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.

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.						

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

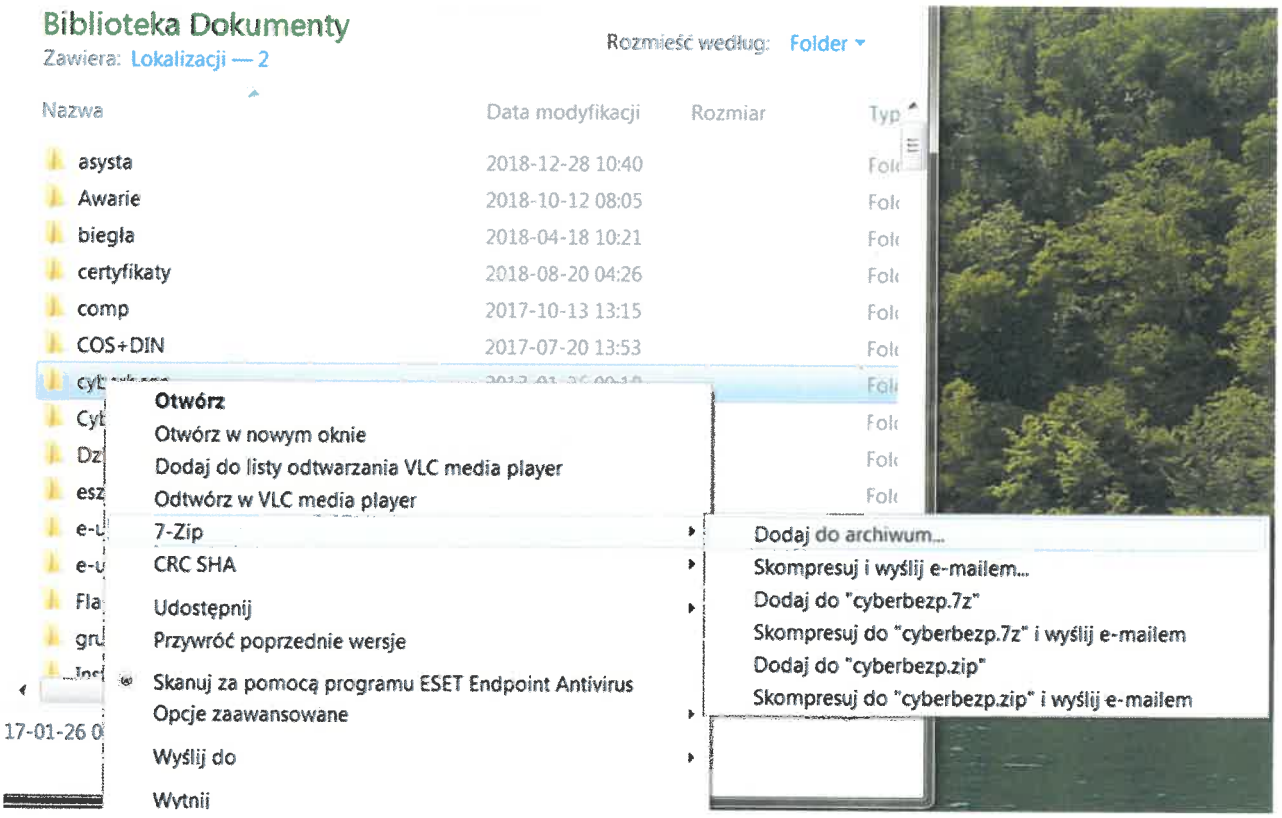
1. Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu potraktowane będą, jako ciężkie naruszenie obowiązków pracowniczych lub naruszenie zasad współpracy.
2. Postępowanie sprzeczne z powyższymi zobowiązaniami, może też być uznane przez pracodawcę/zleceniodawcę za naruszenie 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**.

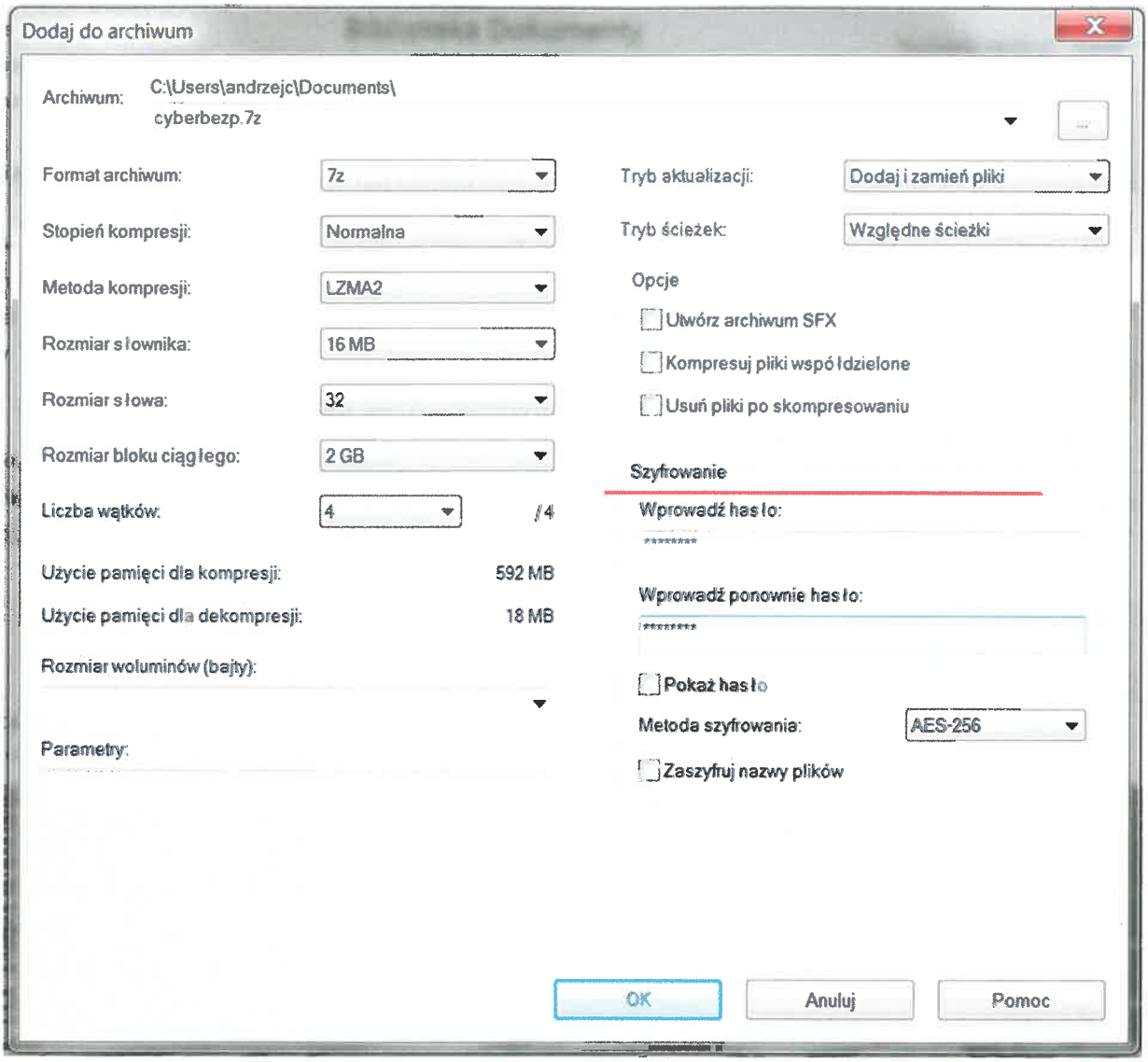
Do szyfrowania należy użyć darmowego programu 7-zip (*do pobrania z strony https://www.7-zip.org/*).

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*".

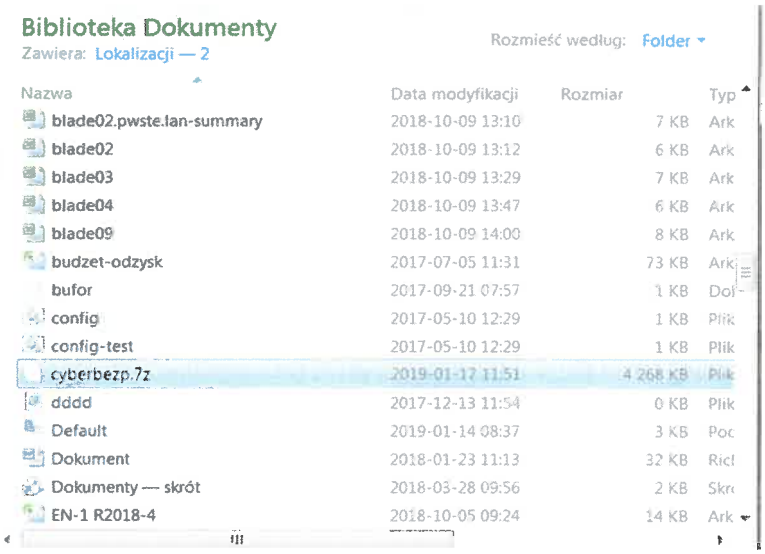


   - otworzy się okno programu „7-zip", gdzie w sekcji „Szyfrowanie" należy wpisać hasło. Hasło powinno mieć co najmniej 10 znaków dobranych losowo (nie powinno się używać nazw związanych z nazwą instytucji, nazwiskiem nadawcy lub odbiorcy).

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.

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.

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.