularza kontaktowego (za pomocą skryptu) i spowodowanie zapełnienia dysku. *Zmasowany atak pojedynczego atakującego (DOS) lub z wielu komputerów jednocześnie (DDOS) na jakąś stronę www lub na portal, aby ją przeciążyć i „zakorkować”*	3	2	6	**Procedura:** • Procedura zabezpieczenia systemu informatycznego **Zabezpieczenia:** • WAF (Web application firewall) • Firewall • Mechanizm captcha (kod z obrazka do przepisania w formularzu) • Systemy SIEM • Testy penetracyjne
Nieuprawniony dostęp lub włamanie do pomieszczeń	Dostęp do: • Budynków • Pomieszczeń biurowych • Archiwów • Serwerowni • Miejsc przechowywania kopii bezpieczeństwa Może skutkować: • dostępem do danych w wersji papierowej • dostępem do plików lub aplikacji lub baz danych • zainstalowaniem nieautoryzowanych urządzeń do dostępu do sieci wewnętrznej • kradzieżą komputerów, nośników	1	3	3	**Procedury:** • Polityka kluczy • Polityka kontroli dostępu **Zabezpieczenia:** • kontrola kluczy zapasowych / kontrola wydawania kluczy • portiernia • proceduralne ograniczenie dostępu do pomieszczeń osobom nieupoważnionym • praca personelu sprzątającego w godzinach pracy i w obecności osób upoważnionych • rozmieszczenie komputerów /drukarek /xero ograniczające dostęp osób nieupoważnionych • dostęp osób nieupoważnionych w obecności osoby upoważnionej • zabezpieczenie dostępu do pomieszczeń zamek elektroniczny z SKD

					• zabezpieczenie dostępu do serwerowni -System Kontroli dostępu i przeciwwłamaniowy • zabezpieczenie dostępu do archiwum (drzwi zamykane na klucz) • zabezpieczenie dokumentacji / danych w pomieszczeniach (/ zamknięte metalowe szafy) • ochrona fizyczna obiektu / pomieszczeń (ochrona własna) • system kontroli dostępu • monitoring wizyjny w obrębie obiektu i otoczeniu
Kradzież / zagubienie sprzętu i nośników poza organizacją	Kradzież / zagubienie: • laptopów • smartfonów, • pendrive • dysków wymiennych	3	2	6	**Procedury:** • Regulamin użytkowania komputerów przenośnych • Procedura zabezpieczenia systemu informatycznego
Nieuprawniony dostęp do infrastruktury IT oraz do programów	• brak kontroli nad dostępem do serwera, plików, programów, komputerów • nadane zbyt wysokie uprawnienia użytkownikom • dostęp osób nieupoważnionych do kopii bezpieczeństwa • łatwy dostęp osób nieupoważnionych do danych prezentowanych na monitorach, drukarkach, kserokopiarkach • niezabezpieczona praca zdalna użytkowników lub serwisu IT	1	3	3	**Procedury:** • Procedura nadawania uprawnień do przetwarzania danych osobowych • Procedura zabezpieczenia systemu informatycznego • Procedura wykonywania przeglądów i konserwacji **Zabezpieczenia:** • szyfrowanie baz danych, aby hacker lub przypadkowy użytkownik nie „widział" danych w bazie • zarządzanie uprawnieniami – profile użytkowników • minimalizacja uprawnień • konta firmowe odseparowane od prywatnych • separacja sieci wewnętrznej od sieci przeznaczonej dla gości • uwierzytelnianie użytkowników z zewnątrz poprzez akceptację wybranych adresów IP • blokada logowania się po kilku błędnie podanych hasłach **Procedury:** • Procedura nadawania uprawnień do przetwarzania danych osobowych • Procedura zabezpieczenia systemu informatycznego • Procedura wykonywania przeglądów i konserwacji • Szkolenia personelu • Regulamin ODO **Zabezpieczenia:** • oświadczenia poufności • zahasłowane wygaszacze ekranu aktywowane po XX minutach nieaktywności użytkownika • ustawienie monitorów uniemożliwiające wgląd w dane osób postronnych • polityka czystego ekranu • filtry polaryzacyjne na monitorach • drukarki wyposażone w kontrolę wydruków (PIN)

Udostępnianie danych osobom nieupoważnionym z sieci publicznej (przez internet)	• dostęp do danych osobowych poprzez stronę www bez logowania się • dostęp do danych osobowych poprzez stronę www po zalogowaniu się (użytkownik może przeglądać dane osobowe innych użytkowników) • dostęp do katalogów udostępnionych pod publicznym adresem IP plików z danymi osobowymi lub kopii bezpieczeństwa (bez logowania się) • udostępnianie plików zaindeksowanych przez roboty google na skutek braku komend chroniących katalogi webowe przez taką indeksacją • przesłanie lub wydawanie informacji osobie nieupoważnionej	1	3	3	**Procedura** • Procedura wykonywania przeglądów i konserwacji • Regulamin ODO **Zabezpieczenia** • Uwierzytelnianie dostępu do zasobów • Testy penetracyjne • Blokada robotów • Systemy DLP (data leak/loss prevention/protection)
Awarie / uszkodzenia elementów IT	Awarie: • dysków • stacji roboczych • urządzeń sieciowych/routerów • drukarek / skanerów • serwera	1	3	3	**Procedury:** • Procedura wykonywania przeglądów i konserwacji **Zabezpieczenia:** • redundancja serwera • macierz IBM5030 w trybie miroringu • system do inwentaryzacji sprzętu • plan ciągłości działania
Błąd / awaria oprogramowania	Awarie: • programu kadrowo-płacowego • poczty • aplikacji www (np. wordpressa) • bazy danych	3	2	6	**Procedury:** • Procedura wykonywania przeglądów i konserwacji **Procedury:** • Zabezpieczenia techniczne **Zabezpieczenia:** • Wirtualizacja
Pożar / eksplozja	• Pożar obiektu • Pożar serwerowni • Pożar serwera • Zniszczenie serwerowni (np. wybuch gazów technicznych)	1	3	3	**Procedury:** • Zabezpieczenia techniczne **Zabezpieczenia:** • gaśnice • system PPOŻ • czujnik dymu w serwerowni • system automatycznego gaszenia serwerowni gazami technicznymi

Zalanie	• Zalanie serwerowni • Zalanie archiwum (powódź, zalanie z rur) • Zalanie pomieszczenia kadr	1	1	1	**Procedury:** • Zabezpieczenia techniczne **Zabezpieczenia:** • składowanie dokumentacji papierowej na podwyższeniu, w szafach metalowych
Przegrzanie / zbyt duża wilgotność	• wysoka temperatura w serwerowni • wysoka wilgotność w archiwum	1	1	1	**Procedury:** • Zabezpieczenia techniczne **Zabezpieczenia:** • klimatyzacja w serwerowni • powiadamianie administratora systemu informatycznego o alertach temperatury • monitoring środowiskowy w serwerowni - czujnik temperaturowy • monitoring środowiskowy w archiwum - czujniki wilgotności
Awaria zasilania	• skoki napięcia • przerwy w dostawie zasilania	1	1	1	**Procedury:** • Zabezpieczenia techniczne **Zabezpieczenia:** • sieć stabilizowana • UPS podtrzymujący zasilanie serwera • UPS na kluczowych elementów systemu IT • •
Nieuprawniona modyfikacja / usunięcie	• niezamierzone lub pomyłkowe zmodyfikowanie / usunięcie danych • sfałszowanie danych przez osoby z wewnątrz lub zewnątrz organizacji	2	3	6	**Procedury:** • Procedura zabezpieczenia systemu informatycznego **Zabezpieczenia:** • Rozliczalność operacji o kluczowe programy/systemy logują operacje tworzenia, zmiany, usuwania rekordu, wglądu w dane, eksportu danych o każdy użytkownik programu/systemu posiada swój indywidualny login
Nieuprawnione kopiowanie danych	• kopiowanie danych z katalogów, dysków, baz, programów • kserowanie i robienie zdjęć przez pracownika lub przez osobę obcą	3	3	9	**Procedury:** • Procedura zabezpieczenia systemu informatycznego • Regulamin ODO

					Zabezpieczenia:
					• Rozliczalność operacji
					  ○ kluczowe programy/systemy logują operacje tworzenia, zmiany, usuwania rekordu, wglądu w dane, eksportu danych
					  ○ każdy użytkownik programu/systemu posiada swój indywidualny login

Brak / błędy w wykonywaniu kopii bezpieczeństwa	• doraźne lub za rzadkie wykonywanie kopii • błędy podczas procesu wykonywania kopi • niemożność odtworzenia kopii ze względu na zmiany w oprogramowaniu	2	2	4	**Procedury:** • Procedura tworzenia kopii zapasowych **Zabezpieczenia:** • Wirtualizacja kopii • wykonywany jest backup serwerów / aplikacji / plików / konfiguracji / licencji /haseł • backup jest zabezpieczony przed ransomeware • kopie zapasowe przechowywane są poza serwerownią • testowanie możliwości odtworzenia kopii • niszczenie/czyszczenie nośników przed utylizacją
Nieprawidłowe / brak procedur niszczenia nośników z danymi –	• wyrzucenie uszkodzonych nośników bez ich zniszczenia • wyrzucanie dokumentów papierowych na śmietnik lub pozostawienie dokumentów w miejscu publicznym • wyrzucenie niezniszczonych , HD, pendrive, DVD	1	3	3	**Procedury:** • Utylizacja elektronicznych nośników i wydruków oraz czyszczenie danych **Zabezpieczenia:** • niszczenie/czyszczenie nośników przed utylizacją • fizyczne niszczenie sprzętu
Nieprawidłowe / brak procedur napraw w serwisach zewnętrznych	• naprawa sprzętu z nośnikami bez umowy lub bez standardu bezpiecznej naprawy	1	1	1	**Procedury:** • Procedura wykonywania przeglądów i konserwacji
Nieprzestrzeganie procedur	• świadome naruszenie pisemnych lub ustnych procedur np. niewylogowywanie się z systemu, przekazywanie haseł osobom nieupoważnionym, naruszenie polityki czystego ekranu lub czystego biurka • naruszenia powyżej wskazane na skutek braków w inteligencji lub z powodów niewiedzy	2	2	4	**Procedury:** • Szkolenia personelu • Regulamin ODO
Pomyłki i błędy administratorów, użytkowników	• udostępnienia katalogów i dysków, serwerów ftp, aplikacji z danymi do powszechnego dostępu przez sieć publiczną –z powodu „ułatwienia pracy” administratorów systemów • łatwe logowanie się do baz i programów „login admin, hasło admin1”	1	3	3	**Procedury:** • Procedura zabezpieczenia systemu informatycznego • Szkolenia personelu • Regulamin ODO

	• dostęp do programów testowych (z prawdziwymi danymi osobowymi) bez logowania • pomyłkowe udostępnienie, wysłanie do złego odbiorcy, błędne zabezpieczenia				
Błędy projektowe / konfiguracyjne	• błędy programistów prowadzące do udostępniania danych z tworzonych lub administrowanych programów • niezabezpieczenie danych w katalogach i bazach webowych i przed indeksacją robotów google	2	2	4	**Zabezpieczenie** • Procedura zabezpieczenia systemu informatycznego • Zabezpieczenie baz i katalogów webowych przed indeksacją wyszukiwarek
Brak aktualnej dokumentacji (instrukcji, opisów, dokumentacji technicznej sprzętu i oprogramowania)	• Brak instrukcji, opisów, dokumentacji technicznej sprzętu i oprogramowania • Brak instrukcji instalacyjnych i konfiguracyjnych środowiska lub oprogramowania *Zagrożenie związane z możliwymi trudnościami w odtworzeniu środowiska i zarządzania nim, gdy np. odejdzie pracownik IT lub będzie on niedostępny podczas krytycznej awarii*	1	3	3	**Procedury:** • Procedury przywracania
Nieprawidłowe / brak umowy o współpracy	Nieprecyzyjnie określone odpowiedzialności we współpracy, co stwarza ryzyko braku zabezpieczeń	1	1	1	**Zabezpieczenia:** • Umowa powierzenia • Pisemne upoważnienia dla podmiotu współpracującego z jasnymi warunkami bezpiecznej pracy z danymi powierzonymi
Nieprawidłowe / brak umowy gwarancyjnej lub wsparcia serwisowego	*Należy uwzględnić, że umowy wymagają przedłużania, czas reakcji nie oznacza czasu naprawy*	1	1	1	**Zabezpieczenie** • stosowane są Umowy powierzenia • w umowach stosuje się SLA • w umowach stosuje się kary umowne za niewywiązywanie się z realizacji umów • Stosowana jest "Procedura napraw w serwisach zewnętrznych"
Upadek firmy outsourcingowej lub dostawczej	• brak zastępstw, np. dla hostingodawcy poczty, dla wsparcia do zakupionej aplikacji • Utrata usługi / aplikacji, którą świadczy pomiot przetwarzający	1	2	2	**Zabezpieczenie** • Redundancja firmy / osoby
Awaria łączy telekomunikacyjnych	Krytyczne dla administratora świadczącego usługi wymagające „internetu”, usługi chmurowe, ISP oraz dostawcy platform SaaS	1	1	1	• Redundancja łączy

Załącznik nr 4 do Polityki Ochrony Danych Osobowych
w PANS w Jarosławiu

FORMULARZ REJESTRU INCYDENTU

Opis/okoliczność naruszenia/ incydentu	Ilość osób dotknięta naruszeniem/incydentem	Skutki naruszenia/incydentu	Działania zaradcze	Data rozpoczęcia wdrożenia działań	Data zakończenia wdrażania działań	Osoba odpowiedzialna za wdrożenie działania

Załącznik nr 5 do Polityki Ochrony Danych Osobowych
w PANS w Jarosławiu

Regulamin Ochrony Danych Osobowych w PANS w Jarosławiu

Niniejszy Regulamin stanowi wykaz podstawowych obowiązków z zakresu przestrzegania zasad ochrony danych osobowych zgodnie z przepisami RODO dla:

- pracowników,
- współpracowników,
- pracowników podmiotów trzecich, posiadających dostęp do danych osobowych przetwarzanych przez Administratora / Podmiot przetwarzający,
- użytkowników systemów informatycznych z dostępem do danych osobowych przetwarzanych przez Administratora / Podmiot przetwarzający.

Każda z w/w osób powinna zapoznać się z poniższym regulaminem oraz zobowiązać się do stosowania zasad w nim zawartych.

SPIS TREŚCI

1 ZASADY BEZPIECZNEGO UŻYTKOWANIA SPRZĘTU IT, DYSKÓW, PROGRAMÓW

1. W przypadku, gdy użytkownik przetwarzający dane osobowe korzysta ze sprzętu IT, zobowiązany jest do jego ochrony przed jakimkolwiek zniszczeniem lub uszkodzeniem. Za sprzęt IT rozumie się: komputery stacjonarne, monitory, drukarki, skanery, ksera, laptopy, służbowe tablety i smartfony.
2. Użytkownik ma obowiązek natychmiast zgłosić zagubienie, utratę lub zniszczenie powierzonego mu sprzętu IT.
3. Samowolne otwieranie (demontaż) sprzętu IT, instalowanie dodatkowych urządzeń (np. twardych dysków, pamięci) lub podłączanie jakichkolwiek niezatwierdzonych urządzeń do systemu informatycznego jest zabronione.
4. Użytkownik jest zobowiązany do uniemożliwienia osobom niepowołanym (np. pracownikom innych działów) wglądu do danych wyświetlanych na monitorach komputerowych – **tzw. „polityka czystego ekranu".**
5. Przed czasowym opuszczeniem stanowiska pracy, użytkownik zobowiązany jest wywołać blokowany hasłem wygaszacz ekranu (WINDOS + L) lub wylogować się z systemu bądź z programu.
6. Po zakończeniu pracy, użytkownik zobowiązany jest:
a) wylogować się z systemu informatycznego, a następnie wyłączyć sprzęt komputerowy,
b) zabezpieczyć stanowisko pracy, w szczególności wszelkie nośniki magnetyczne i optyczne, na których znajdują się dane osobowe.
7. Użytkownik jest zobowiązany do usuwania plików z nośników/dysków, do których mają dostęp inni użytkownicy nieupoważnieni do dostępu do takich plików (np. podczas współużytkowania komputerów).
8. Jeśli użytkownik jest uprawniony do niszczenia nośników, powinien trwale zniszczyć sam nośnik lub trwale usunąć z niego dane (np. zniszczenie płyt DVD w niszczarce, zniszczenie twardego dysku, pendrive np. przy użycia młotka).
9. W przypadku przechowywania na komputerze przenośnym danych osobowych lub stanowiących tajemnicę pracodawcy, użytkownik zobowiązany jest do ich przechowywania na

dysku szyfrowanym, zabezpieczonym, co najmnie 12 znakowym hasłem (duże, małe litery, znaki specjalne lub cyfry).
10.W przypadku kradzieży lub zgubienia komputera przenośnego, Użytkownik powinien natychmiast powiadomić o tym osobę odpowiedzialną za ochronę danych (IOD), zaznaczając jednocześnie, jakiego rodzaju dane były na tym urządzeniu przechowywane.

2 ZASADY UŻYWANIA KOMPUTERÓW PRZENOŚNYCH

1. W przypadku przechowywania na komputerze przenośnym danych osobowych lub stanowiących tajemnicę pracodawcy, użytkownik zobowiązany jest do przechowywania na dysku szyfrowanym, zabezpieczonym, co najmniej 12 znakowym hasłem.
2. Na komputerach przenośnych przeznaczonych do prezentacji multimedialnych (w szczególności umieszczonych w miejscach do których dostęp ma większa liczba pracowników i studentów jak np. sale wykładowe) nie powinny, o ile jest to możliwe, znajdować się dane osobowe lub stanowiące tajemnicę pracodawcy.
3. W przypadku kradzieży lub zgubienia komputera przenośnego, użytkownik powinien natychmiast powiadomić o tym osobę odpowiedzialną za ochronę danych (IOD), zaznaczając jednocześnie, jakiego rodzaju dane były na komputerze przechowywane.
4. W przypadku pozostawiania komputerów przenośnych w biurze zaleca się umieszczenie ich po zakończeniu pracy w zamykanych szafkach.
5. Pracując na komputerze przenośnym w miejscach publicznych użytkownik zobowiązany jest chronić wyświetlane na monitorze informacje przed wglądem osób nieupoważnionych.

3 ZASADY PRACY NA PRYWATNYCH URZĄDZENIACH IT

1. Pracownik może pracować na prywatnym sprzęcie tylko w wyjątkowych sytuacjach.
2. Każdorazowe używanie prywatnych urządzeń przez pracowników administracyjnych niebędących nauczycielami akademickimi, które będą podłączone do sieci lokalnej Uczelni wymaga uprzedniej zgody przełożonego a ponadto powinno być poprzedzone sprawdzeniem przez pracownika Działu Informatyki i zeskanowaniem w celu wykrycia ewentualnych zagrożeń.
3. Jeżeli pracownik wykorzystuje własne urządzenia do pracy z danymi osobowymi, powinno być one odpowiednio zabezpieczone poprzez wprowadzenie haseł zgodnie z polityką haseł.

4 ZARZĄDZANIE UPRAWNIENIAMI

1. Każdy użytkownik z dostępem do danych osobowych (np. na swoim komputerze, na dysku sieciowym, w programie lub aplikacji, w poczcie elektronicznej) musi posiadać swój własny indywidualny identyfikator (login) do logowania.
2. Użytkownik otrzymuje dostęp i odpowiednie uprawnienia do zasobów i aplikacji na polecenie przełożonych i przy realizacji pracowników Działu Informatyki. Procedura nadawania uprawnień została określona w Polityce Ochrony Danych w Państwowej Akademii Nauk Stosowanych im. ks. Bronisława Markiewicza w Jarosławiu.
3. Użytkownicy nie mają prawa do samodzielnej zmiany uprawnień, np. przydzielenia sobie uprawnień administratora.
4. Użytkowników obowiązuje zasada pracy na własnym koncie. Zabronione jest, zatem umożliwianie innym osobom pracy na koncie innego użytkownika.

5 POLITYKA HASEŁ

1. Pierwsze (pierwotne) hasło użytkownika nadawane jest przez Administratora i przekazywane mu w poufny sposób.
2. Użytkownik systemu zobowiązany jest do niezwłocznej zmiany tego hasła.
3. Hasła powinny składać się, z co najmniej 12 znaków.
4. Hasła powinny zawierać duże litery + małe litery + cyfry (lub znaki specjalne).
5. Hasła nie mogą być łatwe do odgadnięcia. Nie powinny być powszechnie używanymi słowami. W szczególności nie należy, jako haseł wykorzystywać: dat, imion i nazwisk osób bliskich, imion zwierząt, popularnych dat, popularnych słów, typowych zestawów: 123456, qwerty.

6. Hasła nie powinny być ujawnianie innym osobom. Nie należy zapisywać haseł na kartkach i w notesach, nie naklejać na monitorze komputera, nie trzymać pod klawiaturą lub w szufladzie.
7. W przypadku ujawnienia hasła – należy natychmiast go zmienić.
8. Jeżeli system nie wymusza zmiany haseł, użytkownik zobowiązany jest do samodzielnej zmiany hasła.
9. W przypadku utraty uprawnień przez osobę administrującą systemem należy niezwłocznie zmienić hasła, do których miała dostęp.

6 ZABEZPIECZENIE DOKUMENTACJI PAPIEROWEJ Z DANYMI OSOBOWYMI

1. Pracownicy są zobowiązani do stosowania tzw. „**polityki czystego biurka**". Polega ona na zabezpieczaniu (zamykaniu) dokumentów np. w szafach, biurkach, pomieszczeniach przed kradzieżą lub wglądem osób nieupoważnionych po godzinach pracy lub podczas ich nieobecności w trakcie godzin pracy. Zabrania się pozostawiania kluczy w zamkach szaf/ biurek.
2. Upoważnieni pracownicy zobowiązani są do niszczenia dokumentów i wydruków w niszczarkach lub utylizacji ich w specjalnych bezpiecznych pojemnikach z przeznaczeniem do bezpiecznej utylizacji.
3. Zabrania się pozostawiania dokumentów z danymi osobowymi poza zabezpieczonymi pomieszczeniami, np. w korytarzach, na kserokopiarkach, drukarkach, w pomieszczeniach konferencyjnych.
4. Zabrania się wyrzucania niezniszczonych dokumentów na śmietnik lub porzucania ich na zewnątrz.

7 ZASADY WYNOSZENIA NOŚNIKÓW Z DANYMI POZA UCZELNIĘ

1. Użytkownicy nie mogą wynosić na zewnątrz organizacji wymiennych elektronicznych nośników informacji z zapisanymi danymi osobowymi bez zgody pracodawcy / zleceniodawcy. Do takich nośników należą m.in.: przenośne twarde dyski, pendrive, płyty CD, DVD, pamięci typu Flash.
2. Dane osobowe wynoszone poza uczelnię muszą być opatrzone hasłem (hasłowane dyski, hasłowane pliki).
3. Należy zapewnić bezpieczne przewożenie dokumentacji papierowej w plecakach, teczkach.
4. Należy korzystać ze sprawdzonych firm kurierskich.
5. W przypadku, gdy dokumenty przewozi pracownik, zobowiązany jest do zabezpieczenia przewożonych dokumentów przed zagubieniem i kradzieżą.

8 ZASADY PRZEBYWANIA W POMIESZCZENIACH SŁUŻBOWYCH POZA GODZINAMI PRACY

1. Przebywanie przez pracowników w pomieszczeniach służbowych poza obowiązującym ich rozkładem czasu pracy, w tym także w dni wolne od pracy jest dozwolone wyłącznie po uzyskaniu zgody przełożonego.
2. Zgoda powinna być wyrażona najpóźniej przed rozpoczęciem pracy poza ustalonymi godzinami pracy.
3. Przebywanie pracowników gospodarczych w pomieszczeniach szczególnie chronionych (pomieszczenia Kwestury, Działu Spraw Pracowniczych, Działu Obsługi Studentów, Działu Informatyki) może odbywać się wyłącznie w obecności osób upoważnionych.

9 ZASADY KORZYSTANIA Z INTERNETU

1. Użytkownik zobowiązany jest do korzystania z Internetu wyłącznie w celach służbowych.
2. Zabrania się zgrywania na dysk twardy komputera oraz uruchamia jakichkolwiek programów nielegalnych oraz plików pobranych z niewiadomego źródła. Pliki takie powinny być ściągane tylko za każdorazową zgodą osoby upoważnionej do administrowania infrastrukturą IT i tylko w uzasadnionych przypadkach. Zabrania się pobierania i samodzielnego instalowania oprogramowania.
3. Użytkownik ponosi odpowiedzialność za szkody spowodowane przez oprogramowanie instalowane z Internetu.

4. Zabrania się korzystania ze stron, na których prezentowane są informacje o charakterze przestępczym, hackerskim, pornograficznym, lub innym zakazanym przez prawo (na większości stron tego typu jest zainstalowane szkodliwe oprogramowanie infekujące w sposób automatyczny system operacyjny komputera szkodliwym oprogramowaniem).
5. Nie należy w opcjach przeglądarki internetowej włączać opcji autouzupełniania formularzy i zapamiętywania haseł.
6. W przypadku korzystania z szyfrowanego połączenia przez przeglądarkę, należy zwracać uwagę na pojawienie się odpowiedniej ikonki (kłódka) oraz adresu www rozpoczynającego się frazą "https:". Dla pewności należy „kliknąć" na ikonkę kłódki i sprawdzić, czy właścicielem certyfikatu jest wiarygodny właściciel.
7. Należy zachować szczególną ostrożność w przypadku podejrzanego żądania lub prośby zalogowania się na stronę lub podania naszych loginów i haseł, PIN-ów, numerów kart płatniczych przez Internet. Szczególnie tyczy się to żądania podania takich informacji przez rzekomy bank. Administratorzy systemów informatycznych do realizacji swoich zadań nie wymagają podawania powyższych danych.

10 ZASADY KORZYSTANIA Z POCZTY ELEKTRONICZNEJ

1. Przesyłanie danych osobowych z użyciem maila poza Uczelnię może odbywać się tylko przez osoby do tego upoważnione.
2. W przypadku przesyłania danych osobowych poza Uczelnię należy wykorzystywać mechanizmy kryptograficzne szyfrowania plików z danymi. Instrukcja przesyłania plików zawierających dane osobowe stanowi załącznik do regulaminu.
3. W przypadku zabezpieczenia plików hasłem, obowiązuje minimum 16 znaków: duże i małe litery i cyfry lub znaki specjalne a hasło należy przesłać inną metodą, np. przekazać w rozmowie telefonicznej lub SMS-em.
4. Zabrania się przesyłania haseł dostępu w tej samej wiadomości, w której przesyłane są dane osobowe.
5. Użytkownicy powinni zwracać szczególną uwagę na poprawność adresu odbiorcy dokumentu.
6. Zaleca się, aby użytkownik podczas przesyłania danych osobowych mailem zawarł w treści prośbę o potwierdzenie otrzymania i zapoznania się z informacją przez adresata.
7. Nie należy otwierać załączników (plików) w mailach nawet od rzekomo znanych nam nadawców bez weryfikacji tegoż nadawcy. Tego typu maile większości przypadków zawierają załączniki ze szkodliwymi programami, które po „kliknięciu" infekują komputer użytkownika oraz często pozostałe komputery w sieci. W wyniku działania takiego szkodliwego oprogramowania może dojść do poważnych incydentów, łącznie z pełną utratą danych osobowych lub zaszyfrowanie m przez kryptowirusy.
8. Bez weryfikacji wiarygodności nadawcy, nie należy „klikać" na hiperlinki w mailach, gdyż mogą to być hiperlinki do stron zainfekowanych lub niebezpiecznych. Użytkownik „klikając" na taki hiperlink bezwiednie infekuje swój komputer oraz często pozostałe komputery w sieci. W wyniku takiej infekcji może dojść do poważnych incydentów, łącznie z pełną utratą danych osobowych lub zaszyfrowanie m przez kryptowirusy.
9. Należy zgłaszać pracownikom Działu Informatyki przypadki podejrzanych emaili.
10. Zabrania się rozsyłania wiadomości e-malii w formie „łańcuszków szczęścia".
11. Podczas wysyłania maili do wielu adresatów jednocześnie, należy użyć metody „Ukryte do wiadomości – BCC". Zabronione jest rozsyłanie maili do wielu adresatów z użyciem opcji „Do wiadomości" (skrót CC).
12. Użytkownicy nie powinni rozsyłać wiadomości e-maili zawierających załączniki o dużym rozmiarze.
13. Użytkownicy powinni okresowo kasować niepotrzebne maile.
14. Mail służbowy jest przeznaczony wyłącznie do wykonywania obowiązków służbowych.
15. Zakazuje się wysyłania korespondencji służbowej na prywatne skrzynki pocztowe pracowników lub innych osób.
16. Użytkownicy mają prawo korzystać z poczty mailowej dla celów prywatnych wyłącznie okazjonalnie i powinno być to ograniczone do niezbędnego minimum.

17. Korzystanie z maila dla celów prywatnych nie może wpływać, na jakość i ilość świadczonej przez użytkownika pracy oraz na prawidłowe i rzetelne wykonywanie przez niego obowiązków służbowych
18. Użytkownicy nie mają prawa korzystać z poczty elektronicznej w celu rozpowszechniania treści o charakterze obraźliwym, niemoralnym lub niestosownym wobec powszechnie obowiązujących zasad postępowania.
19. Użytkownik bez zgody pracodawcy/zleceniodawcy nie ma prawa wysyłać wiadomości zawierających dane osobowe dotyczące pracodawcy/zleceniodawcy, jego pracowników, klientów, dostawców lub kontrahentów za pośrednictwem Internetu, w tym przy użyciu prywatnej elektronicznej skrzynki pocztowej.

11 OCHRONA ANTYWIRUSOWA

1. Użytkownicy zobowiązani są do skanowania plików wprowadzanych z zewnętrznych nośników programem antywirusowym, jeśli system antywirusowy taką funkcje posiada.
2. Zakazane jest wyłączanie systemu antywirusowego podczas pracy systemu informatycznego przetwarzającego dane osobowe.
3. W przypadku stwierdzenia zainfekowania systemu lub pojawienia się komunikatów „np.; Twój system jest zainfekowany!, Zainstaluj program antywirusowy", użytkownik obowiązany jest poinformować niezwłocznie o tym fakcie przełożonego bądź pracownika Działu Informatyki.

12 PROCEDURA NAPRAWY SPRZĘTU W SERWISACH ZEWNĘTRZNYCH

1. Pracownicy Działu Informatyki odpowiadają za sprawdzanie poprawności działania systemów IT, w tym: stacji roboczych, serwerów, drukarek, baz danych, aplikacji, poczty email
2. Pracownicy Działu Informatyki odpowiadają za identyfikację i przyjmowanie zgłoszeń o nieprawidłowościach w działaniu systemu informatycznego oraz oprogramowania celem ich niezwłocznego usunięcia
3. W przypadku napraw dokonywanych na zewnątrz (z komputerów należy uprzednio wymontować dyski i wszelkie nośniki, z urządzeń mobilnych karty pamięci, usunąć dane z nośnika z użyciem specjalistycznego oprogramowania).
4. W przypadku naprawy sprzętu z danymi osobowymi na nośniku - rekomendowane jest zawarcie specjalnego zapisu w umowie serwisowej, gwarantującego bezpieczną naprawę.
5. Rekomendowane jest korzystanie z serwisu, który dokonuje napraw u klienta (umowy gwarancyjne on-site).
6. Czynności konserwacyjne i naprawcze wykonywane przez osoby nieposiadające upoważnień do przetwarzania danych (np. specjalistów z firm zewnętrznych) muszą być wykonywane pod nadzorem osób upoważnionych.
7. Wszelkie prace konserwacyjne i naprawcze sprzętu komputerowego oraz uaktualnienia systemu informatycznego wykonywane przez podmiot zewnętrzny, powinny odbywać się na zasadach określonych w szczegółowej umowie z uwzględnieniem klauzuli dotyczącej ochrony danych.

13 SKRÓCONA INSTRUKCJA POSTĘPOWANIA W PRZYPADKU NARUSZENIA OCHRONY DANYCH OSOBOWYCH

1. Każda osoba upoważniona do przetwarzania danych osobowych zobowiązana jest do powiadomienia pracodawcy/zleceniodawcy w przypadku stwierdzenia lub podejrzenia naruszenia ochrony danych osobowych.
2. Do sytuacji wymagających powiadomienia, należą:
   a) niewłaściwe zabezpieczenie fizyczne pomieszczeń, urządzeń i dokumentów;
   b) niewłaściwe zabezpieczenie sprzętu IT, oprogramowania przed wyciekiem, kradzieżą i utratą danych osobowych;
   c) nieprzestrzeganie zasad ochrony danych osobowych przez pracowników (np. niestosowanie zasady czystego biurka/ekranu, ochrony haseł, niezamykanie pomieszczeń, szaf, biurek).
3. Do incydentów wymagających powiadomienia, należą:

a) zdarzenia losowe zewnętrzne (pożar obiektu/pomieszczenia, zalanie wodą, utrata zasilania, utrata łączności);
b) zdarzenia losowe wewnętrzne (awarie serwera, komputerów, twardych dysków, oprogramowania, pomyłki pracowników Działu Informatyki, użytkowników, utrata / zagubienie danych);
c) umyślne incydenty (włamanie do systemu informatycznego lub pomieszczeń, kradzież danych/sprzętu, wyciek informacji, ujawnienie danych osobom nieupoważnionym, świadome zniszczenie dokumentów/danych, działanie wirusów i innego szkodliwego oprogramowania).

4. Typowe przykłady incydentów wymagające reakcji:
a) ślady na drzwiach, oknach i szafach wskazują na próbę włamania;
b) dokumentacja jest niszczona bez użycia niszczarki;
c) fizyczna obecność w budynku lub pomieszczeniach osób zachowujących się podejrzanie;
d) otwarte drzwi do pomieszczeń, szaf, gdzie przechowywane są dane osobowe;
e) ustawienie monitorów pozwala na wgląd osób postronnych w dane osobowe;
f) wynoszenie danych osobowych w wersji papierowej i elektronicznej na zewnątrz uczelni bez upoważnienia Pracodawcy / Zleceniodawcy;
g) udostępnienie danych osobowych osobom nieupoważnionym w formie papierowej, elektronicznej i ustnej;
h) telefoniczne próby wyłudzenia danych osobowych;
i) kradzież, zagubienie komputerów lub CD, twardych dysków, pendrive z danymi osobowymi;
j) maile zachęcające do ujawnienia identyfikatora i/lub hasła;
k) pojawienie się wirusa komputerowego lub niestandardowe zachowanie komputerów;
l) hasła do systemów przyklejone są w pobliżu komputera.

14 OBOWIĄZEK ZACHOWANIA POUFNOŚCI I OCHRONY DANYCH OSOBOWYCH

1. Każda z osób dopuszczona do przetwarzania danych osobowych jest zobowiązana do:
a) przetwarzania danych osobowych wyłącznie w zakresie i celu przewidzianym w powierzonych przez Pracodawcę/Zleceniodawcę zadaniach;
b) zachowania w tajemnicy danych osobowych, do których mam lub będzie miał/a dostęp w związku z wykonywaniem zadań powierzonych przez Pracodawcę/Zleceniodawcę;
c) niewykorzystywania danych osobowych w celach niezgodnych z zakresem i celem powierzonych zadań przez Pracodawcę/Zleceniodawcę;
d) zachowania w tajemnicy sposobów zabezpieczenia danych osobowych;
e) ochrony danych osobowych przed przypadkowym lub niezgodnym z prawem zniszczeniem, utratą, modyfikacją danych osobowych, nieuprawnionym ujawnieniem danych osobowych, nieuprawnionym dostępem do danych osobowych oraz przetwarzaniem.

2. Jeśli jest to przewidziane, osoba dopuszczona do przetwarzania odbywa szkolenie z zasad ochrony danych osobowych.
3. Osoby zapoznane z treścią niniejszego Regulaminu ODO lub przeszkolone zobowiązane są podpisać Oświadczenie o poufności.
4. Zabrania się przekazywania bezpośrednio lub przez telefon danych osobowych osobom nieupoważnionym lub osobom, których tożsamości nie można zweryfikować lub osobom podszywającym się pod kogoś innego.
5. Zabrania się przekazywania lub ujawniania danych osobom lub instytucjom, które nie mogą wykazać się jasną podstawą prawną do dostępu do takich danych.

15 POSTĘPOWANIE DYSCYPLINARNE

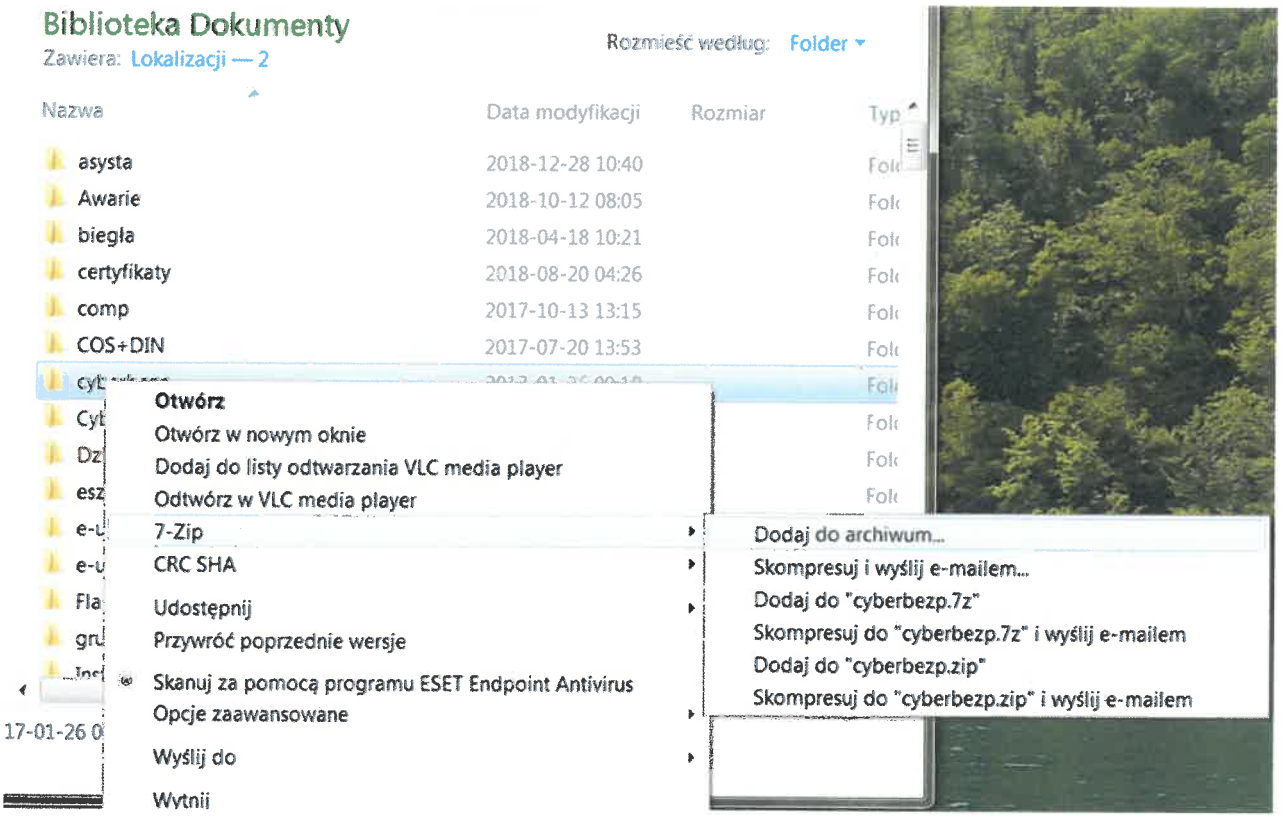
1. Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu potraktowane będą, jako ciężkie naruszenie obowiązków pracowniczych lub naruszenie zasad współpracy.
2. Postępowanie sprzeczne z powyższymi zobowiązaniami, może też być uznane przez pracodawcę/zleceniodawcę za naruszenie przepisów karnych zawartych w ogólnym Rozporządzeniu o ochronie danych UE z dnia 27 kwietnia 2016 r.

Instrukcja przesyłania plików z danymi osobowymi

Jeśli przekazywane elektronicznie informacje, zawierające dane poufne (np. dane osobowe, finansowe) i mają być przekazane za pomocą niezabezpieczonego serwisu web, poczty elektronicznej, nośnika elektronicznego, transmisji, to pliki zawierające te dane **muszą zostać zaszyfrowane przed wysłaniem**.

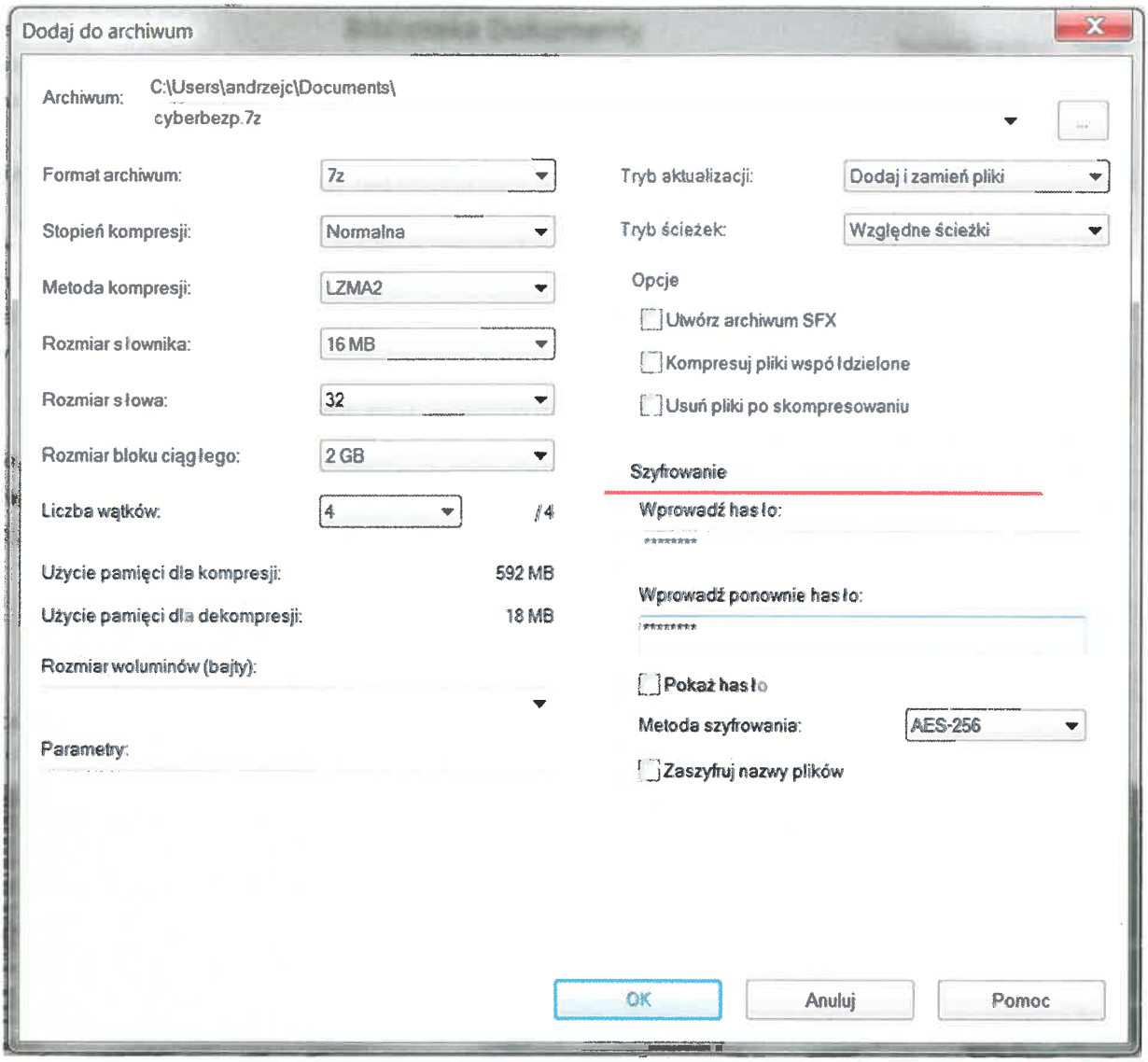
Do szyfrowania należy użyć darmowego programu 7-zip (*do pobrania z strony https://www.7-zip.org/*).

1. Przygotowanie plików z danymi
   - jeśli ma być wysłany więcej niż jeden plik, należy utworzyć nowy katalog tymczasowy i do niego skopiować te pliki.
   - jeśli jest to tylko jeden plik, nie jest to wymagane.
2. Szyfrowanie plików
   - zaznaczamy katalog lub plik do zaszyfrowania i klikamy prawym przyciskiem myszy. Z menu wybieramy opcję „*7-Zip*", a następnie „*Dodaj do archiwum*".

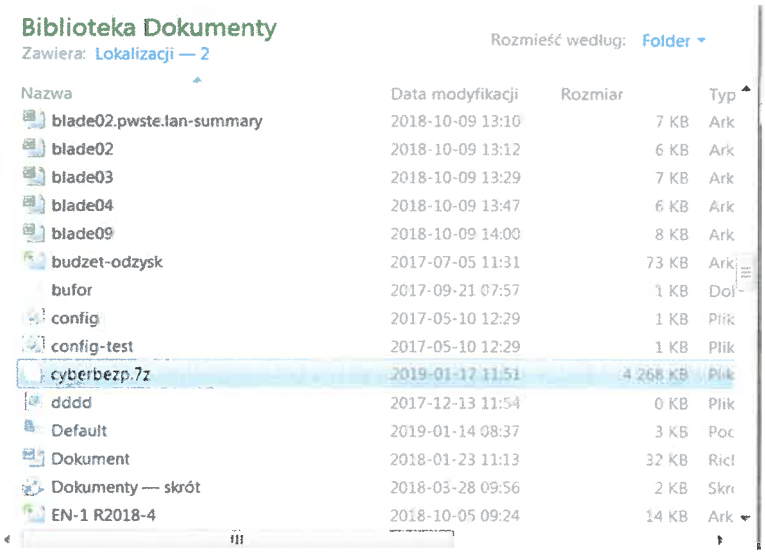


   - otworzy się okno programu „7-zip", gdzie w sekcji „Szyfrowanie" należy wpisać hasło. Hasło powinno mieć co najmniej 10 znaków dobranych losowo (nie powinno się używać nazw związanych z nazwą instytucji, nazwiskiem nadawcy lub odbiorcy).

Nie powinno się zaznaczać opcji „Utwórz archiwum SFX", gdyż tworzy to archiwum typu program (EXE), co w wypadku wysyłania pocztą może zablokować przesłanie wiadomości.



- - Po kliknięciu na OK zostanie utworzony plik archiwum.



3. Wysyłanie pliku
   - Utworzony plik i zaszyfrowany można wysłać pocztą lub umieścić na nośniku elektronicznym lub przekazać przez serwis WEB.

Hasła do pliku nie wolno wysyłać pocztą elektroniczną oraz zapisywać w pliku umieszczonym na nośniku elektronicznym. Nie wolno też umieszczać hasła zapisanego na papierze w przesyłce z nośnikiem.

Bezpieczną metodą przekazania hasła jest przekazanie go w rozmowie telefonicznej, w treści SMS lub wysłanie listem.

4. Jeśli został utworzony katalog tymczasowy z plikami do przekazania, po wykonaniu tej operacji powinien zostać usunięty.

Załącznik nr 6 do Polityki Ochrony Danych Osobowych
w PANS w Jarosławiu

....., dnia .....

Nazwisko i imię .....

Komórka organizacyjna .....

Stanowisko .....

OŚWIADCZENIE O POUFNOŚCI

Oświadczam, iż zapoznano mnie z przepisami dotyczącymi ochrony danych osobowych, w szczególności Rozporządzeniem Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE z 27 kwietnia 2016r. – RODO (Dz. Urz. UE L 119 z 04.05.2016), z postanowieniami *Polityki Ochrony Danych Osobowych w PANS w Jarosławiu oraz Instrukcją zarządzania systemami informatycznymi – wykaz zabezpieczeń* w Państwowej Akademii Nauk Stosowanych im. ks. Bronisława Markiewicza w Jarosławiu.

W szczególności zobowiązuję się do:

- przetwarzania danych osobowych wyłącznie w zakresie i celu przewidzianym w powierzonych przez Administratora zadaniach,
- zachowania w tajemnicy danych osobowych, do których mam lub będę miał/a dostęp w związku z wykonywaniem zadań powierzonych przez Administratora,
- niewykorzystywania danych osobowych w celach niezgodnych z zakresem i celem powierzonych zadań przez Administratora,
- zachowania w tajemnicy sposobów zabezpieczenia danych osobowych,
- ochrony danych osobowych przed przypadkowym lub niezgodnym z prawem zniszczeniem, utratą, modyfikacją danych osobowych, nieuprawnionym ujawnieniem danych osobowych, nieuprawnionym dostępem do danych osobowych oraz przetwarzaniem.

Przyjmuję do wiadomości, iż postępowanie sprzeczne z powyższymi zobowiązaniami może być uznane przez Administratora za naruszenie przepisów Rozporządzenia o ochronie danych UE z dnia 27 kwietnia 2016r.

.....
(podpis oświadczającego)

Polityka kluczy PANS w Jarosławiu

1. Polityka kluczy obejmuje budynki/pomieszczenia Państwowej Akademii Nauk Stosowanych im. ks. Bronisława Markiewicza w Jarosławiu znajdujące się przy ulicy Czarnieckiego 16, Pruchnickiej 2 oraz Grunwaldzkiej 24 w Jarosławiu.
2. Pracowników niebędących nauczycielami akademickimi obowiązuje pięciodniowy tydzień pracy (od poniedziałku do piątku, w godzinach 07:00 – 16:00), pracowników dydaktycznych obowiązuje indywidualnie ustalony wymiar czasu pracy, pracowników ochrony mienia oraz pracowników gospodarczych (personel sprzątający) obowiązuje siedmiodniowy tydzień pracy (od poniedziałku do niedzieli). Dla pracowników niebędących nauczycielami akademickimi może zostać wyznaczony inny niż wyżej wskazany wymiar czasu pracy, stosownie do zapotrzebowania danej jednostki.
3. Pobranie/zdawanie klucza do pomieszczeń administracyjnych znajdujących się w budynku Rektoratu PANS w Jarosławiu następuje przy użyciu depozytora (system Bezpiecznego Klucza), na podstawie dostępu nadanego w systemie elektronicznym oraz legitymacji pracowniczej bądź w szczególnie uzasadnionych przypadkach kodu dostępu.
4. Upoważnienia do pobierania kluczy do pomieszczeń administracyjnych mają wyłącznie osoby zatrudnione w danej jednostce organizacyjnej. Ewidencja dostępu do pomieszczeń prowadzona jest w formie elektronicznej przez Dział Telekomunikacji i Automatyki.
5. Pobieranie/zdawanie kluczy w depozytorze jest automatycznie ewidencjonowane w systemie i nie wymaga potwierdzenia w książce ewidencji pobrań.
6. Klucze do pomieszczeń, w których odbywają się zajęcia dydaktyczne (sale wykładowe, ćwiczeniowe, laboratoria, pracownie przy ul. Czarnieckiego oraz Pruchnickiej) znajdują się w depozytorach umieszczonych na poszczególnych wydziałach. Pobieranie/zdawanie klucza następuje na podstawie dostępu nadanego w systemie elektronicznym oraz legitymacji pracowniczej bądź w szczególnie uzasadnionych przypadkach kodu dostępu. Klucze mają prawo pobierać wyłącznie prowadzący zajęcia. Osoba pobierająca klucz staje się za niego odpowiedzialna.
7. Klucze do pomieszczeń, w których odbywają się zajęcia dydaktyczne znajdujące się w Bibliotece, J1, J2, J3, J5 i Centrum Badawczo-Dydaktycznym z Działem Obsługi Studentów otwierane są za pomocą systemu kontroli dostępu, obsługiwanego legitymacją pracowniczą bądź w szczególnie uzasadnionych przypadkach kodu dostępu. Ewidencja dostępu prowadzona jest w formie elektronicznej przez Dział Informatyki.
8. Klucze do pomieszczeń, w których odbywają się zajęcia dydaktyczne przy ul. Grunwaldzkiej wydawane są przez pracownika ochrony mienia. Pobieranie/zdawanie klucza następuje na podstawie pisemnej ewidencji pobrań.
9. Personel sprzątający posiada własny zbiorczy zestaw kluczy zawierający klucze do wszystkich pomieszczeń, w których prowadzone są prace porządkowe. Zestawy kluczy przechowywane są w pomieszczeniach, do których klucze znajdują się w poszczególnych wydziałach, portierni Domu Studenckiego Victoria bądź Rektoratu.
10. Sposób korzystania z kluczy do Kancelarii Materiałów Niejawnych i Spraw Obronnych opisany został w Instrukcji wydawania i przyjmowania kluczy do pomieszczeń Kancelarii Materiałów Niejawnych.
11. Klucze do Działu Spraw Pracowniczych, Kwestury oraz do pomieszczeń biblioteki pozostają pod osobistym nadzorem pracowników tych jednostek.
12. Wejście do budynku Centrum Badawczo-Dydaktycznego z Działem Obsługi Studentów zabezpieczone jest systemem automatycznego otwierania i zamykania o ustalonych godzinach.
13. Wejście do pomieszczeń Działu Informatyki oraz serwerowni objęte jest systemem kontroli dostępu.
14. Komplety kluczy zapasaowych do serwerowni oraz Działu Informatyki znajdują się w portierni Domu Studenckiego Victoria.
15. Klucze zapasowe do pomieszczeń administracyjnych przechowywane są w zamkniętej na klucz szafie znajdującej się w pokoju 7 i pozostają pod nadzorem pracowników Działu Administracyjno-Gospodarczego. Wydawanie kluczy zapasowych upoważnionym pracownikom może odbywać się tylko w uzasadnionych sytuacjach oraz przypadkach awaryjnych za zgodą osób uprawnionych.

Wydanie kluczy zapasowych wymaga odnotowania w ewidencji ze wskazaniem: kto pobrał klucz, datę pobrania i zwrotu oraz podpisem pobierającego. Klucze zapasowe po ich wykorzystaniu należy niezwłocznie zwrócić do depozytu. Klucze zapasowe do pomieszczeń administracyjnych, w tym pomieszczeń szczególnie chronionych umieszczone są w oddzielnych kopertach, zamkniętych, opisanych oraz oznaczonych przez osobę, która jest za nie odpowiedzialna.

16. Klucze zapasowe do pomieszczeń, w których odbywają się zajęcia dydaktyczne znajdują się w sekretariatach poszczególnych wydziałów. Wydawanie kluczy zapasowych upoważnionym pracownikom może odbywać się tylko w uzasadnionych sytuacjach oraz przypadkach awaryjnych za zgodą osób uprawnionych. Klucze zapasowe po ich wykorzystaniu należy niezwłocznie zwrócić do depozytu. Wydanie kluczy zapasowych wymaga odnotowania w ewidencji ze wskazaniem: kto pobrał klucz, datę pobrania i zwrotu oraz podpisem pobierającego.
17. Pomieszczenia szczególnie chronione, w wyjątkowych, uzasadnionych przypadkach mogą zostać otwarte komisyjnie przez osoby nieposiadające upoważnienia. W takim przypadku sporządza się protokół z uwzględnieniem składu osobowego, powodu otwarcia oraz dokonanych czynności.
18. Klucze służące do zabezpieczenia biurek i szaf muszą być jednoznacznie opisane. Klucze pozostają pod nadzorem pracowników, którzy ponoszą pełną odpowiedzialność za ich należyte zabezpieczenie.
19. Zabrania się pozostawiania kluczy w biurkach i szafach podczas chwilowej nieobecności osób upoważnionych w pomieszczeniu oraz po zakończeniu pracy w danym dniu.
20. Po zakończeniu pracy, klucze służące do zabezpieczenia biurek i szaf muszą być przechowywane w zabezpieczonym miejscu.
21. Po zakończeniu pracy, pracownicy są zobowiązani do zabezpieczenia pomieszczeń a w szczególności (wyłączenia i zabezpieczenia urządzeń elektronicznych oraz elektrycznych, wyłączenia oświetlenia, zabezpieczenia i zamknięcia okien i drzwi).
22. Naruszenie zasad Polityki Kluczy może spowodować wyciągnięcie konsekwencji wynikających z art. 52 kodeksu pracy oraz z art. 363 § 1. kodeksu cywilnego.

Procedura audytu

Celem audytów wewnętrznych jest ocena, czy system ochrony danych osobowych jest skutecznie wdrożony i funkcjonuje zgodnie z wymaganiami RODO. Audyty prowadzone są w sposób obiektywny i bezstronny. Przestrzegana jest zasada, że audytorzy nie audytują własnej pracy.

1. Administrator (ewentualnie IOD) jest odpowiedzialny za planowanie i przeprowadzanie audytów wewnętrznych z roczną częstotliwością lub częściej.
2. Administrator odpowiada za przeprowadzony audyt.
3. Administrator (ewentualnie IOD) opracowuje programy audytów biorąc pod uwagę ważność procesów przetwarzania oraz audytowanych obszarów, jak też wyniki wcześniejszych audytów. Określa on kryteria audytu, jego cel, zakres i ewentualnie metody.
4. Administrator (ewentualnie IOD) jest zobowiązany do przygotowania się do przeprowadzenia audytu, zapoznając się z opisem audytowanego obszaru, stosowanych procedur i wyników poprzednich audytów
5. Administrator (ewentualnie IOD) realizuje działania audytowe mające na celu uzyskanie obiektywnych dowodów potwierdzających poprawność realizowanych zadań, procedur, polityk, zabezpieczeń, celów, spełniania wymagań RODO.
6. W przypadku stwierdzenia uchybień mających wpływ na skuteczność działania systemu ochrony danych zgodnego z RODO, audytor identyfikuje tzw. uchybienia lub spostrzeżenia
7. Wynik audytu zostaje udokumentowany przez Administratora (ewentualnie IOD).
8. Administrator dokonuje przeglądu i analizy wyniku audytu oraz decyduje o inicjowaniu działań korygujących, w przypadku zaistnienia poważnych uchybień.
9. Audyt jest przeprowadzany cyklicznie, nie rzadziej niż raz na rok. Administrator może zarządzić przeprowadzenie audytu doraźnego pełnego i cząstkowego.

Załącznik nr 9 do Polityki Ochrony Danych
PANS w Jarosławiu

Wykaz zabezpieczeń

1. Regulamin Ochrony Danych Osobowych, Polityka Ochrony Danych Osobowych w PANS w Jarosławiu dla pracowników i współpracowników

• osoby zatrudnione przy przetwarzaniu danych zostały zaznajomione z przepisami dotyczącymi ochrony danych osobowych (z Regulaminem Ochrony Danych Osobowych, Polityką Ochrony Danych Osobowych w PANS w Jarosławiu, przepisami RODO)
• osoby zatrudnione przy przetwarzaniu podpisują stosowne Oświadczenie poufności

2. Szkolenia personelu

• szkolenia wewnętrzne

3. Aktualizacja procedur

• realizowane są doraźne kontrole

4. Testy penetracyjne

• realizowane są testy penetracyjne

5. Procedury przywracania w razie incydentu

• stosowana jest "Procedura Plan ciągłości działania"

6. Polityka kluczy / polityka kontroli dostępu

• stosowana jest procedura "Polityka kluczy"
• kontrola kluczy zapasowych
• zakaz wstępu osobom nieupoważnionym
• kontrola wydawania i składowania kluczy (depozytornia kluczy)
• system kontroli dostępu

7. Dostęp do pomieszczeń i sprzętu

• ograniczenie dostępu do pomieszczeń /komputerów /drukarek /ksero
• ograniczenie dostępu do pomieszczeń osobom nieupoważnionym
• dostęp w obecności osoby upoważnionej

8. Zabezpieczenie dostępu do pomieszczeń (w tym biurowych)

• drzwi zamykane na klucz
• system kontroli dostępu

9. Zabezpieczenie dostępu do serwerowni

•System kontroli dostępu
•drzwi zamykane na klucz - ogniotrwałe
• ograniczenie dostępu do serwerowni

10. Zabezpieczenie dostępu do archiwum

• system kontroli dostępu

11. Zabezpieczenie dokumentacji w pomieszczeniach

• zamknięte niemetalowe szafy
• zamknięte metalowe szafy

• klucze do szaf zamykane w oddzielnych szafkach

12. Systemy alarmowe / zabezpieczenia antywłamaniowe
• rolety
• alarm

13. Ochrona fizyczna obiektu / pomieszczeń
• ochrona własna
• monitoring wizyjny

14. Strefy dostępu
• wdrożone strefy ograniczonego dostępu

15. System kontroli dostępu
• portiernia

16. System ppoż.
• system ppoż. w obiekcie
• gaśnice

17. Monitoring środowiskowy
• w serwerowni - czujnik temperaturowy
• powiadamianie administratorów o alertach temperatury

18. Monitoring wizyjny
• monitoring wizyjny w obrębie obiektu i otoczeniu

19. Systemy UPS / agregaty prądotwórcze
• zastosowano UPS podtrzymujący zasilanie serwerów
• zastosowano UPS dla kluczowych elementów systemu IT

20. Systemy antywirusowy i antyspamowy
• wersja stanowiskowa
• wersja serwerowa
• system licencjonowany
• system aktualizowany online
• funkcja skanowania poczty
• funkcja skanowania portów USB
• system antyspamowy

21. Sewery proxy i bramki filtrujące
• skan niebezpiecznej zawartości
• blokada ruchu na podstawie bazy reputacji
• blokada dostępu do określonych stron

22. Systemy firewall, NG firewall, UTM
• Firewall / NG Firewall / UTM do ochrony dostępu do sieci komputerowej
• firewall sprzętowy
• firewall programowy

23. Sondy IDS / IPS
• system IDS/IPS do ochrony dostępu do sieci komputerowej

24. Monitorowanie zużycia

• stosowany jest systemy monitorujący stan usług i zasobów krytycznych (serwerów/ baz danych/ urządzeń sieciowych)

25. Systemy do inwentaryzacji

• stosowany jest system do inwentaryzacji sprzętu

26. Szyfrowanie

• szyfrowanie komunikacji z serwerem poczty (SSL)
• szyfrowanie połączeń internetowych SSL/VPN
• szyfrowanie pendrive
• szyfrowanie dysków komputerów przenośnych (bitlocker)
• szyfrowanie sieci WIFI

27. Hardening

• włączenie szyfrowania
• zmiana domyślnych haseł
• wyłączenie niepotrzebnych funkcji i usług
• dodatki noscript i adblocker do przeglądarek

28. Aktualizacje systemu

• zarządzanie aktualizacjami systemu operacyjnego
• zarządzanie aktualizacjami aplikacji
• zarządzanie aktualizacjami przeglądarek internetowych

29. Backupy i archiwizacja

• stosowana jest "Procedura tworzenia kopii zapasowych"
• wykonywany jest backup serwerów / aplikacji / plików / konfiguracji / licencji /haseł
•kopie zapasowe przechowywane są poza serwerownią
• niszczenie/czyszczenie nośników przed utylizacją

30. Rozliczalność operacji

• program / aplikacja posiada mechanizm odnotowywania wykonywania operacji na danych osobowych. Odnotowane i logowane są: tworzenie rekordu /zmiana /usunięcie / identyfikator użytkownika dokonującego zmianę
• każdy użytkownik posiada swój indywidualny login

31. Postępowanie z nośnikami

• Stosowana jest Procedura postępowania z nośnikami i sprzętem poza uczelnią
• stosowany jest procedura korzystania z komputerów przenośnych"
• ograniczono możliwość kopiowania danych na pendrive

32. Zabezpieczenie pracy użytkowników

• Stosowana jest "Procedura korzystania z Internetu"
• Stosowana jest "Procedura korzystania z poczty elektronicznej"
• zahasłowane wygaszacze ekranu aktywowane w przypadku nieaktywności użytkownika
• poufne ustawienie monitorów

33. Wirtualizacja

• stosowana jest wirtualizacja serwerów

34. Niszczenie nośników

• określone zostały procedury niszczenia nośników

• niszczenie/czyszczenie nośników przed utylizacją

35. Zarządzanie uprawnieniami

• stosowana jest "Procedura zarządzania uprawnieniami"
• minimalizacja uprawnień
• separacja obowiązków
• zarządzanie uprawnieniami
• konta firmowe oddzielone od prywatnych

36. Uwierzytelnianie

• stosowana jest "Polityka haseł"
• długość hasła - 12 znakowe z dużymi i małymi literami i znakami specjalnymi
• użytkownicy zobowiązani są do samodzielnego zmieniania hasła
• zapewniono uwierzytelnianie do aplikacji/ stacji roboczych/ smartfonów /sieci /poczty

37. Umowy serwisowe

• w umowach stosuje się SLA
• w umowach stosuje się kary umowne za niewywiązywanie się z realizacji umów
• Stosowana jest "Procedura napraw w serwisach zewnętrznych"
• odpowiednie klauzule w zakresie przekazywania sprzętów na których znajdują się dane osobowe

Plan ciągłości działania

SPIS TREŚCI

1 PLAN AWARYJNY ODTWORZENIA SYSTEMU INFORMATYCZNEGO PO AWARII KRYTYCZNEJ

1.1 ZASADY POSTĘPOWANIA PRZY ODTWORZENIU SYSTEMU INFORMATYCZNEGO W LOKALIZACJI PODSTAWOWEJ

1. Postępowanie dla odtworzenia systemu zainstalowanego jako maszyna wirtualna:
   1) W razie wystąpienia krytycznej awarii systemu operacyjnego lub usunięcia maszyny wirtualnej obsługiwanej przez system VMware należy:
      a) odtworzyć maszynę wirtualną z ostatniej kopii w systemie Nakivo,
      b) jeśli dla odzyskanej maszyny istnieje bardziej aktualna kopia plików konfiguracyjnych lub danych w systemie kopii zapasowych należy z niego odtworzyć te pliki,
      c) przewidywany czas odtworzenia od 1 do 5 godzin.

2. Postępowanie w razie awarii sprzętowej serwera w szafie blade:
   1) uszkodzenie serwera należy zgłosić do serwisu firmy Lenowo przez stronę serwisu,
   2) system zarządzania automatycznie przeniesie maszyny wirtualne z uszkodzonego serwera na inne sprawne serwery,
   3) w razie uszkodzenia kilku serwerów, co może skutkować obniżeniem mocy obliczeniowej, brakiem pamięci RAM, należy wyłączyć systemy obsługujące niekrytyczne funkcje Uczelni i pozostawić pracujące tylko niezbędne,
   4) po usunięciu awarii serwera należy przenieś na niego maszyny wirtualne z innych serwerów tak by równomiernie rozłożyć obciążenie,
   5) przewidywany czas usunięcia awarii 2 dni robocze.

3. Postępowanie w razie uszkodzenia serwera dla bazy danych Oracle:
   1) uszkodzenie serwera należy zgłosić do serwisu firmy Lenowo przez stronę serwisu,
   2) po usunięciu awarii przez serwis należy odtworzyć system,
   3) jeśli awaria spowodowała uszkodzenia obydwu dysków w serwerze (brak systemu operacyjnego) należy odtworzyć system operacyjny z wykorzystaniem narzędzia **Relax-and-Recover**,
   4) przewidywany czas usunięcia awarii 2 dni robocze.

4. Uszkodzenie podzespołu w szafie blade (switch, switch FC):
   1) uszkodzenie serwera należy zgłosić do serwisu firmy Lenowo przez serwis https://support.lenovo.com/pl/en/,
   2) przewidywany czas usunięcia awarii 2 dni robocze
5. Uszkodzenie serwera typu Rack:
   1) jeśli jest możliwe użycie innego serwera o podobnych parametrach technicznych należy odtworzyć system za pomocą narzędzia **Relax-and-Recover,**
   2) jeśli nie można użyć innego serwera, należy w trybie pilnym wymienić uszkodzone elementy serwera lub zakupić nowy serwer,

3) w razie zakupu nowego serwera lub wymiany dysków należy odtworzyć system operacyjny za pomocą narzędzia **Relax-and-Recover** oraz pliki z systemu kopii zapasowych,
4) przewidywany czas usunięcia awarii od 2 dni roboczych do 3 tygodni.

1.2 ZASADY POSTĘPOWANIA PRZY ODTWORZENIU SYSTEMU INFORMATYCZNEGO W LOKALIZACJI ALTERNATYWNEJ

1. W przypadku zniszczenia serwerowni podstawowej wraz z serwerami należy uruchomić nową w budynku Wydziału Inżynierii Technicznej.
2. Przygotowanie serwerowni wymaga: dostawy serwerów typu Blade lub typu Rack, macierzy dyskowych, urządzeń sieciowych, szaf serwerowych.
3. Przewidywany czas operacji uruchomienia serwerowni zapasowej – minimum od 4 do 6 tygodni

2 PLAN AWARYJNY NA WYPADEK BRAKU ZASILANIA W SERWEROWNI

1. W razie awarii zasilania serwerowni następuje automatycznie przełączenie na zasilanie awaryjne z UPS.
2. Zasilanie z UPS serwerowni działa do około 35 minut.
3. W przypadku dłuższej awarii zasilania, UPS automatycznie wyłączy systemy informatyczne.
4. Awaria trwająca powyżej 12 godzin wymaga uruchomienia generatora prądu do zasilania serwerowni. Agregat należy podłączyć do gniazda 3 fazowego zlokalizowanego na ścianie budynku
5. W razie awarii UPS należy go wyłączyć i zasilać serwerownię bezpośrednio z sieci. W tym celu należy włączyć bypass. Awarię UPS zgłosić do serwisu

3 PLAN AWARYJNY NA WYPADEK USZKODZENIA URZĄDZENIA SIECIOWEGO

1. W razie awarii switcha budynkowego odpowiedzialnego za podłączenie do sieci światłowodowej należy wymienić go na zapasowy przechowywany w Dziale Informatyki – przewidywany czas usunięcia awarii - 4 godziny
2. W razie awarii jednego z przełączników w węźle centralnym należy przełączyć obsługę sieć na sprawny, ograniczając liczbę podłączonych linii światłowodowych do krytycznych potrzeb – przewidywany czas usunięcia awarii 8 godzin.
3. W razie uszkodzenia przełącznika sieciowego należy wymienić go na zapasowy przechowywany w Dziale Informatyki – przewidywany czas usunięcia awarii 2 godziny

4 PLAN AWARYJNY NA WYPADEK UTRATY DOSTĘPU DO SIECI INTERNET

W przypadku niedostępności internetu awarię zgłaszać do firmy Voice-Net telefon **0 801 011 453** lub **0 17 777 3000**. Zgłoszeniu wymaga podania NIP Uczelni **792 17 94 406**. Czas usunięcia awarii do 4 godzin

Jarosław, 19 lipca 2024 r.

Załącznik nr 11 do Polityki Ochrony Danych Osobowych
w PANS w Jarosławiu

WYKAZ POMIESZCZEŃ, W KTÓRYCH PRZETWARZANE SĄ DANE OSOBOWE

L.p.	Lokalizacja – adres	Precyzyjne określenie pomieszczenia	Dział/osoba użytkująca pomieszczenie	Zabezpieczenie pomieszczenia
1.	ul. Czarnieckiego 16, p.nr 111	**Dział Spraw Pracowniczych** (pomieszczenie szczególnie chronione)	Pracownicy działu	drzwi zamykane na klucz, klucz posiadają na wyłączność pracownicy działu, szafki zamykane na klucz, pomieszczenie szczególnie chronione, klucze pod osobistym nadzorem pracowników
2.	ul. Czarnieckiego 16, p.nr 112	**Kwestura** (pomieszczenie szczególnie chronione)	Pracownicy Kwestury	Pomieszczenia zamknięte na klucz, klucze posiadają wyłącznie pracownicy działu, szafy zamykane na klucz
3.	ul. Czarnieckiego 16, p.nr 101, 102, 103, 104, 106, 107, 108, 109, 110	**Biuro Rektora**	Pracownicy Biura Rektora	Pomieszczenia zamknięte na klucz, szafki zamykane na klucz, klucze do pomieszczeń mogą pobierać tylko pracownicy działu
4.	ul. Czarnieckiego 16, p.nr 113	**Kancelaria materiałów niejawnych i spraw obronnych** (pomieszczenie szczególnie chronione)	Pracownicy Kancelarii	Pomieszczenie szczególnie chronione, opatrzone plombą, obowiązuje instrukcja wydawania i pobierania kluczy do pomieszczeń Kancelarii Materiałów Niejawnych
5.	ul. Czarnieckiego 16, p.nr 1,6,7,8	**Dział Administracyjno-Gospodarczy**	Pracownicy działu	Drzwi zamykane na klucz, szafki zamykane na klucz, klucze do pomieszczeń mogą pobierać tylko pracownicy działu
6.	ul. Czarnieckiego 16, p.nr 9b, 10	**Dział Inwestycyjno-Techniczny**	Pracownicy działu	Drzwi zamykane na klucz, szafki zamykane na klucz, klucze do pomieszczeń mogą pobierać tylko pracownicy działu
7.	ul. Czarnieckiego 16, p.nr 2,3,4	**Dział Kształcenia**	Pracownicy działu	Drzwi zamykane na klucz, szafki zamykane na klucz, klucze do pomieszczeń mogą pobierać tylko pracownicy działu
8.	ul. Czarnieckiego 16, p.nr 5a, 5b	**Dział Pozyskiwania Funduszy**	Pracownicy działu	Drzwi zamykane na klucz, szafki zamykane na klucz, klucze do pomieszczeń mogą pobierać tylko pracownicy działu

9.	ul. Czarnieckiego 16, Budynek Biblioteki	**Biblioteka PANS w Jarosławiu**	Portier, pracownicy Biblioteki	Drzwi zamykane na klucz, szafki zamykane na klucz, klucze do pomieszczeń posiadają tylko pracownicy biblioteki
10.	ul. Czarnieckiego 16, p. 9a	**Dział Automatyki i Telekomunikacji**	Pracownicy działu	Drzwi zamykane na klucz, szafki zamykane na klucz, klucze do pomieszczeń mogą pobierać tylko pracownicy działu
11.	ul. Czarnieckiego 16	**Archiwum**	Pracowniciy działu	Drzwi otwierane są za pomocą Systemu Kontroli Dostępu, obsługiwanego kodem indywidualnym albo legitymacją pracowniczą dostęp do pomieszczeń mają wyłącznie pracownicy działu
12.	ul. Czarnieckiego 16, budynek Centrum Badawczo-Dydaktyczne z Działem Obsługi Studentów	**Dział Obsługi Studentów** (pomieszczenie szczególnie chronione)	Pracownicy działu	Drzwi otwierane są za pomocą Systemu Kontroli Dostępu, obsługiwanego kodem indywidualnym albo legitymacją pracowniczą, alarm (dostęp do pomieszczeń, w których znajdują się dane osobowe mają tylko pracownicy działu), alarm, szafki zamykane na klucz
13.	ul. Czarnieckiego 16, budynek J2	**Dział Informatyki** (pomieszczenie szczególnie chronione)	Pracownicy działu	Drzwi otwierane są za pomocą Systemu Kontroli Dostępu, obsługiwanego kodem indywidualnym albo legitymacją pracowniczą dostęp do pomieszczenia mają wyłącznie pracownicy działu
14.	ul. Czarnieckiego 16, budynek Centrum Badawczo-Dydaktyczne z Działem Obsługi Studentów	**Centrum Praktyk Stydenckich z Biurem Karier**	Pracownicy działu	Drzwi otwierane są za pomocą Systemu Kontroli Dostępu, obsługiwanego kodem indywidualnym albo legitymacją pracowniczą
15.	ul. Czarnieckiego 16, budynek wydziału	**Wydział Ekonomii i Zarządzania**	Pracownicy sekretariatu, dziekani	Drzwi zamykane na klucz, szafki zamykane na klucz, klucze do pomieszczeń mogą pobierać tylko pracownicy instytutu
16.	ul. Czarnieckiego 16, budynek wydziału	**Wydział Ochrony Zdrowia**	Pracownicy sekretariatu, dziekani	Drzwi zamykane na klucz, szafki zamykane na klucz, klucze do pomieszczeń mogą pobierać tylko pracownicy wydziału
17.	ul. Czarnieckiego 16, budynek wydziału	**Wydział Inżynierii Technicznej**	Pracownicy sekretariatu, dziekani	Drzwi zamykane na klucz, szafki zamykane na klucz, klucze do pomieszczeń mogą pobierać tylko pracownicy wydziału
18.	ul. Pruchnicka 2, budynek wydziału	**Wydział Humanistyczny**	Pracownicy sekretariatu, dziekani	Drzwi zamykane na klucz, szafki zamykane na klucz, klucze do pomieszczeń mogą pobierać tylko pracownicy wydziału

19.	ul. Pruchnicka 2, budynek wydziału	**Wydział Stosunków Międzynarodowych**	Pracownicy sekretariatu, dziekani	Drzwi zamykane na klucz, szafki zamykane na klucz, klucze do pomieszczeń mogą pobierać tylko pracownicy wydziału
20.	ul. Czarnieckiego 16, budynek Biblioteki	**Studium Języków Obcych**	Pracownicy studium	Drzwi zamykane na klucz, szafki zamykane na klucz, klucze do pomieszczeń posiadają tylko pracownicy studium
21.	ul. Czarnieckiego 16, budynek Hali sportowej	**Studium Wychowania Fizycznego**	Pracownicy studium	Drzwi zamykane na klucz, szafki zamykane na klucz, klucze do pomieszczeń posiadają tylko pracownicy studium

Instrukcja zarządzania Systemami informatycznymi

–

Wykaz zabezpieczeń RODO

w Państwowej Akademii Nauk Stosowanych
im. ks. Bronisława Markiewicza w Jarosławiu

Spis treści

1. Wstęp

Instrukcja stanowi wykaz procedur oraz stosowanych środków technicznych i organizacyjnych mających na celu, zgodnie z Art. 32 RODO, zabezpieczyć przetwarzane dane osobowe przed: przypadkowym lub niezgodnym z prawem zniszczeniem, utratą, modyfikacją danych osobowych, nieuprawnionym ujawnieniem danych osobowych oraz nieuprawnionym dostępem do danych osobowych.

2. Zabezpieczenia fizyczne

1. zabezpieczono dostęp do kluczowej infrastruktury w postaci budynków/ pomieszczeń biurowych /archiwum/serwerowni, miejsc przechowywania kopii bezpieczeństwa,
2. funkcjonuje portiernia,
3. wdrożono zasadę dostępu osób nieupoważnionych do miejsc przetwarzania danych wyłącznie w obecności osoby upoważnionej (praca personelu sprzątającego w godzinach pracy i w obecności osób upoważnionych),
4. rozmieszczenie komputerów /drukarek ogranicza dostęp osób nieupoważnionych,
5. ograniczenie fizycznego dostępu do miejsc, gdzie znajdują się nienadzorowane gniazdka sieciowe (np. sale konferencyjne, korytarze),
6. krytyczne elementy infrastruktury zabezpieczono w zamykanych na klucz szafach serwerowych,
7. rozdzielnie elektryczne zabezpieczono w szafach zamykanych na klucz,
8. dostęp do pomieszczeń (w tym biurowych) zabezpieczono drzwiami zamykanymi na klucz,
9. dostęp do serwerowni zabezpieczono drzwiami podłaczonymi do systemu kontroli dostępu oraz zamykanymi na klucz,
10. dostęp do archiwum zabezpieczono drzwiami zamykanymi na klucz,
11. dostęp do dokumentacji/danych w pomieszczeniach zabezpieczono w zamkniętych metalowych szafach,
12. obiekt/pomieszczenia chronione są przez system monitorujący,
13. zapewniono ochronę obiektu - ochrona własna / firma ochroniarska,
14. stosowana jest Polityka kluczy.

3. Zabezpieczenia techniczne

1. Zastosowano UPS podtrzymujący zasilanie serwerowni oraz UPS dla kluczowych urządzeń sieciowych.
2. Zastosowano monitoring wizyjny w obrębie obiektu i w otoczeniu.
3. Serwerownia w CKA wyposażona w system automatycznego gaszenia pożaru w pozostałe pomieszczenia z infrastrukturą IT wyposażone w gaśnice.
4. Monitoring środowiskowy w serwerowni – czujnik temperatury.
5. Powiadamianie administratora systemu informatycznego o alertach temperatury.
6. Klimatyzacja w serwerowni.
7. Monitoring środowiskowy w archiwum – czujnik wilgotności.
8. Digitalizacja dokumentów archiwalnych.

4. Procedura nadawania uprawnień do przetwarzania danych osobowych.

Celem procedury jest minimalizacja ryzyka przetwarzania danych przez osoby nieupoważnione.

1. Dostęp do systemu informatycznego (np. stacji roboczej, dysku sieciowego, programu lub aplikacji, poczty elektronicznej) nadawany jest każdemu użytkownikowi w formie indywidualnego identyfikatora (loginu) oraz hasła.
2. Każdemu użytkownikowi uprzywilejowanemu (administratorowi) nadawane jest indywidualne konto administracyjne. Nadawanie uprawnień administratora wynika z zakresu czynności Działu Informatyki.
3. Nadawanie, zmiana, odbieranie uprawnień użytkownika do zasobów i aplikacji odbywa się na pisemne polecenie kierownika komórki organizacyjnej.
4. Za wykonanie czynności nadawania, zmiany, odbierania uprawnień użytkownikowi odpowiada administrator systemu informatycznego.

5. Obowiązuje zasada minimalizacji uprawnień.
6. Identyfikator użytkownika po wyrejestrowaniu z systemu informatycznego nie może być przydzielany innej osobie.
7. Użytkowników obowiązuje zasada pracy na własnym koncie. Zabronione jest umożliwianie innym osobom pracy na koncie innego użytkownika. Zasada ta obowiązuje również administratorów systemów
8. W przypadku pracy z uprawnieniami użytkownika uprzywilejowanego, każdy Administrator systemu zobowiązany jest do bieżącej pracy na koncie roboczym. Użycie tzw. konta administracyjnego (np. "root" lub "admin") dopuszczalne jest jedynie w sytuacjach awaryjnych lub podczas poważnych zmian wprowadzanych wadministrowanym systemie.

5. Metody i środki uwierzytelnienia

Celem procedury jest zapewnienie, że do systemów informatycznych przetwarzających dane osobowe mają dostęp jedynie osoby do tego upoważnione.

1. Pierwsze (pierwotne) hasło użytkownika nadawane jest przez Administratora i przekazywane mu w poufny sposób.
2. Obowiązuje polityka haseł opisana w Regulaminie Ochrony Danych.
3. Zastosowano mechanizm blokady dostępu po 10 próbach nieudanego logowania się.
4. Hasła administracyjne zdeponowane są w sejfie (lub w innym bezpiecznym miejscu).
5. W przypadku utraty uprawnień przez osobę administrującą systemem należy niezwłocznie zmienić hasła, do których miała dostęp.
6. W przypadkach awaryjnych (np. nieobecność administratora) hasło może być przekazane decyzją Kierownika Działu Informatyki osobie zastępującej administratora.
7. Po ustaniu sytuacji awaryjnej, Administrator jest zobowiązany do zmiany hasła.

6. Procedura tworzenia kopii zapasowych

1. Kopie zapasowe serwera (z zawartością plików i baz danych) tworzone są w sposób zautomatyzowany przez system informatyczny
2. Kopie tworzy się codziennie po godzinie 22:00
3. Kopie całościowe sporządzane zgodnie z regułami tworzenia kopii przyrostowych nie rzadziej, niż raz na miesiąć.
4. Dane z bazy danych, w formacie exportu są sporządzane, codzienie a raz na miesiąc zapisywane na nośniku optycznym.
5. Kopie są przechowywane na wydzielonym macierzach dyskowych.
6. Dział Informatyki sprawuje nadzór nad prawidłowością wykonania kopii zapasowych.
7. Niszczenie nośników z kopiami odbywa się komisyjnie. Nośniki niszczone są przez fizyczne zniszczenie.

7. Utylizacja elektronicznych nośników i wydruków oraz czyszczenie danych

1. Podlegające likwidacji uszkodzone lub przestarzałe nośniki a szczególności twarde dyski z danymi osobowymi ze stacji roboczych i laptopów/ pendrive /pamięci flash / dyski SSD / płyty DVD / telefony komórkowe / smartfony są niszczone w sposób fizyczny w tym również komisyjnie wg Załącznika- Protokół zniszczenia uszkodzonych nośników. Stosowana metoda niszczenia, to fizyczne niszczenie (pocięcie, nawiercenie, młotkowanie) wymontowanych nośników / użycie degaussera /zmielenie w specjalistycznej firmie potwierdzone protokołem zniszczenia lub certyfikatem bezpieczeństwa firmy utylizacyjnej lub nagraniem z procesu transportu i utylizacji.
2. Nośniki informacji zamontowane w sprzęcie IT a w szczególności twarde dyski muszą być wyczyszczone specjalistycznym oprogramowaniem zanim zostaną przekazane poza obszar organizacji (np. sprzedaż lub darowizna komputerów stacjonarnych/ laptopów/smartfonów).
3. Dokumentacja papierowa niszczona jest w niszczarkach.

8. Procedura zabezpieczenia systemu informatycznego

8.1. Ochrona przed nieautoryzowanym dostępem do sieci lokalnej

Stosowane zabezpieczenia mają na celu zabezpieczenie systemów informatycznych przed nieautoryzowanym dostępem do sieci lokalnej.

1. Dokonuje się aktualizacji oprogramowania (firmware / sterowniki) urządzeń sieciowych oraz innych (np. w urządzeniach jak: routery, switche, access pointy, firewalle, macierze, dyski NAS, drukarki, skanery, serwery)
2. Dokonywana jest konfiguracja urządzeń sieciowych oraz innych (routery, switche, access pointy, firewalle, macierze, dyski NAS, drukarki, skanery) w celu zabezpieczenia przed nieuprawnionym dostępem do nich (np. zmiana domyślnych haseł na urządzeniach, zmiana domyślnych nazw kont administratora w urządzeniach, konfiguracja portów na routerze).
3. Dokonuje się aktualizacji oprogramowania systemów i aplikacji (systemy operacyjne) na stacjach roboczych/ systemy operacyjne serwerów/przeglądarki www. Aktualizacja dokonywana jest zgodnie z zaleceniami producentów oraz opinią rynkową, co do bezpieczeństwa i stabilności nowych wersji (np. aktualizacje, service pack-i, łatki).
4. Monitoring usług sieciowych, np.: DHCP, DNS, SSH, htpp, SMTP, SNMP oraz utrzymuje się niezbędne usługi oraz dezaktywuje pozostałe.
5. Zastosowano system klasy EDR na serwerach i krytycznych stacjach roboczych.
6. Zastosowano system antywirusowy (na serwerach, na stacjach roboczych).
7. Zastosowano filtry antyspamowy.
8. Łacze do internetu jest zabezpieczone przez Firewall sprzętowy zintegrowany z routerem
9. Każdy serwer na zdefiniowane reguły filtrowania ruchu sieciowego by udostępniać tylko niezbędne usługi i porty .
10. Zastosowano mechanizmy kontroli dostępu do sieci w postaci IDS/IPS do wykrywania i blokowania ataków do sieci komputerowej, technikę NAT.
11. Sieć bezprzewodową zabezpieczono przez wymóg autoryzacji użytkownika.
12. Zabezpieczenie baz i katalogów webowych przed indeksacją wyszukiwarek.

8.2. Zabezpieczenia infrastruktury IT

1.
2. Serwery wyposażono w dwie macierze dyskowe pracujące w trybie mirroringu w celu ochrony danych osobowych przed skutkami awarii jednej macierzy i pojedynczego dysku.
3. Zastosowano wirtualizację serwerów.
4. Zastosowano redundantne serwery dla wirtualizacji.
5. Zastosowano blokadę zapisu na nośnikach wymiennych (USB, nośniki optyczne) na stacjach roboczych.
6. Dokonano dezaktywacji nieużywanych gniazd sieciowych (np. przez wypięcie przewodów lub wyłączenie portów na switchu).
7. Drukarki ogólnodostępne z funkcją kontroli odbioru wydruków (Karta elektroniczna lub PIN).
8. Na stacjach roboczych zastosowano „zahasłowane wygaszacze ekranu”, aktywowane po 5 minutach nieaktywności użytkownika.
9. Ustawienie monitorów uniemożliwiające wgląd w dane przez osoby postronne.

8.3. Zabezpieczenia aplikacji

1. Zapewniono rozliczalność operacji dla pracy w kluczowych aplikacjach / bazach / serwerach plików.
2. W ramach rozliczalności logowane są operacje tworzenia, zmiany (historii zmian), usuwania rekordu, wglądu w dane, eksportu danych do plików.
3. Zabezpieczono interfejsy programistyczne poprzez zmianę domyślnych loginów i haseł/ wyłączenie dostępu zdalnego, gdy nie jest wymagany.
4. Zabezpieczenie testowych wersji aplikacji poprzez zmianę domyślnych loginów i haseł/ wyłączenie dostępu zdalnego, gdy nie jest wymagany.
5. W kluczowych aplikacjach stosuje się terminację sesji.

6. Dla aplikacji webowych stosowane jest szyfrowanie połączeń internetowych z użyciem protokołu SSL.
7. Formularze kontaktowe na stronach www zabezpieczono protokołem SSL.

9. Procedura naprawy w serwisach zewnętrznych.

1. Dział Informatyki odpowiada za sprawdzenie poprawności działania systemu IT, w tym: stacji roboczych, serwerów, drukarek, baz danych, aplikacji, poczty elektronicznej.
2. Dział Informatyki odpowiada za identyfikację i przyjmowanie zgłoszeń o nieprawidłowościach w działaniu systemu informatycznego oraz oprogramowania celem ich niezwłocznego usunięcia.
3. W przypadku napraw dokonywanych na zewnątrz (z komputerów należy uprzednio wymontować dyski i wszelkie nośniki, z urządzeń mobilnych karty pamięci, usunąć dane z nośnika z użyciem specjalistycznego oprogramowania).
4. W przypadku naprawy sprzętu z danymi osobowymi na nośniku - rekomendowane jest zawarcie specjalnego zapisu w umowie serwisowej, gwarantującego bezpieczną naprawę (należy na to zwrócić uwagę przy zakupach sprzętu).
5. W przypadku naprawy sprzętu z danymi osobowymi na nośniku - rekomendowane jest przekazywanie do naprawy uszkodzonego sprzętu z danymi zaszyfrowanymi na dysku / karcie pamięci. Sprzęt przekazywany jest do serwisu bez podania hasła.
6. Rekomendowane jest korzystanie z serwisu, który dokonuje napraw u klienta (umowy gwarancyjne on-site).
7. Czynności konserwacyjne i naprawcze wykonywane przez osoby nieposiadające upoważnień do przetwarzania danych (np. specjalistów z firm zewnętrznych) muszą być wykonywane pod nadzorem osób upoważnionych.
8. Wszelkie prace konserwacyjne i naprawcze sprzętu komputerowego oraz uaktualnienia systemu informatycznego wykonywane przez podmiot zewnętrzny, powinny odbywać się na zasadach określonych w szczegółowej umowie z uwzględnieniem klauzuli dotyczącej ochrony danych.

10.Procedura wykonywania przeglądów i konserwacji

1. Stosowany jest system wykrywania słabości i zagrożeń (Skanery podatności).
2. Stosowany jest system do monitoringu aktywności użytkowników.
3. Dział Informatyki jest odpowiedzialny za monitoring/przegląd logów aktywności aplikacji/baz.
4. Dział Informatyki jest odpowiedzialny za monitoring/przegląd logów aktywności oraz uprawnień użytkowników i administratorów.
5. Dział Informatyki odpowiada za optymalizację zasobów serwerowych, wielkości pamięci i dysków pamięci, optymalizację baz danych.
6. Dział Informatyki odpowiada za sprawdzanie poprawności działania systemu IT w tym: stacji roboczych, serwerów, drukarek, baz danych, aplikacji, poczty email.
7. Dział Informatyki odpowiada za identyfikację i przyjmowanie zgłoszeń o nieprawidłowościach w działaniu systemu informatycznego oraz oprogramowania celem ich niezwłocznego usunięcia.