Wyższa Szkoła Ekonomiczna
w Białymstoku
15-703 Białystok, ul. Zwycięstwa 14/3
tel./fax (85) 652-00-24, tel. (85) 652-09-97
REGON 050383717, NIP 542-17-21-665

Zarządzenie nr 15 /2019
Rektora Wyższej Szkoły Ekonomicznej w Białymstoku
z dnia 30 września 2019 r.

w sprawie zmiany Polityki Ochrony Danych Osobowych w Wyższej Szkole Ekonomicznej w Białymstoku

Na podstawie art. 23 ust. 1 ustawy z 20 lipca 2018 r. Prawo o szkolnictwie wyższym i nauce (Dz. U. z 2018 r. poz. 1668) oraz Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (Dz. U. UE. L. 119/1 z dnia 4 maja 2016 r.) zwanego dalej RODO oraz Ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych, (Dz. U. z 2018 r., poz. 1000), zarządzam, co następuje:

§ 1

Wprowadza się dokument **Polityka Ochrony Danych Osobowych w Wyższej Szkole Ekonomicznej w Białymstoku którego integralną część stanowią załączniki Nr 1-11**,

§ 2

Dokument, o którym mowa w § 1 ma zastosowanie na wszystkich stanowiskach pracy i innych miejscach, w których przetwarzane są dane osobowe w Wyższej Szkole Ekonomicznej w Białymstoku **i jej jednostkach organizacyjnych.**

§ 3

Zobowiązuje się kierowników jednostek organizacyjnych do zapoznania pracowników zatrudnionych w danej jednostce przy przetwarzaniu danych osobowych oraz pracujących w systemach informatycznych z treścią wprowadzonej **Polityki Ochrony Danych Osobowych w Wyższej Szkole Ekonomicznej w Białymstoku, a w szczególności z** treścią załącznika **Nr 8** ***Instrukcja Zarządzania RODO – Wykaz zabezpieczeń RODO*** oraz **Nr 9** ***Regulamin Ochrony Danych Osobowych*** do dokumentu Polityka Ochrony Danych Osobowych.

§ 4

W związku z wprowadzeniem niniejszego Zarządzenia, z dniem 30.09.2019 r. traci moc obowiązującą *Zarządzenie Nr 16/2018 Rektora Wyższej Szkoły Ekonomicznej w Białymstoku z dnia 31 sierpnia 2018 roku w sprawie wprowadzenia przepisów wewnętrznych regulujących zagadnienia ochrony danych osobowych oraz pracy w systemach informatycznych służących do przetwarzania danych osobowych w Wyższej Szkole Ekonomicznej w Białymstoku.*

§ 5

Zarządzenie wchodzi w życie z dniem 01.10.2019 r.

REKTOR
dr Aleksander Prokopiuk
Rektor

Wyższa Szkoła Ekonomiczna
w Białymstoku
15-703 Białystok, ul. Zwycięstwa 14/3
tel./fax (85) 652-00-24, tel. (85) 652-09-97
REGON 050383717, NIP 542-17-21-656

Polityka Ochrony Danych Osobowych w Wyższej Szkole Ekonomicznej w Białymstoku

1 WSTĘP

Polityka Ochrony Danych Osobowych jest dokumentem opisującym zasady ochrony danych osobowych stosowane przez Wyższą Szkołę Ekonomiczną w Białymstoku, administratora danych osobowych, zwaną dalej Administratorem, w celu spełnienia wymagań Rozporządzenia PE i RE 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych (RODO).

Polityka stanowi jeden ze środków organizacyjnych, mających na celu wykazanie, że przetwarzanie danych osobowych odbywa się zgodnie z powyższym Rozporządzeniem.

2 ANALIZA RYZYKA

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

Przyjęto, że analiza ryzyka przeprowadzana jest dla zbiorów danych osobowych (kategorii osób)

2.1 DEFINICJE

1. Aktywa – środki materialne i niematerialne mające wpływ na przetwarzanie danych osobowych
2. Naruszenie (Incydent) ochrony danych osobowych - to 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
3. Zagrożenie - potencjalne naruszenie (potencjalny incydent)
4. Skutki - rezultaty niepożądanego incydentu (straty w wypadku wystąpienia zagrożenia)
5. Ryzyko - prawdopodobieństwo, że określone zagrożenie wystąpi i spowoduje straty lub zniszczenie aktywów

2.2 REJESTR CZYNNOŚCI PRZETWARZANIA (INWENTARYZACJA DANYCH OSOBOWYCH)

Wyższa Szkoła Ekonomiczna w Białymstoku, administrator danych osobowych, jest zobowiązana zgodnie z art. 30 RODO do prowadzenia rejestru czynności przetwarzania. Rejestr stanowi podstawę do przeprowadzenia analizy ryzyka.

1. Administrator prowadzi rejestr zgodnie z załącznikiem Rejestr czynności przetwarzania (wykaz zbiorów danych osobowych) - załącznik Nr 1.
2. Podmiot przetwarzający prowadzi rejestr zgodnie z Rejestr czynności prowadzony przez podmiot przetwarzający (Rejestr kategorii przetwarzania) - załącznik Nr 2.

2.3 WYZNACZENIE ZAGROŻEŃ

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.

2.4 WYLICZENIE RYZYKA DLA ZAGROŻEŃ

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

2.4.1 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

2.4.2 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 Arkusz analizy ryzyka RODO - załącznik Nr 3

2.4.3 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)

2.5 PLAN POSTĘPOWANIA Z RYZYKIEM

1. Wszędzie, gdzie Administrator decyduje się obniżyć ryzyko, wyznacza listę zabezpieczeń do wdrożenia, termin realizacji i osoby odpowiedzialne, patrz Plan postępowania z ryzykiem - załącznik Nr 4
2. Administrator zobowiązany jest do monitorowania wdrożenia zabezpieczeń

3 UPOWAŻNIENIA

1. Administrator odpowiada za nadawanie / anulowanie upoważnień do przetwarzania danych w zbiorach (dla kategorii osób) w postaci papierowej oraz w systemach informatycznych.
2. Każda osoba upoważniona musi przetwarzać dane wyłącznie na polecenie administratora lub na podstawie przepisu prawa.
3. Upoważnienie do przetwarzania danych osobowych zawiera zakres nadawanych uprawnień do przetwarzania danych osobowych określonych stanowiskiem pracy lub zakresem obowiązków i czynności, do którego nadawane są uprawnienia, datę nadania upoważnienia oraz, jeśli upoważnienie nadawane jest terminowo, datę wygaśnięcia upoważnienia lub warunków jego wygaśnięcia. Patrz załącznik - Upoważnienie do przetwarzania danych osobowych - załącznik Nr 5
4. Administrator prowadzi rejestr osób upoważnionych w celu sprawowania kontroli nad prawidłowym dostępem do danych osób upoważnionych. Rejestr ma charakter pomocniczy i nie jest wymagany przepisami RODO, patrz załącznik - Rejestr osób upoważnionych - załącznik Nr 6
5. W przypadku powierzenia przetwarzania danych do Podmiotu przetwarzającego, Administrator jest zobowiązany do sporządzenia z nim umowy powierzenia, stanowiącą podstawę upoważnienia dla osób z Podmiotu przetwarzającego, patrz załącznik - Umowa powierzenia uniwersalna Wzór - załącznik Nr 7

4 ŚRODKI TECHNICZNE I ORGANIZACYJNE ZABEZPIECZAJĄCE DANE OSOBOWE

1. Administrator prowadzi wykaz zabezpieczeń, które stosuje w celu ochrony danych osobowych, patrz załącznik - Instrukcja zarządzania RODO - załącznik Nr 8 .
2. W instrukcji wskazano stosowane zabezpieczenia proceduralne oraz zabezpieczenia jako środki techniczne i organizacyjne.

3. Instrukcja jest aktualizowana, jeśli zajdzie taka potrzeba po przeprowadzeniu analizy ryzyka.

5 Regulamin Ochrony Danych Osobowych

Regulamin ma na celu zapewnienie wiedzy osobom przetwarzającym dane osobowe odnośnie bezpiecznych zasad przetwarzania, patrz załącznik - Regulamin Ochrony Danych Osobowych - załącznik Nr 9.

Po zapoznaniu się z zasadami ochrony danych osobowych, osoby zobowiązane są do potwierdzenia znajomości tych zasad i deklaracji ich stosowania poprzez podpisanie Oświadczenia o poufności - załącznik Nr 10 .

6 Instrukcja postępowania z incydentami

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 Inspektora Ochrony Danych.
2. Do typowych sytuacji powodujących wzrost podatności na zagrożenie 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 administratorów systemów informatycznych, 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 lub 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, patrz załącznik - Formularz rejestracji incydentu - załącznik Nr 11
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.

REKTOR

dr Aleksander Prokopiuk

Wyższa Szkoła Ekonomiczna
w Białymstoku
15-703 Białystok, ul. Zwycięstwa 14/3
tel./fax (85) 652-00-24, tel. (85) 652-09-97
REGON 050383717, NIP 542-17-21-656

Załącznik Nr 1

do dokumentu Polityka Ochrony danych osobowych w Wyższej Szkole Ekonomicznej w Białymstoku

Rejestr czynności przetwarzania jako Wykaz zbiorów danych osobowych

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/imiona i nazwisko, dane o wykształceniu, stażu pracy, uprawnieniach zawodowych, dane kontaktowe wskazane przez kandydata **2. Cele przetwarzania** Rekrutacja pracowników	**1. Informacje (dokumentacja papierowa)** CV, kwestionariusz osobowy dla osoby ubiegającej się o zatrudnienie **2. Programy i systemy operacyjne** Windows, Microsoft Office, Serwery usługowe (WWW, poczta, serwery plików), pliki z danymi kandydatów, **3. Infrastruktura IT** Serwery, stacje robocze, przełączniki	1. Przesłanie CV mailem na adres wse@wse.edu.pl 2. Złożenie CV w sekretariacie lub u kierownika odpowiedniej jednostki organizacyjnej 3. Wyłonienie kandydata 4. Przekazanie CV do działu kadr celem skierowania na badania lekarskie oraz celem zatrudnienia

3. Kategorie odbiorców Brak **4. Kategorie odbiorców w państwach trzecich** lub w organizacjach międzynarodowych – brak **5. Planowane terminy usunięcia poszczególnych kategorii danych** W przypadku udzielonej zgody na bieżącą rekrutację – czas przechowywania 2 miesiące, w przypadku udzielonej zgody kandydatów na przyszłe rekrutacje – czas przechowywania określono na 1 rok **6. Opis technicznych i organizacyjnych środków bezpieczeństwa** Patrz: Instrukcja zarządzania RODO, Regulamin ODO **7. Podstawa prawna przetwarzania** RODO: Art.6, ust 1, lit. a (na podst. zgody osoby) RODO:Art.6, lit. c (przepis prawa). Kodeks pracy art. 22^1	sieciowe, routery, drukarki, skanery, kserokopiarki, centrala telefoniczna, strukturalna sieć LAN (okablowanie, gniazda, patchpanele, krosownice) **4. Infrastruktura** Pomieszczenia działu kadr, Sekretariat, Pomieszczenia Kierowników jednostek organizacyjnych **5. Pracownicy i współpracownicy** Pracownik działu kadr, Administratorzy SI, Sekretarka, Kierownicy jednostek organizacyjnych **6. Outsourcing** BIAMAN Politechnika Białostocka–dostawca Internetu	4. Usunięcie CV po wymaganym czasie w przypadku niezatrudnienia 5. Złożenie kwestionariusza osobowego dla przez kandydata do pracy
1. Opis kategorii osób (nazwa zbioru) ***Pracownicy etatowi, umowy zlecenia, umowy o dzieło*** **1.a Opis kategorii danych osobowych** Dane identyfikacyjne, dane adresowe, dane o Oddziale NFZ, dane członków rodziny (w przypadku zgłoszenia do ubezpieczenia zdrowotnego lub korzystania z opieki lub zasiłków opiekuńczych), wysługa lat pracy, dane o wykształceniu, stawka wynagrodzenia, dane o czasie pracy, przyznanych nagrodach, potrąceniach, zajęcia komornicze, numery kont dla przelewów bankowych pracownika, stopniu niepełnosprawności, wizerunek pracownika (w przypadku udzielenia zgody) **2. Cele przetwarzania** Zatrudnianie pracowników i spełnienie obowiązków prawnych z tym związanych **3. Kategorie odbiorców** Medycyna pracy, ZUS, US i inne podmioty przewidziane przepisami prawa **4. Kategorie odbiorców w państwach trzecich** lub w organizacjach międzynarodowych – brak **5. Planowane terminy usunięcia poszczególnych kategorii danych** 50 lub 10 lat [art. 94 9b)[9] Kodeksu pracy, art. 51 u ustawy o narodowym zasobie archiwalnym i archiwach (Dz. U. z 2018 r., poz. 217 ze zm.)]oraz art.125 e ust. 4 ustawy o emeryturach i rentach z Funduszu Ubezpieczeń Społecznych (Dz. U. z 2018 r. poz. 1270 ze zm.) **6. Opis technicznych i organizacyjnych środków bezpieczeństwa** Patrz: Instrukcja zarządzania RODO, Regulamin ODO **7. Podstawa prawna przetwarzania** RODO: Art. 6, ust 1, lit. a (za zgodą pracowników) ubezpieczenie grupowe pracowników, wykorzystanie wizerunku wizerunku w mediach społecznościowych lub na stronie www w celu działań promocyjno-marketingowych	**1. Informacje (dokumentacja papierowa)** Kwestionariusz osobowy dla pracownika, Akta osobowe, Dokumentacja BHP, Dokumentacja czasu pracy, Dokumentacja wynagrodzenia, Oświadczenie osoby świadczącej pracę na podstawie umowy zlecenia lub dzieło, umowa zlecenie lub dzieło i inna dokumentacja z tym związana **2. Programy i systemy operacyjne** Windows, Microsoft Office, Serwery usługowe (WWW, poczta, serwery plików, bazy danych), Systemy: POL-on, USOS, Płatnik, PFRON - SODIR, pliki z danymi pracowników, System Płace, Finansowo-Księgowy Tytan SQL ETOB **3. Infrastruktura IT** Serwery, stacje robocze, przełączniki sieciowe, routery, AP, kontroler AP, laptopy, drukarki, skanery, kserokopiarki, centrala telefoniczna, strukturalna sieć LAN (okablowanie, gniazda, patchpanele, krosownice) **4. Infrastruktura** Pomieszczenia działu kadr, Kwestura, Serwerownia, Archiwum **5. Pracownicy i współpracownicy** Pracownik kadr, Pracownik płac, Kwestor, Administratorzy SI, Sekretarka, Kierownicy jednostek organizacyjnych, Prorektorzy **6. Outsourcing** ETOB dostawca oprogramowania i wsparcia technicznego - System Finansowo-Księgowy, Płace, Tytan SQL ETOB Umowa powierzenia - Firma ubezpieczeniowa (ubezpieczenia grupowe dobrowolne) BIAMAN Politechnika Białostocka–dostawca Internetu Kancelaria Prawna – umowa o obsługę prawną	1. Zaprowadzenie akt osobowych i innej dokumentacji zatrudnieniowej 2. Wprowadzenie danych do systemu kadrowo –płacowego, USOS, POLON 3. Rozliczanie czasu pracy pracowników 4. Rozliczanie pracowników z ZUS oraz z US, wypłaty wynagrodzenia, organizacja wyjazdów służbowych, ubezpieczenia społecznego, ubezpieczenia chorobowego, ubezpieczenia grupowego pracowników, prowadzenie dokumentacji dot. dofinansowania do wynagrodzeń z PFRON 5. Przekazanie do Archiwum

RODO: Art.6, lit. c (przepis prawa). Kodeks pracy art. 22^1 i odpowiednie rozporządzenia, Ustawa o systemie ubezpieczeń społecznych, Ustawa o podatku dochodowym od osób fizycznych) RODO: Art.6, lit. b (realizacja umowy) umowy o pracę, umowy zlecenia, umowy o dzieło RODO: Art.6, ust.1 lit. d – (prawnie uzasadniony interes realizowany przez administratora) – ewentualne dochodzenie i odpieranie roszczeń, monitoring wizyjny)		
1. Opis kategorii osób (nazwa zbioru) ***Kandydaci na studia*** **1.a Opis kategorii danych osobowych** Dane identyfikacyjne, dane adresowe, dane kontaktowe, dane o wykształceniu **2. Cele przetwarzania** Nabór i rekrutacja na studia wyższe **3. Kategorie odbiorców** Podmioty uprawnione na podstawie przepisów prawa lub inne podmioty publiczne w oparciu o stosowną podstawę prawną **4. Kategorie odbiorców w państwach trzecich** lub w organizacjach międzynarodowych– brak **5. Planowane terminy usunięcia poszczególnych kategorii danych** W przypadku osób przyjętych na studia - przeniesienie do teczki akt osobowych studenta, w przypadku osób nieprzyjętych – po zakończeniu rekrutacji. **6. Opis technicznych i organizacyjnych środków bezpieczeństwa** Patrz: Instrukcja zarządzania RODO, Regulamin ODO **7. Podstawa prawna przetwarzania** RODO: Art.6, ust 1, lit. a (na podst. zgody kandydata) RODO: Art.6, ust 1, lit. c (przepis prawa) - Ustawa Prawo o szkolnictwie wyższym i nauce oraz odpowiednie rozporządzenia	**1. Informacje (dokumentacja papierowa)** Podanie o przyjęcie na studia **2 . Programy i systemy operacyjne** Windows, Microsoft Office, Serwery usługowe (WWW, poczta, serwery plików, bazy danych), System IRK, pliki z danymi kandydatów, System Finansowo-Księgowy Tytan SQL ETOB **3. Infrastruktura IT** Serwery, stacje robocze, przełączniki sieciowe, routery, drukarki, skanery, kserokopiarki, centrala telefoniczna, strukturalna sieć LAN (okablowanie, gniazda, patchpanele, krosownice) **4. Infrastruktura** Pomieszczenia działu spraw studenckich, Sekretariat **5. Pracownicy i współpracownicy** Pracownicy Działu Spraw Studenckich, Administratorzy SI, Prorektorzy, Kwestor, pracownicy Kwestury **6. Outsourcing** BIAMAN Politechnika Białostocka– dostawca Internetu	1. Złożenie podania w dziale spraw studenckich lub pocztą mailową 2. Rejestracja w systemie Internetowa Rejestracja Kandydatów, 4.Wpłata wpisowego 3. Usunięcie, w przypadku nieprzyjęcia na studia, po zakończenia rekrutacji
1. Opis kategorii osób (nazwa zbioru) ***Studenci*** **1.a Opis kategorii danych osobowych** Dane identyfikacyjne, dane adresowe, dane kontaktowe, dane o wykształceniu, dane o postępach w nauce, dane o statusie, członkach rodziny, sytuacji materialnej, stopniu niepełnosprawności, dane o rachunku bankowym studenta, wizerunek studenta (do celów marketingowych w przypadku uzyskania zgody) **2. Cele przetwarzania** Realizacja umowy o świadczenie usług edukacyjnych w ramach studiów wyższych,, dokumentacja przebiegu studiów, spełnienie obowiązków informacyjnych, archiwizacyjnych, statystycznych, informowanie o przebiegu kształcenia, zawarcie umowy ubezpieczenia, korzystanie z funduszu pomocy materialnej dla studentów, zgłoszenie do ubezpieczenia zdrowotnego studenta, rozliczanie płatności, ewentualne dochodzenie i odpieranie roszczeń	**1. Dokumentacja papierowa** Teczka akt osobowych studenta, decyzje administracyjne, umowa o kształcenie, dokumentacja związana z ubieganiem się i otrzymaniem stypendium socjalnego/osób niepełnosprawnych, faktura, dokumentacja windykacyjna, sądowa **2 . Programy i systemy operacyjne** Windows, Microsoft Office, Serwery usługowe (WWW, poczta, serwery plików, bazy danych), Systemy: POL-on, NAVA, USOS, Płatnik, pliki z danymi studentów, Email, System Finansowo-Księgowy Tytan SQL ETOB **3. Infrastruktura IT** Serwery, stacje robocze, przełączniki sieciowe, routery, AP, kontroler AP, laptopy, drukarki, skanery, kserokopiarki, centrala telefoniczna, strukturalna sieć LAN (okablowanie, gniazda, patchpanele, krosownice) **4. Infrastruktura** Pomieszczenia Działu spraw studenckich,	1. Podpisanie umowy 2. Zaprowadzenie teczek osobowych studenta i innej dokumentacji związanej z procesem kształcenia 2. Wprowadzanie danych do systemu USOS 3. Wprowadzanie danych do systemu POL-on, NAVA 4. Zaprowadzenie dokumentacji stypendialnej, przesyłanie środków z funduszu pomocy materialnej dla studentów na rachunek bankowy studenta 5. Prowadzenie dokumentacji odbywanych praktyk zawodowych, zawarcie umowy ubezpieczenia 6. Rozliczanie płatności, wystawianie faktur, windykacja należności, rozstrzyganie spraw spornych 7. Przekazanie do Archiwum

3. Kategorie odbiorców Podmioty uprawnione na podstawie przepisów prawa: Ministerstwo nauki i szkolnictwa wyższego, ZUS, Kancelaria Prawna, Firma ubezpieczeniowa, WKU, Straż Graniczna i inne podmioty publiczne na podstawie stosownych podstaw prawnych, ewentualnie kancelaria prawna, firma windykacyjna **4. Kategorie odbiorców w państwach trzecich** lub w organizacjach międzynarodowych – brak **5. Planowane terminy usunięcia poszczególnych kategorii danych** - teczkę akt osobowych studenta przechowuje się 50 lat przepis prawa - ustawa Prawo o szkolnictwie wyższym i nauce - wizerunek do celów marketingowych - do czasu obowiązywania zgody lub jej wycofania - ewentualnie do zaspokojenia lub przedawnienia roszczeń **6. Opis technicznych i organizacyjnych środków bezpieczeństwa** Patrz: Instrukcja zarządzania RODO, Regulamin ODO **7. Podstawa prawna przetwarzania** RODO: Art.6, ust 1, lit. a (na podst. zgody osoby) - wizerunek studenta do celów marketingowych RODO: Art.6, ust 1, lit. b (realizacja umowy) - umowa o świadczenie usług edukacyjnych w ramach studiów wyższych, umowa ubezpieczenia - dane identyfikacyjne, dane adresowe, dane kontaktowe, dane o wykształceniu RODO: Art.6, ust 1, lit. c (przepis prawa) - Ustawa Prawo o szkolnictwie wyższym i nauce oraz odpowiednie rozporządzenia, Ustawa o systemie ubezpieczeń społecznych – spełnienie obowiązków informacyjnych, archiwizacyjnych, statystycznych, informowanie o przebiegu kształcenia, zgłoszenie do ubezpieczenia zdrowotnego, udzielenie pomocy z funduszu pomocy materialnej (dane o statusie, członkach rodziny, sytuacji materialnej, stopniu niepełnosprawności, dane o rachunku bankowym) RODO: Art.6, ust.1 lit. d – (prawnie uzasadniony interes realizowany przez administratora) - ewentualna windykacja należności, rozstrzyganie spraw spornych, monitoring wizyjny	Kwestura, Pomieszczenie pełnomocnika ds. praktyk studenckich, Serwerownia, Archiwum **5. Pracownicy i współpracownicy** Pracownicy Działu Spraw Studenckich, Pełnomocnik ds. praktyk studenckich, Księgowe, Administratorzy SI, Nauczyciele akademiccy **6. Outsourcing** ETOB dostawca oprogramowania i wsparcia technicznego - System Finansowo-Księgowy Tytan SQL ETOB BIAMAN Politechnika Białostocka– dostawca Internetu Kancelaria Prawna – umowa o obsługę prawną Personalizowanie legitymacji studenckich - umowa Politechnika Białostocka Uniwersytet im. A. Mickiewicza w Poznaniu – dostawca oprogramowania USOS Poczta Polska - w zakresie adresu	
1. Opis kategorii osób *Kandydaci na studia podyplomowe* **1.a Opis kategorii danych osobowych** Dane identyfikacyjne, dane adresowe, dane kontaktowe, dane o wykształceniu, dane o miejscu pracy **2. Cele przetwarzania** Nabór i rekrutacja na studia podyplomowe **3. Kategorie odbiorców** Podmioty uprawnione na podstawie przepisów prawa lub inne podmioty publiczne w oparciu o stosowną podstawę prawną	**1. Informacje (dokumentacja papierowa)** Podanie o przyjęcie na studia podyplomowe **2. Programy i systemy operacyjne** Windows, Microsoft Office, Serwery usługowe (WWW, poczta, serwery plików, bazy danych), pliki z danymi kandydatów, System Finansowo-Księgowy Tytan SQL ETOB **3. Infrastruktura IT** Serwery, stacje robocze, przełączniki sieciowe, routery, drukarki, skanery,	1. Złożenie podania w pomieszczeniu pełnomocnika rektora ds. studiów podyplomowych lub pocztą mailową 2.Wpłata wpisowego 3. Usunięcie, w przypadku nieprzyjęcia na studia, po zakończenia przewidzianego okresu

4. Kategorie odbiorców w państwach trzecich lub w organizacjach międzynarodowych - brak **5. Planowane terminy usunięcia poszczególnych kategorii danych** W przypadku przyjęcia na studia podyplomowe przeniesienie do teczki akt osobowych słuchacza W przypadku nieprzyjęcia - 1 rok po zakończeniu rekrutacji (o ile uzyskana została zgoda na przetwarzanie do celów przyszłej rekrutacji) **6. Opis technicznych i organizacyjnych środków bezpieczeństwa** Patrz: Instrukcja zarządzania RODO, Regulamin ODO **7. Podstawa prawna przetwarzania** RODO: Art.6, ust 1, lit. a (na podst. zgody kandydata) RODO: Art.6, ust 1,lit. c (przepis prawa) - Ustawa Prawo o szkolnictwie wyższym i nauce oraz odpowiednie rozporządzenia	kserokopiarki, centrala telefoniczna, strukturalna sieć LAN (okablowanie, gniazda, patchpanele, krosownice) Laptopy, Smartfony **4. Infrastruktura** Pomieszczenie Pełnomocnika Rektora ds. studiów podyplomowych, Kwestura, **5. Pracownicy i współpracownicy** Pełnomocnik Rektora ds. studiów podyplomowych, Księgowe Informatycy/ Administratorzy SI **6. Outsourcing** brak	
1. Opis kategorii osób *Słuchacze studiów podyplomowych* **1.a Opis kategorii danych osobowych** Dane identyfikacyjne, dane adresowe, dane kontaktowe, dane o wykształceniu, rachunku bankowym słuchacza, dane o miejscu pracy **2. Cele przetwarzania** Realizacja umowy o świadczenie usług edukacyjnych w ramach studiów podyplomowych, dokumentowanie przebiegu studiów podyplomowych, spełnienie obowiązków informacyjnych, archiwizacyjnych, statystycznych, informowanie o przebiegu kształcenia, Ewentualne dochodzenie i odpieranie roszczeń **3. Kategorie odbiorców** Podmioty uprawnione na podstawie przepisów prawa lub inne podmioty publiczne w oparciu o stosowną podstawę prawną Drukarnia – drukowanie świadectw ukończenia studiów, Ewentualnie kancelaria prawna, firma windykacyjna **4. Kategorie odbiorców w państwach trzecich** lub w organizacjach międzynarodowych– brak **5. Planowane terminy usunięcia poszczególnych kategorii danych** - na podstawie przepisów prawa (ustawa Prawo o szkolnictwie wyższym i nauce Teczka akt osobowych słuchacza przechowuje się 50 lat - ewentualnie do zaspokojenia lub przedawnienia roszczeń **6. Opis technicznych i organizacyjnych środków bezpieczeństwa** Patrz: Instrukcja zarządzania RODO, Regulamin ODO **7. Podstawa prawna przetwarzania** RODO: Art.6, ust 1,lit. c (przepis prawa) - Ustawa Prawo o szkolnictwie wyższym i nauce oraz odpowiednich rozporządzeń RODO: Art.6, ust 1, lit. b (realizacja umowy) -	**1. Informacje (dokumentacja papierowa)** Umowa o kształcenie na studiach podyplomowych, teczka akt osobowych słuchacza faktura, dokumentacja windykacyjna **2. Programy i systemy operacyjne** Windows, Microsoft Office, Serwery usługowe (WWW, poczta, serwery plików, bazy danych), Systemy USOS, pliki z danymi słuchaczy, System Finansowo-Księgowy Tytan SQL ETOB **3. Infrastruktura IT** Serwery, stacje robocze, przełączniki sieciowe, routery, AP, kontroler AP, laptopy, drukarki, skanery, kserokopiarki, centrala telefoniczna, strukturalna sieć LAN (okablowanie, gniazda, patchpanele, krosownice) **4. Infrastruktura** Pomieszczenie Pełnomocnika Rektora ds. studiów podyplomowych, Pomieszczenie kadr, Kwestura, Archiwum **5. Pracownicy i współpracownicy** Pełnomocnik Rektora ds. studiów podyplomowych, Księgowe Informatycy/ Administratorzy SI, Nauczyciele akademiccy, Wykładowcy **6. Outsourcing** ETOB dostawca oprogramowania i wsparcia technicznego - System Finansowo-Księgowy Tytan SQL ETOB BIAMAN Politechnika Białostocka– dostawca Internetu Kancelaria Prawna – umowa o obsługę prawną Drukowanie legitymacji studenckich - umowa Politechnika Białostocka Uniwersytet im. A. Mickiewicza w Poznaniu – dostawca oprogramowania USOS Drukarnia- drukowanie świadectw, umowa powierzenia Poczta Polska - w zakresie adresu	1. Podpisanie umowy 2. Zaprowadzenie teczek osobowych słuchacza i innej dokumentacji związanej z procesem kształcenia 2. Wprowadzanie danych do systemu USOS 3. Rozliczanie płatności, wystawianie faktur, windykacja należności, ewentualne dochodzenie i odpieranie roszczeń 7. Przekazanie do Archiwum

umowa o świadczenie usług edukacyjnych w ramach studiów podyplomowych RODO: Art.6, ust.1 lit. d – (prawnie uzasadniony interes realizowany przez administratora) - ewentualna windykacja należności, rozstrzyganie spraw spornych, monitoring wizyjny		
1. Opis kategorii osób ***Nabór i rekrutacja do szkoły podstawowej*** **1.a Opis kategorii danych osobowych** Dane kandydatów, rodziców/ opiekunów prawnych: dane identyfikacyjne (imię i nazwisko, pesel), adresowe, kontaktowe, informacja o stanie rodziny, stanie zdrowia, zdrowia, dane o miejscu pracy rodziców **2. Cele przetwarzania** Nabór i rekrutacja do szkoły **3. Kategorie odbiorców** Podmioty uprawnione na podstawie przepisów prawa lub inne podmioty publiczne w oparciu o stosowną podstawę prawną **4. Kategorie odbiorców w państwach trzecich** lub w organizacjach międzynarodowych (i ich nazwy) – brak **5. Planowane terminy usunięcia poszczególnych kategorii danych** 1 rok [art. 160 ust. 2 ustawy z 14 grudnia 2016 r. Prawo oświatowe (Dz. U. z 2017 r., poz. 59)] **6. Opis technicznych i organizacyjnych środków bezpieczeństwa** Patrz: Instrukcja zarządzania RODO, Regulamin ODO **7. Podstawa prawna przetwarzania** RODO: Art.6, ust 1, lit. a (na podst. zgody osoby) RODO: Art.6, ust 1, lit. c - Przepis prawa. Ustawa z dnia 14 grudnia 2016 r. Prawo oświatowe (Dz. U. z 2017 r., poz., 59)	**1. Informacje (dokumentacja papierowa)** Karta zgłoszenia dziecka do szkoły w formie papierowej **2. Programy i systemy operacyjne** Windows, Microsoft Office, Serwery usługowe (WWW, poczta, serwery plików), pliki z danymi kandydatów **3. Infrastruktura IT** Serwery, stacje robocze, przełączniki sieciowe, routery, drukarki, skanery, kserokopiarki, centrala telefoniczna, strukturalna sieć LAN (okablowanie, gniazda, patchpanele, krosownice), smartfony **4. Infrastruktura** Sekretariat szkoły, Gabinet dyrektora szkoły **5. Pracownicy i współpracownicy** Dyrektor szkoły, Nauczyciele **6. Outsourcing** BIAMAN Politechnika Białostocka– dostawca Internetu	1. Dostarczenie Karty zgłoszenia dziecka do szkoły do Gabinetu dyrektora szkoły lub drogą mailową 2. Wybór uczniów 3. W przypadku przyjęcia do szkoły - przeniesienie do dokumentacji szkoły, w przypadku nieprzyjęcia – usunięcie po upływie określonego czasu
1. Opis kategorii osób ***Uczniowie szkoły podstawowej*** 1.a Opis kategorii danych osobowych Dane uczniów, rodziców/opiekunów prawnych: dane identyfikacyjne (imię i nazwisko, pesel), adresowe, kontaktowe, informacja o stanie rodziny, wyroki sądu rodzinnego, informacja o pieczy zastępczej, informacja o potrzebie kształcenia specjalnego, o niepełnosprawności, oddział szkoły, arkusze ocen, świadectwa, wyniki egzaminów, opinie psychologa i pedagoga, dane o rachunku bankowym (w związku z pobieraniem opłat), dane osób upoważnionych przez rodziców do odbioru dziecka ze szkoły (za zgodą rodziców i osób upoważnionych), wizerunek ucznia (za zgodą rodziców) **2. Cele przetwarzania** Kształcenie i realizacja obowiązku szkolnego Realizacja umowy o świadczenie usług edukacyjnych w ramach szkoły podstawowej	**1. Informacje (dokumentacja papierowa)** umowy (czesne), dzienniki lekcyjne, , księga uczniów, arkusze ocen, świadectwa, **2. Programy i systemy operacyjne** Windows, Microsoft Office, Serwery usługowe (WWW, poczta, serwery plików, bazy danych), Systemy: SIO, ODPN, USOS, System Finansowo-Księgowy Tytan SQL ETOB, Pliki z danymi uczniów i rodziców **3. Infrastruktura IT** Serwery, stacje robocze, przełączniki sieciowe, routery, AP, kontroler AP, drukarki, skanery, kserokopiarki, centrala telefoniczna, strukturalna sieć LAN (okablowanie, gniazda, patchpanele, krosownice), smartfony **4. Infrastruktura** Sekretariat szkoły, Pokój nauczycielski, gabinet higienistki, Kwestura, Archiwum **5. Pracownicy i współpracownicy** Dyrektor szkoły, Nauczyciele, Logopeda, Księgowe	1.Popisanie umowy 2. Założenie ewidencji uczniów, 3. Prowadzenie dziennika lekcyjnego 4. Złożenie informacji o realizacji obowiązku szkolnego do szkół obwodowych uczniów 4. Założenie i prowadzenie bieżącej dokumentacji dydaktyczno-wychowawczej: arkusze ocen, arkusze obserwacji, opiniowanie 5. Egzaminowanie i wystawianie świadectw 6. Prowadzenie dziennika lekcyjnego 7.Rozliczanie płatności, monitorowanie i windykacja należności, rozstrzyganie spraw spornych 8. Przekazanie do Archiwum

Ewentualne dochodzenie roszczeń **3. Kategorie odbiorców** Podmioty uprawnione na podstawie przepisów prawa takie jak: Ministerstwo Edukacji Narodowej, Kuratorium oraz Zakład opieki zdrowotnej (higienistka), Obwodowa szkoła podstawowa (informacja o realizacji obowiązku szkolnego), lub inne podmioty publiczne w oparciu o stosowną podstawę prawną, ewentualnie kancelaria prawna, firma windykacyjna **4. Kategorie odbiorców w państwach trzecich** lub w organizacjach międzynarodowych (i ich nazwy) – brak **5. Planowane terminy usunięcia poszczególnych danych** - Przekazane dane osobowe będą przechowywane w różnych okresach czasu w oparciu o Instrukcję Kancelaryjną na podstawie: Ustawy z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach oraz Rozporządzenia Ministra Kultury z dnia 16 września 2002 r. w sprawie postępowania z dokumentacją, zasad jej klasyfikowania i kwalifikowania oraz zasad i trybu przekazywania materiałów archiwalnych do archiwów państwowych. - do momentu cofnięcia zgody lub 1 rok - ewentualnie do zaspokojenia lub przedawnienia roszczeń **6. Opis technicznych i organizacyjnych środków bezpieczeństwa** Patrz: Instrukcja zarządzania RODO, Regulamin ODO **7. Podstawa prawna przetwarzania** RODO: Art.6, ust 1, lit. a (na podst. zgody) - wizerunek ucznia, udział w konkursach, wycieczkach, zawodach, cele marketingowe, weryfikacja tożsamości osób odbierających dzieci za szkoły RODO: Art.6, ust 1, lit. b (realizacja umowy) – umowa o świadczenie usług edukacyjnych w ramach szkoły podstawowej RODO: Art.6, ust 1, lit. c (przepis prawa) – Ustawa z dnia 14 grudnia 2016 r. Prawo oświatowe (Dz. U. z 2017 r., poz 59, odpowiednie rozporządzenia MEN RODO: Art.6, ust.1 lit. d – (prawnie uzasadniony interes administratora) - ewentualna windykacja należności, rozstrzyganie spraw spornych, monitoring wizyjny	**6. Outsourcing** ETOB - dostawca oprogramowania i wsparcia technicznego - System Finansowo-Księgowy Tytan SQL ETOB BIAMAN Politechnika Białostocka– dostawca Internetu Kancelaria Prawna – umowa o obsługę prawną Uniwersytet im. A. Mickiewicza w Poznaniu – dostawca oprogramowania USOS	
1. Opis kategorii osób ***Nabór i rekrutacja do przedszkola*** **1.a Opis kategorii danych osobowych** Dane dzieci, rodziców/opiekunów prawnych: dane identyfikacyjne, (imię i nazwisko, pesel) adresowe, kontaktowe, o stanie zdrowia i potrzebach żywieniowych dzieci, dane o miejscu pracy rodziców **2. Cele przetwarzania** Nabór i rekrutacja do przedszkola	**1. Informacje (dokumentacja papierowa)** Identyfikacyjne **2. Programy i systemy operacyjne** Windows, Microsoft Office, Serwery usługowe (WWW, poczta, serwery plików), pliki z danymi kandydatów, System Finansowo-Księgowy Tytan SQL ETOB **3. Infrastruktura IT** Serwery, stacje robocze, przełączniki sieciowe, routery, drukarki, skanery,	1. Dostarczenie Karty zapisu dziecka do przedszkola do Gabinetu dyrektora przedszkola lub drogą mailową 2.Zakwafifikowanie wychowanków 3. W przypadku przyjęcia do przedszkola przeniesienie do dokumentacji przedszkola, w przypadku nieprzyjęcia – usunięcie po upływie określonego czasu

3. Kategorie odbiorców Podmioty uprawnione na podstawie przepisów prawa lub inne podmioty publiczne w oparciu o stosowną podstawę prawną np. Obwodowa rejonowa szkoła podstawowa (informacja o realizacji obowiązku przedszkolnego w przypadku 6-latków) **4. Kategorie odbiorców w państwach trzecich** lub w organizacjach międzynarodowych (i ich nazwy) – brak **5. Planowane terminy usunięcia poszczególnych kategorii danych** 1 rok [art. 160 ust. 2 ustawy z 14 grudnia 2016 r. Prawo oświatowe (Dz. U. z 2017 r., poz. 59)] **6. Opis technicznych i organizacyjnych środków bezpieczeństwa** Patrz: Instrukcja zarządzania RODO, Regulamin ODO **7. Podstawa prawna przetwarzania** RODO: Art.6, ust 1, lit. a (na podst. zgody osoby) Art.6, ust 1, lit. c - Przepis prawa. Ustawa z dnia 14 grudnia 2016 r. Prawo oświatowe (Dz. U. z 2017 r., poz. 59	kserokopiarki, centrala telefoniczna, strukturalna sieć LAN (okablowanie, gniazda, patchpanele, krosownice) **4. Infrastruktura** Gabinet Dyrektora przedszkola, Archiwum **5. Pracownicy i współpracownicy** Dyrektor przedszkola, Nauczyciele **6. Outsourcing** BIAMAN Politechnika Białostocka– dostawca Internetu	
1. Opis kategorii osób *Wychowankowie przedszkola* **1.a Opis kategorii danych osobowych** Dane dzieci, rodziców/opiekunów prawnych: dane identyfikacyjne (imię i nazwisko, pesel), adresowe, kontaktowe, informacja o stanie rodziny, stanie zdrowia i potrzebach żywieniowych dziecka, wyroki sądu rodzinnego, informacja o pieczy zastępczej, dane o rachunku bankowym (w związku z pobieraniem opłat), dane osób upoważnionych przez rodziców do odbioru dziecka z przedszkola (za zgodą rodziców i osób upoważnionych), wizerunek wychowanka do celów marketingowych w mediach społecznościowych i na stronie WWW przedszkola (za zgodą rodziców) **2. Cele przetwarzania** Realizacja celów dydaktycznych, opiekuńczych i wychowawczych Realizacja umowy oświadczenie usług edukacyjnych e ramach opieki przedszkolnej Ewentualne dochodzenie roszczeń **3. Kategorie odbiorców** Podmioty uprawnione na podstawie przepisów prawa takie jak: Ministerstwo Edukacji Narodowej, Kuratorium, ODPN, Poradnia psych-pedagogiczna, Obwodowa szkoła podstawowa (informacja o realizacji obowiązku przedszkolnego w przypadku 6-latków) lub inne podmioty publiczne w oparciu o stosowną podstawę prawną, ewentualnie kancelaria prawna, firma windykacyjna **4. Kategorie odbiorców w państwach trzecich** lub w organizacjach międzynarodowych (i ich nazwy) – brak	**1. Informacje (dokumentacja papierowa)** Karta zapisu dziecka do przedszkola, umowa dziennik zajęć, księga wychowanków, karty pracy dziecka **2. Programy i systemy operacyjne** Windows, Microsoft Office, Serwery usługowe (WWW, poczta, serwery plików, bazy danych), Systemy: SIO, ODPN, USOS, Pliki z danymi wychowanków System Finansowo-Księgowy Tytan SQL ETOB, **3. Infrastruktura IT** Serwery, stacje robocze, przełączniki sieciowe, routery, AP, kontroler AP, drukarki, skanery, kserokopiarki, centrala telefoniczna, strukturalna sieć LAN (okablowanie, gniazda, patchpanele, krosownice) Serwerownia, Stacje robocze **4. Infrastruktura** Pokój dyrektora, Pokój nauczycielski, Kwestura, Archiwum **5. Pracownicy i współpracownicy** Dyrektor przedszkola, Nauczyciele, Księgowe **6. Outsourcing** ETOB dostawca oprogramowania i wsparcia technicznego - System Finansowo-Księgowy Tytan SQL ETOB BIAMAN Politechnika Białostocka– dostawca Internetu Kancelaria Prawna – umowa o obsługę prawną Uniwersytet im. A. Mickiewicza w Poznaniu – dostawca oprogramowania USOS „Szkolna strona" – hosting strony WWW umowa powierzenia	1. Podpisanie umowy 2. Wpis wychowanków do dzienników zajęć 3. Prowadzenie księgi wychowanków 4. Prowadzenie dokumentacji przebiegu działalności dydaktycznej, opiekuńczej wychowawczej: arkusze obserwacji i diagnozy gotowości szkolnej 5. Karty pracy dziecka 6. Rozliczanie płatności, monitorowanie i windykacja należności, rozstrzyganie spraw spornych 7. Przekazanie do Archiwum

5. Planowane terminy usunięcia poszczególnych Przekazane dane osobowe będą przechowywane w różnych okresach czasu, w oparciu o Instrukcję Kancelaryjną na podstawie Ustawy z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach oraz Rozporządzenia Ministra Kultury z dnia 16 września 2002 r. w sprawie postępowania z dokumentacją, zasad jej klasyfikowania i kwalifikowania oraz zasad i trybu przekazywania materiałów archiwalnych do archiwów państwowych - do momentu cofnięcia zgody albo 1 rok (w przypadku jej niecofnięcia) - ewentualnie do zaspokojenia lub przedawnienia roszczeń **6. Opis technicznych i organizacyjnych środków bezpieczeństwa** Patrz: Instrukcja zarządzania RODO, Regulamin ODO **7. Podstawa prawna przetwarzania** RODO: Art.6, ust 1, lit. a (na podst. zgody) – wizerunek wychowanka, udział w konkursach, wycieczkach, zawodach, cele marketingowe, weryfikacja tożsamości osób odbierających dzieci z przedszkola RODO: Art.6, ust 1, lit. b (realizacja umowy) – umowa o świadczenie usług edukacyjnych w ramach opieki przedszkolnej, RODO: Art.6, ust 1, lit. c (przepis prawa) – Ustawa z dnia 14 grudnia 2016 r. Prawo oświatowe (Dz. U. z 2017 r., poz. 59, odpowiednie rozporządzenia MEN RODO: Art.6, ust.1 lit. d – (prawnie uzasadniony interes administratora) - ewentualna windykacja należności, rozstrzyganie spraw spornych, monitoring wizyjny		
1. Opis kategorii osób ***Nabór i rekrutacja do klubu dziecięcego*** **1.a Opis kategorii danych osobowych** Dane identyfikacyjne (imię i nazwisko, pesel), adresowe, kontaktowe dziecka i rodziców/opiekunów prawnych, miejsce pracy, informacje o liczbie i wieku rodzeństwa, informacje o stanie zdrowia, diecie, rozwoju psychoruchowym dziecka i ewentualnym stopniu niepełnosprawności **2. Cele przetwarzania** Nabór do klubu dziecięcego **3. Kategorie odbiorców** Brak **4. Kategorie odbiorców w państwach trzecich** lub w organizacjach międzynarodowych (i ich nazwy) – nie dotyczy **5. Planowane terminy usunięcia poszczególnych kategorii danych** W przypadku przyjęcia dziecka do klubu – przeniesione do dokumentacji podopiecznego w przypadku odmowy przyjęcia do klubu – 1 rok, jeśli rodzice wyrażą zgodę lub do jej cofnięcia	**1. Informacje (dokumentacja papierowa)** Karta zapisu dziecka do klubu **2. Programy i systemy operacyjne** Windows, Microsoft Office, Serwery usługowe (WWW, poczta, serwery plików), pliki z danymi kandydatów **3. Infrastruktura IT** Serwery, stacje robocze, przełączniki sieciowe, routery, drukarki, skanery, kserokopiarki, centrala telefoniczna, strukturalna sieć LAN (okablowanie, gniazda, patchpanele, krosownice), smartfony **4. Infrastruktura** Pomieszczenie osoby kierującej pracą klubu dziecięcego, sale opieki **5. Pracownicy i współpracownicy** Osoba kierująca pracą klubu dziecięcego, Opiekunki **6. Outsourcing** BIAMAN Politechnika Białostocka– dostawca Internetu	1. Przyjęcie kart zapisu dziecka do klubu 2.Wybór podopiecznych 3. Usunięcie danych osób nieprzyjętych po upływie określonego czasu

6. Opis technicznych i organizacyjnych środków bezpieczeństwa Patrz: Instrukcja zarządzania RODO, Regulamin ODO **7. Podstawa prawna przetwarzania** RODO: Art.6, ust 1, lit. a (na podst. zgody osoby) RODO Art.6, ust 1, lit. c - Przepis prawa Ustawa z dnia 4 lutego 2011 o opiece nad dziećmi do lat 3		
1. Opis kategorii osób ***Podopieczni, byli podopieczni klubu dziecięcego*** **1.a Opis kategorii danych osobowych** Dane identyfikacyjne (imię i nazwisko, pesel), adresowe, kontaktowe dziecka i rodziców/opiekunów prawnych, dane o miejscu pracy rodziców, dane o rachunku bankowym (w związku z pobieraniem opłat) informacje o liczbie i wieku rodzeństwa, informacje o stanie zdrowia, diecie, rozwoju psychoruchowym dziecka i ewentualnym stopniu niepełnosprawności, wizerunek dziecka (na podstawie zgody rodzica), dane osób upoważnionych przez rodziców do odbioru dziecka z klubu (na podstawie zgody) **2. Cele przetwarzania** Realizacja zadań opiekuńczych, wychowawczych i dydaktycznych Realizacja umowy **3. Kategorie odbiorców** Podmioty uprawnione na podstawie przepisów prawa lub inne podmioty publiczne w oparciu o stosowne podstawy prawne, ewentualnie kancelaria prawna, firma windykacyjna **4. Kategorie odbiorców w państwach trzecich** lub w organizacjach międzynarodowych (i ich nazwy) – brak **5. Planowane terminy usunięcia poszczególnych kategorii danych** – do momentu cofnięcia zgody lub 1 rok – ewentualnie do zaspokojenia lub przedawnienia roszczeń **6. Opis technicznych i organizacyjnych środków bezpieczeństwa** Patrz: Instrukcja zarządzania RODO, Regulamin ODO **7. Podstawa prawna przetwarzania** RODO Art.6, ust 1, lit. a (na podstawie zgody) -upublicznianie wizerunku na stronie WWW i w mediach społecznościowych, uwierzytelnianie tożsamości osób odbierających dzieci z klubu RODO: Art.6, ust 1, lit. b (realizacja umowy) - umowa o świadczenie opieki RODO Art.6, ust 1, lit. c - Przepis prawa Ustawa z dnia 4 lutego 2011 o opiece nad dziećmi do lat 3 RODO: Art.6, ust.1 lit. d – (prawnie uzasadniony interes realizowany przez administratora) - ewentualna windykacja należności, rozstrzyganie spraw spornych, monitoring wizyjny	**1. Informacje (dokumentacja papierowa)** Umowy o świadczeni opieki, w formie papierowej, Dzienniki zajęć, Dzienniki frekwencji, pozostała dokumentacja **2. Programy i systemy operacyjne** Windows, Microsoft Office, Serwery usługowe (WWW, poczta, serwery plików), pliki z danymi podopiecznych, System finansowo-Księgowy Tytan SQL ETOB **3. Infrastruktura IT** Serwery, stacje robocze, przełączniki sieciowe, routery, drukarki, skanery, kserokopiarki, centrala telefoniczna, strukturalna sieć LAN (okablowanie, gniazda, patchpanele, krosownice), smartfony **4. Infrastruktura** Pomieszczenia klubu dziecięcego, Pomieszczenie osoby kierującej pracą klubu dziecięcego, Kwestura **5. Pracownicy i współpracownicy** Osoba kierująca pracą klubu dziecięcego, Opiekunki, Księgowe **6. Outsourcing** ETOB dostawca oprogramowania i wsparcia technicznego - System Finansowo-Księgowy Tytan SQL ETOB BIAMAN Politechnika Białostocka– dostawca Internetu Kancelaria Prawna – umowa o obsługę prawną	1. Sporządzenie umowy oświadczenie opieki 2. Prowadzenie dziennika zajęć. 3. Usunięcie danych osobowych po upływie określonego czasu.

1. Opis kategorii osób (nazwa zbioru) ***Kontrahenci (usługobiorcy, najemcy)*** **1.a Opis kategorii danych osobowych** Dane identyfikacyjne, dane adresowe **2. Cele przetwarzania** Sprzedaż/ usługa dla osób fizycznych prowadzących własną działalność gospodarczą **3. Kategorie odbiorców** US, Bank w zakresie przelewów, ewentualnie kancelaria prawna, firma windykacyjna **4. Kategorie odbiorców w państwach trzecich** lub w organizacjach międzynarodowych (i ich nazwy) – brak **5. Planowane terminy usunięcia poszczególnych kategorii danych** dane kontrahenta przechowywane są przez okres 6 lat (art. 86 § 1 Ordynacji podatkowej) - dane kontrahentów przetwarzane są do momentu ustania przetwarzania w celach analityki oraz planowania biznesowego **6. Opis technicznych i organizacyjnych środków bezpieczeństwa** Patrz: Instrukcja zarządzania RODO, Regulamin ODO **7. Podstawa prawna przetwarzania** RODO Art.6, ust 1, lit. c - Przepis prawa - Ordynacja podatkowa Art.6, ust 1, lit. b –(RODO) dane niezbędne do realizacji umowy i wystawienia faktury Art.6, ust 1, lit. f (RODO) – prawnie usprawiedliwiony interes administratora - dane kontrahentów przetwarzane są do momentu ustania przetwarzania w celach analityki oraz planowania biznesowego oraz w celu dochodzenia roszczeń	**1. Informacje (dokumentacja papierowa)** Zamówienia, faktury, umowy **2. Programy i systemy operacyjne** Windows, Microsoft Office, Serwery usługowe (WWW, poczta, serwery plików), pliki z danymi kontrahentów, System finansowo-Księgowy Tytan SQL ETOB **3. Infrastruktura IT** Serwery, stacje robocze, przełączniki sieciowe, routery, drukarki, skanery, kserokopiarki, centrala telefoniczna, strukturalna sieć LAN (okablowanie, gniazda, patchpanele, krosownice), smartfony **4. Infrastruktura** Pomieszczenia Działu Technicznego, Serwerownia, Kwestura **5. Pracownicy i współpracownicy** Pracownik działu technicznego, Administrator SI, Księgowe, Kwestor **6. Outsourcing** ETOB - dostawca oprogramowania i wsparcia technicznego - System Finansowo-Księgowy Tytan SQL ETOB BIAMAN Politechnika Białostocka – dostawca Internetu Kancelaria Prawna – umowa o obsługę prawną Poczta Polska - w zakresie adresu	1. Złożenie oferty 2. Przyjęcie zamówienia / podpisanie umowy 3. Wystawienie faktury 4. Księgowanie, 5. Rozliczanie płatności, monitorowanie i windykacja należności, rozstrzyganie spraw spornych
1. Opis kategorii osób (nazwa zbioru) ***Kontrahenci (dostawcy)*** **1.a Opis kategorii danych osobowych** Dane identyfikacyjne, dane adresowe **2. Cele przetwarzania** Realizacja umów na dostawę towarów lub usług świadczonych przez osoby fizyczne prowadzące działalność gospodarczą **3. Kategorie odbiorców** Bank w zakresie przelewów, **4. Kategorie odbiorców w państwach trzecich** lub w organizacjach międzynarodowych (i ich nazwy) – brak **5. Planowane terminy usunięcia poszczególnych kategorii danych** dane kontrahenta przechowywane są przez okres 6 lat (art. 86 § 1 Ordynacji podatkowej). LUB dane kontrahentów przetwarzane są do momentu ustania przetwarzania w celach analityki oraz planowania biznesowego lub dochodzenia roszczeń na podstawie Art.6, ust 1, lit. f (RODO) – prawnie usprawiedliwionego interesu administratora **6. opis technicznych i organizacyjnych środków bezpieczeństwa** Patrz: Instrukcja zarządzania RODO, Regulamin ODO **7. Podstawa prawna przetwarzania** Art.6, ust 1, lit. b – dane niezbędne do	**1. Informacje (dokumentacja papierowa)** Zamówienia, faktury od dostawcy, umowy **2. Programy i systemy operacyjne** Windows, Microsoft Office, Serwery usługowe (WWW, poczta, serwery plików), pliki z danymi podopiecznych, System finansowo-Księgowy ETOB **3. Infrastruktura IT** Serwery, stacje robocze, przełączniki sieciowe, routery, drukarki, skanery, kserokopiarki, centrala telefoniczna, strukturalna sieć LAN (okablowanie, gniazda, patchpanele, krosownice), smartfony **4. Infrastruktura** Pomieszczenie Działu Technicznego Serwerownia, Kwestura **5. Pracownicy i współpracownicy** Kierownicy jednostek organizacyjnych, Kierownik DziałuTechnicznego, Administrator SI, Księgowe **6. Outsourcing** ETOB dostawca oprogramowania i wsparcia technicznego - System Finansowo-Księgowy Tytan SQL ETOB BIAMAN Politechnika Białostocka– dostawca Internetu Kancelaria Prawna – umowa o obsługę prawną Poczta Polska - w zakresie adresu	1. Zbieranie ofert dostawców 2. Umowa z dostawcą / Zamówienie towaru, usługi (przesłanie do dostawcy mailem) 3. Przyjęcie faktury– mailem lub papierowo 4. Wprowadzenie danych do FK ETOB 5. Księgowanie 6. Realizacja płatności za faktury

realizacji umowy		
1. Opis kategorii osób (nazwa zbioru) ***Czytelnicy biblioteki*** **1.a Opis kategorii danych osobowych** Dane identyfikacyjne, adresowe, kontaktowe **2. Cele przetwarzania** Zapewnienie ochrony udostępnianych i wypożyczanych zbiorów Dochodzenie ewentualnych roszczeń Prowadzenia statystyk dotyczących korzystania z biblioteki **3.Kategorie odbiorców** podmioty uprawnione do uzyskania danych osobowych na podstawie przepisów prawa, za zgodą i w zakresie udostępnionym przez administratora danych np. firmy windykacyjne, firmy wspierające obsługę informatyczną **4. Kategorie odbiorców w państwach trzecich** lub w organizacjach międzynarodowych (i ich nazwy) – brak **5. Planowane terminy usunięcia poszczególnych kategorii danych** Po zakończeniu studiów i podpisaniu karty obiegowej Ewentualnie do czasu zaspokojenia lub przedawnienia roszczeń **6. Opis technicznych i organizacyjnych środków bezpieczeństwa** Patrz: Instrukcja zarządzania RODO, Regulamin ODO **7. Podstawa prawna przetwarzania** RODO: Art.6, ust 1,lit. c (przepis prawa) – Ustawa o bibliotekach z dnia 27 czerwca 1997 r., Ustawa z dnia 29 czerwca 1995 r. o statystyce publicznej o RODO: Art.6, ust.1 lit. f – (prawnie uzasadniony interes realizowany przez administratora) – ewentualne dochodzenie roszczeń, windykacja należności, monitoring wizyjny	**Informacje (dokumentacja papierowa)** Karta zapisu do biblioteki, dziennik odwiedzin czytelni, kwitariusz opłat tytułem kar bibliotecznych **2. Programy i systemy operacyjne** Windows, Microsoft Office, Serwery usługowe (WWW, poczta, serwery plików), pliki z danymi czytelników, System MAK, System finansowo-Księgowy ETOB **3. Infrastruktura IT** Serwery, stacje robocze, przełączniki sieciowe, routery, drukarki, skanery, kserokopiarki, centrala telefoniczna, strukturalna sieć LAN (okablowanie, gniazda, patchpanele, krosownice), laptopy **4. Infrastruktura** Pomieszczenia Biblioteki, pomieszczenie Kwestury, Serwerownia **5. Pracownicy i współpracownicy** Pracownicy biblioteki, Księgowe **6. Outsourcing** ETOB dostawca oprogramowania i wsparcia technicznego - System Finansowo-Księgowy Tytan SQL ETOB BIAMAN Politechnika Białostocka– dostawca Internetu	1. Wypełnienie karty zapisu do biblioteki 2. Wprowadzenie danych do bazy czytelników w programie MAK 3. Bieżące prowadzenie dziennika odwiedzin czytelni 4. Kwitowanie opłat karnych 5. Usunięcie z bazy danych i zniszczenie karty zapisu
1. Opis kategorii osób (nazwa zbioru) ***Korzystający z pokoi gościnnych w Domu studenta WSE*** **1.a Opis kategorii danych osobowych** Dane identyfikacyjne, dane adresowe **2. Cele przetwarzania** Świadczenie usługi noclegowej, wypełnienie obowiązku prawnego wynikającego z przepisów prawa podatkowego, zabezpieczenie interesu administratora w przypadku konieczności dochodzenia roszczeń **3. Kategorie odbiorców** Podmioty uprawnione na podstawie przepisów prawa lub inne podmioty publiczne w oparciu o stosowne podstawy prawne **4. Kategorie odbiorców w państwach trzecich** lub w organizacjach międzynarodowych (i ich nazwy) – brak **5. Planowane terminy usunięcia poszczególnych kategorii danych** Monitoring - 60 dni/do nadpisania	**Informacje (dokumentacja papierowa)** **2. Programy i systemy operacyjne** Windows, Microsoft Office, Serwery usługowe (WWW, poczta, serwery plików), pliki z danymi gości, System finansowo-Księgowy ETOB **3. Infrastruktura IT** Serwery, stacje robocze, przełączniki sieciowe, routery, drukarki, skanery, kserokopiarki, centrala telefoniczna, strukturalna sieć LAN (okablowanie, gniazda, patchpanele, krosownice), laptopy, smartfony **4. Infrastruktura** Pomieszczenie pracownika odpowiedzialnego za realizację zakwaterowania, Kwestura, Portiernia, **5. Pracownicy i współpracownicy** Wyznaczony pracownik odpowiedzialny za realizację zakwaterowania, portierzy, księgowe **6. Outsourcing**	1.Rezerwacja pobytu telefoniczna lub internetowa lub poprzez Booking.com 2. Wniesienie opłaty za pobyt, ewentualnie wystawienie faktury zarejestrowanie jako kontrahenta- usługobiorcy 3. Zakwaterowanie po przedstawieniu dokumenty tożsamości do wglądu i dowodu zapłaty.

W przypadku wystawienia faktury - 6 lat (art. 86 § 1 Ordynacji podatkowej). **6. Opis technicznych i organizacyjnych środków bezpieczeństwa** Patrz: Instrukcja zarządzania RODO, Regulamin ODO Patrz: Instrukcja zarządzania RODO, Regulamin ODO **7. Podstawa prawna przetwarzania** Art.6, ust 1, lit. b – dane niezbędne do realizacji umowy o świadczenie usługi RODO: Art.6, ust 1,lit. c (przepis prawa) dane kontrahenta przechowywane są przez okres 6 lat (art. 86 § 1 Ordynacji podatkowej). : Art.6, ust.1 lit. f – (prawnie uzasadniony interes realizowany przez administratora) – ewentualne dochodzenie roszczeń, windykacja należności, monitoring wizyjny	ETOB dostawca oprogramowania i wsparcia technicznego - System Finansowo-Księgowy Tytan SQL ETOB BIAMAN Politechnika Białostocka– dostawca Internetu, Booking com	
1. Opis kategorii osób (nazwa zbioru) ***Rejestr korespondencyjny*** **1a. Opis kategorii danych osobowych** Dane identyfikacyjne, dane adresowe **2. Cele przetwarzania** Zarządzanie korespondencją przychodzącą i wychodzącą **3. Kategorie odbiorców** Poczta Polska **4. Kategorie odbiorców w państwach trzecich** lub w organizacjach międzynarodowych– brak **5. Planowane terminy usunięcia poszczególnych kategorii danych** 5 lat **6. Opis technicznych i organizacyjnych środków bezpieczeństwa** Patrz: Instrukcja zarządzania RODO, Regulamin ODO **7. Podstawa prawna przetwarzania** Art.6, ust 1, lit. f – jako prawnie usprawiedliwiony interes administratora (jeśli rejestr jest prowadzony do celów organizacyjnych)	**1. Informacje (dokumentacja papierowa)** Książka korespondencyjna **2. Programy i systemy operacyjne** **3. Infrastruktura IT** **4. Infrastruktura** Sekretariat, system alarmowy **5. Pracownicy i współpracownicy** Sekretarka **6. Outsourcing** Poczta polska	1. Rejestracja papierowa korespondencji wysyłanej i otrzymywanej. 2. Usunięcie z upływem przewidzianego czasu
1. Opis kategorii osób (nazwa zbioru) ***Monitoring wizyjny*** **1a. Opis kategorii danych osobowych** Wizerunek **2. Cele przetwarzania** Zabezpieczenie obiektu, mienia i osób przebywających w budynku i na obszarze monitorowanym **3. Kategorie odbiorców** Firma ochroniarska, ubezpieczeniowi **4. Kategorie odbiorców w państwach trzecich** lub w organizacjach międzynarodowych (i ich nazwy) – brak **5. Planowane terminy usunięcia poszczególnych kategorii danych** 30 dni. Dane są nadpisywane **6. Opis technicznych i organizacyjnych środków bezpieczeństwa** Patrz: Instrukcja zarządzania RODO, Regulamin ODO **7. Podstawa prawna przetwarzania** Art.6, ust 1, lit. f na podstawie prawnie uzasadnionego interesu administratora	**1. Informacje (dokumentacja papierowa)** brak **2. Programy i systemy operacyjne** Rejestratory z oprogramowaniem **3. Infrastruktura IT** Kamery, Stacja robocza- PC, Pliki z danymi wizyjnymi **4. Infrastruktura** Portiernia-Stanowisko monitoringu, pomieszczenie, w którym zamontowano rejestrator, system kontroli dostępu do pomieszczeń **5. Pracownicy i współpracownicy** Portierzy, Pracownik działu technicznego, Administrator SI **6. Outsourcing** **brak**	System monitoringu składa się z rejestratorów i kamer. Dostęp do rejestratorów i do zapisów posiadają portierzy. Wydawanie zapisów odbywa się za zgodą rektora na wezwanie upoważnionego organu w oparciu o przedstawione podstawy prawne

1. Opis kategorii osób (nazwa zbioru) *Archiwum* **1a. Opis kategorii danych osobowych** Dane osobowe byłych pracowników, byłych studentów, słuchaczy studiów podyplomowych, uczniów, wychowanków przedszkola, księga uczniów, listy płac, kartoteki wynagrodzeń **2. Cele przetwarzania** Archiwizowanie **3. Kategorie odbiorców** Podmioty uprawnione na podstawie przepisów prawa lub inne podmioty publiczne w oparciu o stosowne podstawy prawne **4. Kategorie odbiorców w państwach trzecich** lub w organizacjach międzynarodowych (i ich nazwy) – brak **5. Planowane terminy usunięcia poszczególnych kategorii danych** Przekazane dane osobowe będą przechowywane w różnych okresach czasu w oparciu o Instrukcję Kancelaryjną na podstawie: Ustawy z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach oraz Rozporządzenia Ministra Kultury z dnia 16 września 2002 r. w sprawie postępowania z dokumentacją, zasad jej klasyfikowania i kwalifikowania oraz zasad i trybu przekazywania materiałów archiwalnych do archiwów państwowych. **6. Opis technicznych i organizacyjnych środków bezpieczeństwa** Patrz: Instrukcja zarządzania RODO, Regulamin ODO **7. Podstawa prawna przetwarzania** RODO: Art.6, ust 1,lit. c (przepis prawa) Ustawa z dnia 14 lipca 1983r. o narodowym zasobie archiwalnym i archiwach. Rozporządzenie Ministra Kultury i Dziedzictwa Narodowego z dnia 20 października 2015 r. w sprawie klasyfikowania i kwalifikowania dokumentacji, przekazywania materiałów archiwalnych do archiwów państwowych i brakowania dokumentacji niearchiwalnej (Dz. U. 2015, poz. 1743)	**1. Informacje (dokumentacja papierowa)** Teczki akt osobowych byłych pracowników, teczki akt osobowych byłych studentów i słuchaczy, księga uczniów, listy płac, kartoteki wynagrodzeń. **2. Programy i systemy operacyjne** **3. Infrastruktura IT** **4. Infrastruktura** Pomieszczenie Archiwum **5. Pracownicy i współpracownicy** Pracownicy archiwum **6. Outsourcing**	1.Przekazanie dokumentacji dotyczącej poszczególnej kategorii czynności przez kierowników jednostek organizacyjnych lub osób przez nich upoważnionych. 2. Sporządzenie protokołu przekazania dokumentów do archiwum 3.Przechowywanie dokumentów w sposób zapobiegający ich uszkodzeniu, zniszczeniu, utracie integralności. 4. Umożliwienie dostępu do dokumentów przechowywanych w archiwum jedynie osobom, które posiadają do tego stosowne upoważnienie.
1. Opis kategorii osób (nazwa zbioru) Dane osobowe użytkowników platformy E-Publikacje Nauki Polskiej **1a. Opis kategorii danych osobowych** Imię i nazwisko, adres mailowy użytkownika, nick użytkownika **2. Cele przetwarzania:** korzystanie z usług serwisu tj. zamówienia dostępu do Publikacji znajdujących się w katalogu e-Publikacje Nauki Polskiej epnp.pl **3. Kategorie odbiorców**: podmioty, którym powierzono dane w celu zapewnienia wsparcia technicznego oraz zapewnienia bezpieczeństwa świadczonych usług **4. Kategorie odbiorców w państwach trzecich** lub w organizacjach międzynarodowych (i ich nazwy) – brak **5. Planowane terminy usunięcia poszczególnych kategorii danych:** dane będą	**Infrastruktura IT**: **Infrastruktura:** biuro Projektu **Pracownicy i współpracownicy:** osoby zarządzające projektem-koordynatorzy projektu **Outsourcing: -** dostawca serwera dedykowanego Firma IQ, udzielenie wsparcia technicznego – Infiniti Group sp. z o.o.	1.Rejestracja użytkownika w systemie 2.Utworzenie i wpisanie loginu oraz hasła 3.Usunięcie danych po upływie określonego czasu 3 lat od daty ostatniego logowania.

przez okres 3 lat od daty ostatniego logowania do serwisu. Po tym czasie zostaną usunięte. **6. Opis technicznych i organizacyjnych środków bezpieczeństwa** Patrz: Instrukcja zarządzania RODO, Regulamin ODO **7. Podstawa prawna przetwarzania** Art.6, ust 1,lit. b RODO (niezbędność do wykonania umowy)		

REKTOR

dr Aleksander Prokopiuk

Wyższa Szkoła Ekonomiczna
w Białymstoku
15-703 Białystok, ul. Zwycięstwa 14/3
tel./fax (85) 652-00-24, tel. (85) 652-09-97
REGON 050383717, NIP 542-17-21-656

Załącznik Nr 2
do dokumentu Polityka Ochrony danych osobowych w Wyższej Szkole Ekonomicznej w Białymstoku

Rejestr kategorii czynności przetwarzania

prowadzony przez Podmiot przetwarzający na podstawie Art. 30, ust 2 RODO

1. Podmiot przetwarzający: Wyższa Szkoła Ekonomiczna w Białymstoku, 15-703 Białystok, ul. Zwycięstwa 14/3
2. Dane kontaktowe inspektora ochrony danych: iod@wse.edu.pl
3. Nazwa oraz dane kontaktowe administratora, w imieniu którego działa podmiot przetwarzający Zarząd Województwa Podlaskiego Departament Rozwoju Regionalnego Urzędu Marszałkowskiego Województwa Podlaskiego, ul. Poleska 89, 18-874 Białystok, Wojewódzki Urząd Pracy w Białymstoku, ul. Pogodna 22, 15-354 Białystok, jako Instytucja Zarządzająca.
4. Kategorie odbiorców w państwach trzecich lub w organizacjach międzynarodowych Nie dotyczy
5. Nazwa państwa trzeciego lub organizacji międzynarodowej, gdy mają zastosowanie tam przekazania danych osobowych Nie dotyczy

1. Opis kategorii osób (nazwa zbioru) *Kandydaci na uczestników Projektu realizowanego z udziałem funduszy unijnych „Elastyczny klub malucha = Rodzic na rynku pracy" na podstawie umowy powierzenia* **1a. Opis kategorii danych osobowych** Dane osobowe kandydatów na uczestników projektu, współmałżonków i ich dzieci **2. Cele przetwarzania** Udział w rekrutacji do w/w projektu **3. Kategorie odbiorców** - podmioty upoważnione na podstawie przepisów prawa **4. Kategorie odbiorców w państwach trzecich** lub w organizacjach międzynarodowych (i ich nazwy) – brak **5. Planowane terminy usunięcia poszczególnych kategorii danych** W przypadku nie zakwalifikowania się od projektu – po zakończonej rekrutacji, w przypadku zakwalifikowania - dane osobowe będą przekazane do dokumentacji uczestników projektu **6. Opis technicznych i organizacyjnych środków bezpieczeństwa** Patrz: Instrukcja zarządzania RODO, Regulamin ODO **7. Podstawa prawna przetwarzania** RODO: Art. 6, ust 1,lit. c (przepis prawa) oraz Rodo Art. 6 ust.1 lit. e – wykonanie zadania w interesie publicznym wynikającego z zapisów ustawy wdrożeniowej – dane osobowe są niezbędne dla realizacji RPO WP na lata 2014 -2020 RODO: Art. 6, ust 1,lit. a (na podstawie zgody)	**1. Informacje (dokumentacja papierowa)** Formularz zgłoszeniowy, załączniki - zaświadczenia, oświadczenia **2. Programy i systemy operacyjne** Windows, Microsoft Office, Serwery usługowe (WWW, poczta, serwery plików, bazy danych), **3. Infrastruktura IT** Serwery, stacje robocze, przełączniki sieciowe, routery, drukarki, skanery, kserokopiarki, centrala telefoniczna, strukturalna sieć LAN (okablowanie, gniazda, patchpanele, krosownice), **4. Infrastruktura** Pomieszczenie Biura Projektu, Kwestura **5. Pracownicy i współpracownicy** Personel Projektu **6. Outsourcing** ETOB dostawca oprogramowania i wsparcia technicznego - System Finansowo-Księgowy Tytan SQL ETOB BIAMAN Politechnika Białostocka– dostawca Internetu	1.Złożenie przez kandydatów formularzy rekrutacyjnych oraz wymaganych załączników (w formie papierowej) do biura projektu. 2.Weryfikowanie przez personel projektu spełnienia warunków rekrutacji. 3.Sprządzenie list rekrutacyjnych oraz listy rezerwowej. 4. Zniszczenie lub zwrot dokumentacji kandydatom niespełniających warunków uczestnictwa w projekcie. 5. Przekazanie do dokumentacji projektowej formularzy rekrutacyjnych osób zakwalifikowanych do projektu.
1. Opis kategorii osób (nazwa zbioru) *Uczestnicy Projektu realizowanego z udziałem funduszy unijnych „Elastyczny klub malucha = Rodzic na rynku pracy"na podstawie umowy powierzenia* **1a. Opis kategorii danych osobowych** Dane osobowe uczestników Projektu, współmałżonków i ich dzieci **2. Cele przetwarzania** Realizacja w/w Projektu w zakresie zarządzania, kontroli, audytu, ewaluacji, monitorowania, sprawozdawczości i raportowania **3. Kategorie odbiorców** Instytucje pośredniczące we wdrażaniu RPOWP na lata 2014-2020, podmioty wykonujące na zlecenie badanie ewaluacyjne lub	**1. Informacje (dokumentacja papierowa)** Deklaracja uczestnictwa, załączniki - zaświadczenia, oświadczenia **2. Programy i systemy operacyjne** Windows, Microsoft Office, Serwery usługowe (WWW, poczta, serwery plików), Centrala telefoniczna, System - Centralny System Informatyczny **3. Infrastruktura IT** Serwery, stacje robocze, przełączniki sieciowe, routery, drukarki, skanery, kserokopiarki, centrala telefoniczna,	1. Zaprowadzenie dokumentacji projektowej składającej się z formularza rekrutacyjnego, deklaracji uczestnictwa w projekcie wraz z wymaganymi załącznikami. 2. Wprowadzenie danych do systemu SL 2014-2020. 3.Monitorowanie na bieżąco danych w systemie SL 2014-

realizujące kontrole i audyt oraz podmioty upoważnione na podstawie przepisów prawa **4. Kategorie odbiorców w państwach trzecich** lub w organizacjach międzynarodowych (i ich nazwy) – brak **5. Planowane terminy usunięcia poszczególnych kategorii danych** W przypadku nie zakwalifikowania się od projektu – po zakończonej rekrutacji, w przypadku zakwalifikowania - dane osobowe będą przechowywane w okresach określonych w obowiązującej Instrukcji Kancelaryjnej opracowanej na podstawie Ustawy z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach oraz Rozporządzenia Ministra Kultury z dnia 16 września 2002 r. w sprawie postępowania z dokumentacją, zasad jej klasyfikowania i kwalifikowania oraz zasad i trybu przekazywania materiałów archiwalnych do archiwów państwowych. **6. Opis technicznych i organizacyjnych środków bezpieczeństwa** Patrz: Instrukcja zarządzania RODO, Regulamin ODO **7. Podstawa prawna przetwarzania** RODO: Art.6, ust 1,lit. c (przepis prawa) oraz RODO :Art. 6 ust.1 lit. e – wykonanie zadania w interesie publicznym wynikającego z zapisów ustawy wdrożeniowej – dane osobowe są niezbędne dla realizacji RPO WP na lata 2014-2020	strukturalna sieć LAN (okablowanie, gniazda, patchpanele, krosownice) **4. Infrastruktura** Pomieszczenie Biura Projektu **5. Pracownicy i współpracownicy** Personel Projektu **6. Outsourcing** brak	2020. Bieżące uzupełnianie wymaganej dokumentacji. 4. Archiwizacja dokumentów projektowych.

REKTOR

dr Aleksander Prokopiuk

Wyższa Szkoła Ekonomiczna
w Białymstoku
15-703 Białystok, ul. Zwycięstwa 14/3
tel./fax (85) 652-00-24, tel. (85) 652-09-97
REGON 050383717, NIP 542-17-21-656

Załącznik Nr 3

do dokumentu Polityka Ochrony danych osobowych w Wyższej Szkole Ekonomicznej w Białymstoku

Arkusz analizy ryzyka

Analiza obejmuje następujące zbiory - kategorie osób

1. Kandydaci do pracy
2. Pracownicy etatowi, umowy zlecenia, umowy o dzieło, byli pracownicy
2. Kandydaci na studia
4. Studenci, byli studenci
5. Kandydaci na studia podyplomowe
6. Słuchacze studiów podyplomowych, byli słuchacze
7. Rekrutacja do szkoły podstawowej
8. Uczniowie, byli uczniowie
9. Rekrutacja do przedszkola
10. Wychowankowie, byli wychowankowie
11. Rekrutacja do klubu dziecięcego
12. Podopieczni klubu dziecięcego, byli podopieczni
13. Kontrahenci dostawcy
14. Kontrahenci klienci
15. Korzystający z pokoi gościnnych
16. Czytelnicy biblioteki

17. Rejestr korespondencyjny

18. Monitoring

19. Archiwum

20. Kopie zapasowe

21. Użytkownicy serwisu e-PNP

Legenda: 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	1	1	**2**	**Procedura:** • Szkolenia personelu • Regulamin ODO **Zabezpieczenie:** • Systemy antywirusowy i antyspamowy • Sewery proxy i bramki filtrujące o blokada ruchu na podstawie bazy reputacji o blokada dostępu do określonych stron
Nakłanianie do wykonania czynności	• Mail z dyspozycją przelewu wysłany do księgowej z rzekomego konta „osoby zarządzającej" • Fax/mail z fakturą od rzekomego „dostawcy" z informacją o zmianie numeru konta bankowego do opłacenia faktur	1	1	1	**Procedura:** • Szkolenia personelu • Regulamin ODO
Instalacja szkodliwego oprogramowania / działanie szkodliwego oprogramowania	Szkodliwe oprogramowanie (backdoory, exploity, exploitpaki, keyloggery).	1	2	2	**Procedura:** • Szkolenia personelu • Regulamin ODO **Zabezpieczenie:** • Systemy antywirusowy i antyspamowy • Sewery proxy i bramki filtrujące o skan niebezpiecznej zawartości o blokada ruchu na podstawie bazy reputacji o blokada dostępu do określonych stron
Podrzucone nośniki danych	Atakujący pozostawia w biurze lub w dziale księgowości specjalnie przygotowany pendrive z zainstalowanym samouruchamiającym się szkodliwym programem. W wielu	1	2	2	**Procedura:** • Szkolenia personelu • Regulamin ODO

	przypadkach z CIEKAWOŚCI pracownicy sprawdzają jego zawartość wkładając go do portu USB. W wyniku tego uruchamiają nieświadomie szkodliwe oprogramowanie (backdoory, exploity, exploitpaki, keyloggery).				**Zabezpieczenie:** • Dopuszczenie do użycia wyłącznie zakwalifikowanych pendrivów
Ataki telefoniczne	• 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 student/słuchacz i prosi o udzielenie informacji stanowiących dane osobowe • Intruz przedstawia się jako rodzic/opiekun prawny i prosi o udzielenie informacji stanowiących dane osobowe	1	1	1	**Procedura:** • Szkolenia personelu • Regulamin ODO
Łamanie haseł	Łamanie haseł metodami słownikowymi i siłowymi (brute force) : • do baz danych • do serwera • do aplikacji www (np. do wordpressa) • do poczty • do windows na stacjach roboczych • do routera • do firewalla	1	3	3	**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 • Stosowanie słownikowych lub popularnych haseł, np. Grazynka1, qwerty, 12345678 • Stosowanie jednego hasła do wielu (często wszystkich) systemów	1	2	2	**Procedura:** • Metody i środki uwierzytelnienia (polityka haseł) • Szkolenia personelu **Zabezpieczenia:** • długość hasła - 8 znaków • hasło zawiera duże, małe litery cyfry lub znaki specjalne • częstotliwość zmiany hasła – 60 dni • uwierzytelnianie do o aplikacji, o stacji roboczych o dysku sieciowego o sieci o poczty o smartfona • Testy penetracyjne
Ataki na sprzęt - Włamania do urządzeń nieaktualizowanych	Ataki na urządzenia sieciowe oraz inne, które działają dzięki umieszczonemu na nich oprogramowaniu (firmware / sterowniki) Zagrożenie dla nast. elementów: • routery	1	3	3	**Procedura:** • Procedura zabezpieczenia systemu informatycznego **Zabezpieczenia:** • Testy penetracyjne

	• switche • access pointy • firewall • macierz • dysk NAS • drukarki i skanery				• 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 • • drukarki i skanery	1	3	3	**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 niezabezpieczonych interfejsów lokalnych	Atakujący wpina się do urządzeń IT przez ich niezabezpieczone porty konfiguracyjne (USB, Ethernet lub COM - szeregowe) Zagrożenie dla nast. elementów: • routery • switche • firewalle • serwery • drukarki i skanery	1	3	3	**Procedura:** • Procedura zabezpieczenia systemu informatycznego **Zabezpieczenia:** • 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	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
Ataki na oprogramowanie - Wykorzystanie	Atak z wykorzystaniem znanych dziur w niezaktualizowanym oprogramowaniu Zagrożenie dla programów	1	3	3	**Procedura:** • Procedura zabezpieczenia systemu informatycznego • Procedura wykonywania przeglądów i konserwacji

znanych dziur w nieaktualizowanym oprogramowaniu	• 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)				**Zabezpieczenia:** • Stosowane jest 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
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 • 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
Ataki na oprogramowanie - Włamania z wykorzystaniem najczęstszych błędów programistycznych	Programiści pisząc programowanie często popełniają te same, znane błędy.	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
Skanowanie sieci i	Udostępniane w Internecie serwery, urządzenia sieciowe i	1	3	3	**Procedura:**

usług	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.				• 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	3	3	**Z Procedura:** • Procedura zabezpieczenia systemu informatycznego **zabezpieczenia:** • Odseparowanie wifi dla gości/klientów od sieci wewnętrznej • Stosowanie odpowiednich standardów szyfrowania • Stosowanie mocnych 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 o blokada ruchu na podstawie bazy reputacji o blokada dostępu do określonych stron • Firewall 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) • Security Information and Event Managment (analityczny system do wykrywania 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 *Dezaktywacja gniazdek sieciowych, które nie są używane w danym pomieszczeniu przez komputery i drukarki ma na celu uniemożliwienie podpięcia się do nich intruza z własnym laptopem lub urządzeniem szpiegującym. Gniazda nieużywane powinny być odłączone fizycznie od switcha w szafie, lub konfiguracyjnie poprzez wyłączenie zbędnych portów na switchu.*
Atak ransomeware	Ransomeware - Program do szyfrowania plików. Instaluje się z maili lub z hiperlinków w mailach lub poprzez odwiedziny	1	3	3	**Procedura:** • Procedura zabezpieczenia systemu informatycznego

	zainfekowanej strony. Są też znane przypadki infekcji poprzez sieć lokalną. Odszyfrowanie wymaga zapłaty np. 500 USD. Bardzo groźny				• Procedura tworzenia kopii zapasowych • **Procedura:** • Szkolenia personelu • Regulamin ODO **Zabezpieczenia:** • Systemy antywirusowy i antyspamowy • Kopie bezpieczeństwa kluczowych danych zabezpieczone przed szyfrowaniem przez ransomeware (np. utrzymanie poza siecią, najlepiej na nośnikach typu taśmy lub utrzymywanie obrazów-kopii wirtualnych serwerów) • 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 • 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)	1	2	2	**Procedura:** • Procedura nadawania uprawnień do przetwarzania danych osobowych • Procedura wykonywania przeglądów i konserwacji **Zabezpieczenia:** • 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.	1	2	2	**Procedura:** • Procedura zabezpieczenia systemu informatycznego **Zabezpieczenia:** • WAF (Web application firewall) • Firewall • Mechanizm captcha (kod z obrazka do przepisania w formularzu) • 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	1	1	1	**Procedury:** • Polityka kluczy • Polityka kontroli dostępu **Zabezpieczenia:** • kontrola kluczy zapasowych / kontrola wydawania kluczy / kontrola składowania kluczy • portiernia • ograniczenie dostępu do pomieszczeń osobom nieupoważnionym (zakaz wstępu) • personel sprzątający zobowiązany do zachowania poufności poprzez pisemne podpisanie oświadczeń o poufności

	• zainstalowaniem nieautoryzowanych urządzeń do dostępu do sieci wewnętrznej • kradzieżą komputerów, nośników				• rozmieszczenie komputerów /drukarek /xero ograniczające dostęp osób nieupoważnionych • dostęp osób nieupoważnionych w obecności osoby upoważnionej • zabezpieczenie dostępu do pomieszczeń (drzwi zamykane na klucz zabezpieczenie dostępu do serwerowni (drzwi zamykane na klucz) zabezpieczenie dostępu do archiwum (drzwi zamykane na klucz) • zabezpieczenie dokumentacji / danych w pomieszczeniach (zamknięte niemetalowe szafy / zamknięte metalowe szafy / sejf ogniotrwały / skrytki na klucze) • systemy alarmowe / zabezpieczenia antywłamaniowe (system alarmowy) • ochrona fizyczna obiektu / pomieszczeń (ochrona własna) • system kontroli dostępu (wdrożone strefy ograniczonego dostępu / system kart wejściowych) • monitoring wizyjny w obrębie obiektu i otoczeniu
Kradzież / zagubienie sprzętu i nośników poza organizacją (jeśli dane osobowe występują na tych nośnikach)	Kradzież / zagubienie: • smartfonów, • pendrive	1	1	1	**Procedury:** • Procedura zabezpieczenia systemu informatycznego **Zabezpieczenia:** • Stosowanie szyfrowanych dysków przenośnych • Stosowanie szyfrowanych pendrive • Uwierzytelnianie do urządzeń typu smartfon
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	1	1	1	**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 • program do zarządzania uprawnieniami • zarządzanie uprawnieniami – profile użytkowników • minimalizacja uprawnień • separacja sieci wewnętrznej od sieci przeznaczonej dla gości (dla wifi i dla Ethernet) np. w salach konferencyjnych • dopuszczenie do użycia wyłącznie zakwalifikowanych pendrive • 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 10 minutach nieaktywności użytkownika • ustawienie monitorów uniemożliwiające wgląd w dane osób postronnych
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	2	2	**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	2	2	**Procedury:** • Procedura wykonywania przeglądów i konserwacji **Zabezpieczenia:** • macierz RAID • system do inwentaryzacji sprzętu • system do zarządzania licencjami • plan ciągłości działania
Błąd / awaria oprogramowania	Awarie: • programu kadrowo-płacowego • poczty • aplikacji www (np. wordpressa) • bazy danych	1	3	3	**Procedury:** • Procedura wykonywania przeglądów i konserwacji **Procedury:** • Zabezpieczenia techniczne **Zabezpieczenia:** • Wirtualizacja
Pożar / eksplozja	• Pożar obiektu • Pożar serwerowni • Pożar serwera	1	3	3	**Procedury:**

	• Zniszczenie serwerowni (np. wybuch gazów technicznych)				• Zabezpieczenia techniczne **Zabezpieczenia:** • gaśnice • system PPOŻ • serwerownia z materiałów niepalnych • czujnik dymu w serwerowni
Zalanie	• Zalanie serwerowni • Zalanie archiwum (powódź, zalanie z rur)	1	3	3	**Procedury:** • Zabezpieczenia techniczne **Zabezpieczenia:** • podłoga techniczna • składowanie dokumentacji papierowej na podwyższeniu • digitalizacja dokumentów archiwalnych
Przegrzanie / zbyt duża wilgotność	• wysoka temperatura w serwerowni • wysoka wilgotność w archiwum	1	3	3	**Procedury:** • Zabezpieczenia techniczne **Zabezpieczenia:** • klimatyzacja w serwerowni
Awaria zasilania	• skoki napięcia • przerwy w dostawie zasilania	1	3	3	**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
		1	1	1	**Procedury:**
					
					• Procedura zabezpieczenia systemu informatycznego
					
					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

Nieuprawnione kopiowanie danych	• kopiowanie danych z katalogów, dysków, baz, programów • kserowanie i robienie zdjęć przez pracownika lub przez osobę obcą	1	1	1	**Procedury:** • Procedura zabezpieczenia systemu informatycznego • Regulamin ODO **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 • Blokada portów USB • Blokada funkcji eksportu danych w kluczowych programach / systemach
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	1	3	3	**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	1	1	**Procedury:** • Regulamin ODO • Utylizacja elektronicznych nośników i wydruków oraz czyszczenie danych **Zabezpieczenia:** • niszczarki paskowe, niszczenie/czyszczenie nośników przed utylizacją
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	1	1	1	**Procedury:** • Szkolenia personelu • Regulamin ODO

	inteligencji lub z powodów niewiedzy				
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" • dostęp do programów testowych (z prawdziwymi danymi osobowymi) bez logowania • pomyłkowe udostępnienie, wysłanie do złego odbiorcy, błędne zabezpieczenia	2	3	6	**Procedury:** • Procedura zabezpieczenia systemu informatycznego • Szkolenia personelu • Regulamin ODO
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	1	1	1	**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	1	1	**Procedury:** • Procedury przywracania

Wyższa Szkoła Ekonomiczna
w Białymstoku
15-703 Białystok, ul. Zwycięstwa 14/3
tel./fax (85) 652-00-24, tel. (85) 652-09-97
REGON 050383717, NIP 542-17-21-656

Załącznik Nr 4

do dokumentu Polityka Ochrony danych osobowych w Wyższej Szkole Ekonomicznej w Białymstoku

PLAN POSTĘPOWANIA Z RYZYKIEM

Aktywa	Zagrożenie	Proponowane zabezpieczenie	Osoba odpowiedzialna	Przewidywana data wprowadzenia

REKTOR

dr Aleksander Prokopiuk

Wyższa Szkoła Ekonomiczna
w Białymstoku
15-703 Białystok, ul. Zwycięstwa 14/3
tel./fax (85) 652-00-24, tel. (85) 652-09-97
REGON 050383717, NIP 542-17-21-656

Załącznik Nr 5
do dokumentu Polityka Ochrony danych osobowych w Wyższej Szkole Ekonomicznej w Białymstoku

Białystok, dn. .....

UPOWAŻNIENIE
do przetwarzania danych osobowych

Z dniem ..... **upoważniam** Panią/Pana ....., *zatrudnioną/ego przez Wyższą Szkołę Ekonomiczną w Białymstoku, wykonującą/ego czynności na podstawie umowy zlecenie, będącą/ym współpracownikiem*,* administratora danych osobowych, *do przetwarzania danych osobowych w celach związanych z wykonywaniem obowiązków na stanowisku ..... / wykonywaniem następujących czynności na podstawie umowy zlecenia ..... lub do obsługi następujących zbiorów danych .....** oraz do **obsługi systemu informatycznego i urządzeń wchodzących w jego skład.**

Niniejsze upoważnienie obejmuje przetwarzanie danych osobowych w formie tradycyjnej - papierowej i elektronicznej.

Upoważnienie wygasa z chwilą rozwiązania umowy o pracę, zmiany stanowiska pracy, zakończenia współpracy.

.....
podpis administratora

.....
podpis pracownika

** wybrać właściwe*

Załącznik nr 6
do dokumentu Polityka Ochrony danych osobowych w Wyższej Szkole Ekonomicznej w Białymstoku

Rejestr osób upoważnionych do przetwarzania danych osobowych w Wyższej Szkole Ekonomicznej w Białymstoku					
L.p.	**Imię i nazwisko**	**Stanowisko służbowe**	**Data nadania upoważnienia**	**Data ustania upoważnienia**	**Uwagi**

Załącznik Nr 7
do dokumentu Polityka Ochrony danych osobowych w Wyższej Szkole Ekonomicznej w Białymstoku

UMOWA
powierzenia przetwarzania danych osobowych, zwana dalej Umową

zawarta w ..... w dniu ..... r. pomiędzy: .....
z siedzibą w ....., zarejestrowaną/ym w ..... pod numerem ....., posiadającą/ym numer NIP ..... oraz numer REGON ....., reprezentowaną/ym przez: ....., zwaną/ym dalej Zleceniodawcą,

a

.....z siedzibą w ....., zarejestrowaną/ym w ..... pod numerem ....., posiadającą/ym numer NIP ..... oraz numer REGON ....., reprezentowaną/ym przez: ....., zwaną/ym dalej Zleceniobiorcą

§ 1
Definicje

1. Podmiot przetwarzający – podmiot, któremu powierzono przetwarzanie danych osobowych na mocy umowy powierzenia ze Zleceniodawcą, zwany dalej Zleceniobiorcą
2. Administrator - organ, jednostka organizacyjna, podmiot lub osoba, decydujące o celach i środkach przetwarzania danych osobowych, zwany także Zleceniodawcą
3. Zbiór danych - każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie,
4. Przetwarzanie danych - jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych,
5. Rozporządzenie- Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych),
6. Inny podmiot przetwarzający - podmiot, któremu podmiot przetwarzający w imieniu administratora pod-powierzył w całości lub częściowo przetwarzanie danych osobowych

§ 2
Przedmiot Umowy, cel, charakter i zakres

1. Przedmiotem umowy jest powierzenie przez Zleceniodawcę danych osobowych do przetwarzania przez Zleceniobiorcę
2. Celem powierzenia jest: .....

.....

3. Charakter przewarzania danych dotyczy przetwarzania danych osobowych w formie papierowej, przy wykorzystaniu systemów informatycznych (lub systemach monitoringu wizyjnego / głosowego) * *wybrać odpowiednio*

§ 3
Czas trwania

1. Zleceniobiorca uprawniony jest do przetwarzania powierzonych danych do dnia wygaśnięcia lub rozwiązania Umowy.
2. W terminie ..... dni od ustania Umowy, Zleceniobiorca zobowiązany jest do usunięcia powierzonych danych, ze wszystkich nośników, programów i aplikacji w tym również kopii, chyba, że obowiązek ich dalszego przetwarzania wynika z odrębnych przepisów prawa.
3. *(warunkowo)* Zleceniobiorca w terminie ..... dni od ustania Umowy zobowiązany jest do zwrotu powierzonych danych na nośnikach papierowych lub elektronicznych

§4
Obowiązki i prawa

1. Zleceniobiorca zobowiązuje się współpracować ze Zleceniodawcą w zakresie udzielania odpowiedzi na żądania osoby, której dane dotyczą, opisane w rozdziale III Rozporządzenia *(w szczególności w zakresie informowania i przejrzystej komunikacji, dostępu do danych, obowiązku informacyjnego, prawa dostępu, prawa do sprostowania danych, usunięcia danych, ograniczenia przetwarzania, przenoszenia danych, prawa sprzeciwu oraz informowania o zautomatyzowanym podejmowaniu decyzji).*
2. Zleceniobiorca zobowiązuje się do pomocy Zleceniodawcy w wywiązaniu się z obowiązków określonych w art. 32-36 Rozporządzenia *(w szczególności dla bezpieczeństwa przetwarzania, zgłaszania naruszenia ochrony danych osobowych organowi nadzorczemu, zawiadamiania osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych, przeprowadzania oceny skutków dla ochrony danych osobowych, konsultacji z organem nadzorczym)*
3. Zleceniobiorca zobowiązuje się do udostępnienia Zleceniodawcy wszelkich informacji niezbędnych do wykazania spełnienia obowiązków spoczywających na Zleceniobiorcy oraz umożliwi Zleceniodawcy lub audytorowi upoważnionemu przez Zleceniodawcę przeprowadzanie audytów, w tym inspekcji, współpracując przy działaniach sprawdzających i naprawczych

§5
Zgłaszanie incydentów

1. Zleceniobiorca zobowiązuje się po stwierdzeniu naruszenia ochrony danych osobowych do zgłoszenia tego Zleceniodawcy bez zbędnej zwłoki
2. Informacja przekazana Zleceniodawcy powinna zawierać co najmniej:

a. opis charakteru naruszenia oraz - o ile to możliwe - wskazanie kategorii i przybliżonej liczby osób, których dane zostały naruszone i ilości/rodzaju danych, których naruszenie dotyczy
b. opis możliwych konsekwencji naruszenia,

c. opis zastosowanych lub proponowanych do zastosowania przez Zleceniobiorcę środków w celu zaradzenia naruszeniu, w tym minimalizacji jego negatywnych skutków.

§ 6
(paragraf warunkowy – pozostaje, gdy występuje podopowierzenie)
Korzystanie przez Zleceniobiorcę z usług innego podmiotu przetwarzającego

1. Zleceniobiorca w ramach realizacji Umowy korzysta z usług innego podmiotu przetwarzającego a Zleceniodawca przyjmuje to do wiadomości i wyraża na to zgodę
2. W przypadku zmian dotyczących dodania lub zastąpienia innych podmiotów przetwarzających, Zleceniobiorca jest zobowiązany do poinformowania o tym Zleceniodawcę
3. Jeżeli inny podmiot przetwarzający nie wywiąże się ze spoczywających na nim obowiązków ochrony danych, pełna odpowiedzialność wobec Zleceniodawcy za wypełnienie obowiązków tego innego podmiotu przetwarzającego spoczywa na Zleceniobiorcy

§7
Deklarowane środki techniczne i organizacyjne

1. Zleceniobiorca gwarantuje, że każda osoba realizująca Umowę zobowiązana jest do bezterminowego zapewnienia poufności danych osobowych przetwarzanych w związku z wykonywaniem Umowy, a w szczególności do tego, że nie będzie przekazywać, ujawniać i udostępniać tych danych osobom nieuprawnionym. Jednocześnie każda osoba realizująca Umowę zobowiązana jest do zachowania w tajemnicy sposobów zabezpieczenia danych osobowych
2. Zleceniobiorca deklaruje stosowanie środków technicznych i organizacyjnych określonych w art. 32 Rozporządzenia, jako adekwatnych do zidentyfikowanego ryzyka naruszenia praw lub wolności powierzonych danych osobowych a w szczególności:

a. pseudonimizację i szyfrowanie danych osobowych;
b. zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania;
c. zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego;
d. regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania

3. Zleceniobiorca zobowiązuje się za pomocą odpowiednich środków technicznych lub organizacyjnych stosować ochronę powierzonych danych przed niedozwolonym lub niezgodnym z prawem przetwarzaniem (zniszczeniem, utraceniem, zmodyfikowaniem, nieuprawnionym ujawnieniem lub nieuprawnionym dostępem do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych) oraz przypadkową utratą, zniszczeniem lub uszkodzeniem.

§7a
Szczegółowe deklarowane środki techniczne i organizacyjne
(przykład szczegółowej listy wymagań dla usługi administracji - serwisu IT – „jeśli istnieje potrzeba uszczegółowienia innych zakresów umów – poniżej należy stworzyć dedykowaną listę zabezpieczeń, którą Administrator oczekuje od Podmiotu przetwarzającego")

1. Zleceniobiorca zobowiązuje się dopuszczać do przetwarzania danych osobowych osoby realizujące Umowę (podać ewentualnie funkcje osób, serwisanci, konsultanci, ...) poinformowane i przeszkolone z zasad bezpieczeństwa pracy z danych osobowymi
2. Każda osoba realizująca Umowę zobowiązana jest do przetwarzania danych osobowych do których uzyskała dostęp wyłącznie w zakresie i celu przewidzianym w Umowie.
3. Każda osoba realizująca Umowę zobowiązana jest do zapewnienia poufności danych osobowych przetwarzanych w związku z wykonywaniem Umowy a w szczególności do tego, że nie będzie przekazywać, ujawniać i udostępniać tych danych osobom nieuprawnionym.
4. Każda osoba realizująca Umowę zobowiązuje się do zachowania w tajemnicy sposobów zabezpieczenia danych osobowych o ile nie są one jawne.
5. Każda osoba realizująca Umowę zobowiązana jest do nie powodowania niezgodnych z Umową zmian danych lub utraty, uszkodzenia lub zniszczenia tych danych.
6. Każda osoba realizująca Umowę zobowiązuje się do niedokonywania jakiegokolwiek kopiowania i utrwalania danych osobowych poza systemami informatycznymi Zleceniodawcy
7. W przypadku wykorzystania sieci publicznej, każda osoba realizująca Umowę zobowiązuje się do stosowania zabezpieczonego przed podsłuchem połączenia zdalnego (VPN, SSL, podać inne).
8. Każda osoba realizująca Umowę zobowiązuje się do pracy w systemach Zleceniodawcy z użyciem uwierzytelnienia

§8
Postanowienia końcowe

1. Umowa zastępuje wszelkie inne ustalenia dokonane pomiędzy Zleceniobiorcą a Zleceniodawcą dotyczące przetwarzania danych osobowych bez względu na to, czy zostały uregulowane umową czy innym instrumentem prawnym.
2. W zakresie nieuregulowanym Umową mają zastosowanie przepisy prawa obowiązującego na terenie Rzeczypospolitej Polskiej, w tym Rozporządzenia.
3. Wszelkie zmiany Umowy wymagają formy pisemnej pod rygorem nieważności.
4. Umowę sporządzono w dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze Stron.

....

Wyższa Szkoła Ekonomiczna
w Białymstoku
15-703 Białystok, ul. Zwycięstwa 14/3
tel./fax (85) 652-00-24, tel. (85) 652-09-97
REGON 050383717, NIP 542-17-21-656

Załącznik Nr 8
do dokumentu Polityka Ochrony danych osobowych w Wyższej Szkole Ekonomicznej w Białymstoku

Instrukcja zarządzania RODO – wykaz zabezpieczeń RODO w Wyższej Szkole Ekonomicznej w Białymstoku

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 i pomieszczeń biurowych, archiwów, serwerowni, miejsc przechowywania kopii bezpieczeństwa.
2. Funkcjonuje portiernia.
3. Wdrożono zasadę dostępu osób nieupoważnionych do miejsc przetwarzania danych wyłącznie w obecności osoby upoważnionej (praca personel sprzątający zobowiązana do zachowania poufności).
4. Rozmieszczenie komputerów, drukarek, xero 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 zamykanymi na klucz, funkcjonuje system alarmowy.
10. Archiwum zabezpieczono drzwiami zamykanymi na klucz.
11. Dokumentację oraz dane na nośnikach zabezpieczono w zamkniętych na klucz niemetalowych szafach, metalowych szafach, sejfie ogniotrwałym.
12. Obiekt i pomieszczenia chronione są przez system alarmowy.
13. Zapewniono ochronę obiektu - ochrona własna, firma ochroniarska - w przypadku uruchomienie alarmu.
14. Wdrożono system stref ograniczonego dostępu.
15. Stosowana jest **Polityka kluczy - załącznik 1.**

3. Zabezpieczenia techniczne

1. Zastosowano UPS do serwera, UPS podtrzymujący zasilanie serwera, UPS na kluczowych elementów systemu IT.
2. Zastosowano monitoring wizyjny w obrębie obiektu i w otoczeniu.
3. Serwerownia wyposażona w gaśnice.
4. Serwerownia z materiałów niepalnych.
5. Czujnik dymu w serwerowni.
6. Podłoga techniczna w serwerowni.
7. Klimatyzacja w serwerowni.
8. Archiwum - składowanie dokumentacji papierowej na podwyższeniu.
9. Digitalizacja dokumentów archiwalnych.

4. Procedura nadawania i odbierania upoważnień i uprawnień do przetwarzania danych osobowych.

Celem procedury jest minimalizacja ryzyka przetwarzania danych przez osoby nieupoważnione.

1. Do danych osobowych mogą być dopuszczone wyłącznie osoby posiadające upoważnienie do przetwarzania danych osobowych nadane przez Rektora.
2. Upoważnienie do przetwarzania danych osobowych zawiera zakres nadawanych uprawnień do przetwarzania danych osobowych określonych stanowiskiem pracy lub zakresem obowiązków i czynności, do którego nadawane są uprawnienia, datę nadania upoważnienia oraz, jeśli upoważnienie nadawane jest terminowo, datę wygaśnięcia upoważnienia lub warunków jego wygaśnięcia.
3. Jeżeli osoba mająca przetwarzać dane osobowe nie jest pracownikiem Uczelni, z wnioskiem o nadanie jej upoważnienia oraz uprawnień w systemie informatycznym występuje kierownik jednostki zlecającej upoważnianej osobie przetwarzanie danych osobowych.
4. Prowadzony jest rejestr nadanych upoważnień. **Wzór rejestru upoważnień stanowi - Załącznik 2**
5. Odebranie upoważnienia do przetwarzania danych osobowych może mieć miejsce, gdy:
   1) z pracownikiem/zleceniobiorcą została rozwiązana (zakończona) umowa o pracę lub współpraca,
   2) zakres obowiązków służbowych pracownika uległ zmianie, która spowodowała utratę potrzeby przetwarzania danych osobowych,
   3) osoba spowodowała swoim celowym działaniem incydent mający negatywny wpływ na bezpieczeństwo przetwarzanych danych osobowych,
   4) istnieje uzasadniona obawa, że przetwarzanie danych osobowych przez osobę wiąże się z poważnym ryzykiem utraty poufności, integralności lub dostępności tych danych.
6. Upoważnienie do przetwarzania danych osobowych przygotowywane jest w 3 egzemplarzach: po jednym dla upoważnianej osoby, Inspektora Ochrony Danych, oraz do akt osobowych pracownika.
7. Po udzieleniu upoważnienia do przetwarzania danych osobowych, każdemu użytkownikowi nadawany jest dostęp do systemu informatycznego (np. stacji roboczej, dysku sieciowego, programu lub aplikacji, poczty elektronicznej) w formie indywidualnego identyfikatora (loginu).
8. Nadawanie, zmiana, odbieranie uprawnień użytkownika do zasobów i aplikacji odbywa się na polecenie Rektora.
9. Za wykonanie czynności nadawania, zmiany, odbierania uprawnień w systemie informatycznym użytkownikowi odpowiada Administrator SI.
10. Obowiązuje zasada minimalizacji uprawnień.
11. Identyfikator użytkownika po wyrejestrowaniu z systemu informatycznego nie może być przydzielany innej osobie.
12. Użytkowników obowiązuje zasada pracy na własnym koncie. Zabronione jest umożliwianie innym osobom pracy na koncie innego użytkownika.
13. Administrator SI 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 w administrowanym systemie.

5. Metody i środki uwierzytelnienia (polityka haseł)

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

1. Użytkownik uzyskuje dostęp do systemu informatycznego, w którym przetwarzane są dane osobowe, wyłącznie poprzez podanie własnego identyfikatora (loginu) i hasła.
2. Identyfikator jest w sposób jednoznaczny przypisany użytkownikowi. Użytkownik jest odpowiedzialny za wszystkie czynności wykonane przy użyciu jego identyfikatora.
3. Identyfikator składa się z dowolnej liczby znaków, musi być jednak unikatowy w danym systemie i jednoznacznie identyfikować w nim użytkownika.
4. Jeśli system nie umożliwia użytkownikowi przy tworzeniu konta (rejestracji użytkownika) podania hasła, użytkownik otrzymuje, przekazane mu w poufny sposób, od administratora systemu hasło początkowe z chwilą przystąpienia do pracy w systemie informatycznym i jest zobowiązany zmienić je po pierwszym zalogowaniu na sobie tylko znany ciąg znaków.
5. Hasło składa się z co najmniej 8 znaków.
6. Hasło musi zawierać małe i wielkie litery oraz cyfry lub znaki specjalne.
7. Hasło nie powinno się składać z kombinacji znaków mogących ułatwić jego odgadnięcie lub odszyfrowanie przez osoby nieuprawnione (np.: imię, nazwisko użytkownika).
8. Administrator określa dla danego systemu ewentualne dodatkowe wymagania co do stosowanych metod i środków uwierzytelniania użytkownika, na przykład konieczność cyklicznego wymuszania przez system zmiany hasła.
9. Hasło nie może być zapisane w miejscu dostępnym dla osób nieuprawnionych i należy je zachować w tajemnicy, również po upływie ważności.
10. Użytkownik nie może udostępniać osobom nieuprawnionym (w tym również innym pracownikom upoważnionym do przetwarzania danych osobowych w danym systemie, z wyłączeniem w szczególnych przypadkach administratorów systemu) swojego identyfikatora oraz hasła.
11. W przypadku, gdy istnieje podejrzenie, że hasło mogła poznać osoba nieuprawniona, użytkownik zobowiązany jest niezwłocznie zmienić hasło oraz powiadomić o tym fakcie Administratora SI (a ten Inspektora Ochrony Danych) lub bezpośrednio Inspektora Ochrony Danych.
12. Komputery, na których przetwarza się (w tym przechowuje) dane osobowe muszą być zabezpieczone przed nieuprawnionym dostępem poprzez ustanowienie hasła w systemie operacyjnym (np. Windows).
13. Hasła administracyjne zarejestrowane w programie EWIDA STANDARD (baza danych sprzętu i oprogramowania).
14. W przypadku utraty uprawnień przez osobę administrującą systemem należy niezwłocznie zmienić hasła, do których miała dostęp.

6. Procedura tworzenia kopii zapasowych

1. Dane osobowe przetwarzane w systemie informatycznym oraz systemy (aplikacje) przetwarzające dane osobowe podlegają zabezpieczeniu poprzez tworzenie kopii zapasowych.
2. Za tworzenie kopii zapasowych zbiorów danych osobowych oraz systemów odpowiedzialny jest administrator SI lub inna osoba przez niego wyznaczona.
3. Kopie zapasowe serwera (z zawartością plików i baz danych) tworzone są w sposób zautomatyzowany w oparciu o (specjalne oprogramowanie / skrypt / wykorzystanie programowej funkcji serwera)
4. Kopie bezpieczeństwa sporządzane są dla dokumentacji gromadzonej na dyskach stacji roboczych użytkowników oraz całej zawartości dysku C (system i aplikacje) na dodatkowym dysku twardym o nazwie „BACKUP"
5. Kopie dysków systemowych stacji roboczych robione są automatycznie w trakcie instalowania aktualizacji systemowych oraz ważnych zmian w oprogramowaniu
6. Całościowe kopie baz danych systemów finansowo-księgowych sporządzane są przez uruchomienie funkcji backup w trakcie uruchomienia programu finansowo-księgowego przynajmniej raz w tygodniu i są zapisywane na dedykowanym serwerze, a następnie kopiowane na nośnik CD-R, bądź DVD-R
7. Całościowe kopie bazy danych Uczelnianego Systemu Obsługi Studiów „USOS" tworzone są codziennie w oparciu o automatyczny skrypt, a następnie zapisywane są na nośnik CD-R.
8. Kopie istotnych plików sporządzane są na wydzielonym serwerze SMB oraz na nośnikach danych w postaci płyt CD-R oraz DVD-R
9. Kopie zapasowe danych z systemu informatycznego wykonywane na płytach CD-R oraz DVD-R lub innych nośnikach danych przechowuje się w innych pomieszczeniach niż te, w których przechowywane są zbiory danych wykorzystywane do bieżącej pracy. Kopie zapasowe przechowuje się w sposób uniemożliwiający nieuprawnione przejęcie, modyfikacje, uszkodzenie lub zniszczenie.
10. Dostęp do nośników danych z kopiami zapasowymi danych osobowych przetwarzanych w systemach informatycznych ma wyłącznie administrator systemów informatycznych (lub osoba wyznaczona przez niego do wykonywania kopii zapasowych)
11. Za zniszczenie kopii zapasowych sporządzanych indywidualnie (lokalnie) przez użytkownika systemu odpowiada użytkownik.
12. Kopie takie należy niszczyć niezwłocznie po ustaniu ich przydatności.
13. Niszczenie dysków z kopiami odbywa się komisyjnie. Nośniki niszczone są przez fizyczne zniszczenie, pocięcie po wymontowaniu z obudowy.

7. Utylizacja elektronicznych nośników i wydruków oraz czyszczenie danych

1. Przeznaczone do likwidacji uszkodzone lub przestarzałe nośniki danych zawierające dane osobowe (twarde dyski z danymi osobowymi ze stacji roboczych i laptopów / pendrive / pamięci flash / dyski SSD / płyty DVD / telefony komórkowe / smartfony, pozbawia się wcześniej zapisu tych danych, a w przypadku, gdy nie jest to możliwe, uszkadza się je w sposób uniemożliwiający ich odczytanie, to jest trwale i nieodwracalnie niszczy fizycznie do stanu uniemożliwiającego rekonstrukcję nośnika i odzyskanie danych. Powyższe czynności wykonuje się komisyjnie wg **Załącznika nr 3 - Protokół zniszczenia uszkodzonych nośników.**

2. Nośniki informacji zamontowane w sprzęcie IT a w szczególności twarde dyski muszą być wyczyszczone programem do wielokrotnego nadpisywania danych (co uniemożliwia odczytanie zapisanych na nośniku danych), zanim zostaną przekazane poza obszar Uczelni (np. sprzedaż lub darowizna komputerów stacjonarnych / laptopów / smartfonów).
3. Dokumentacja papierowa niszczona jest w niszczarkach paskowych.
4. Dokumentacja papierowa niszczona jest za pośrednictwem firmy niszczącej dokumenty. Firma zobowiązana jest do wykazania się bezpieczną procedurą utylizacji.

8. Procedura zabezpieczenia systemu informatycznego

8.1. Bezpieczeństwo przetwarzania danych poza siedzibą uczelni

1. Użytkownicy komputerów przenośnych wynoszonych poza obszar organizacji, na których są przetwarzane dane osobowe są zobowiązani do przestrzegania zasad bezpieczeństwa i podpisania **Regulaminu użytkowania komputerów przenośnych - Załącznik 4.**
2. Dyski przenośne / pendrive wynoszone poza organizację muszą być zaszyfrowane.
3. Sprzęt mobilny (smartfony/tablety) zabezpieczono mechanizmem uwierzytelniania.
4. Sprzęt mobilny wyposażony jest w oprogramowanie umożliwiające blokowanie dostępu, czyszczenie zawartości.

8.2. Ochrona przed nieautoryzowanym dostępem do sieci lokalnej

Sposób zabezpieczenia systemu informatycznego przed działaniem złośliwego oprogramowania

1. Za **ochronę systemu informatycznego** przed złośliwym oprogramowaniem (przed wirusami komputerowymi, końmi trojańskimi, robakami komputerowymi, oprogramowaniem szpiegującym, wykradającym dane lub hasła dostępu itp.) odpowiada administrator systemu.
2. Na każdym komputerze, na którym przetwarzane są dane osobowe musi być zainstalowane oprogramowanie chroniące komputer przed złośliwym oprogramowaniem (program antywirusowy).
3. Za działanie programu antywirusowego na komputerze, na którym przetwarzane są dane osobowe odpowiada użytkownik komputera.
4. Program antywirusowy musi być aktywny przez cały czas pracy komputera, na którym przetwarzane są dane osobowe.
5. Niedozwolone jest wyłączanie, blokowanie i odinstalowywanie przez użytkownika oprogramowania zabezpieczającego komputer przed złośliwym oprogramowaniem oraz nieautoryzowanym dostępem z zewnątrz (skaner, program antywirusowy, firewall itp.).
6. W przypadku stwierdzenia na komputerze złośliwego oprogramowania, użytkownik zobowiązany jest do zaprzestania wykonywania jakichkolwiek czynności w komputerze i niezwłocznego powiadomienia o stwierdzeniu złośliwego oprogramowania administratora systemu (jeśli dotyczy) lub Inspektora Ochrony Danych.
7. Niedozwolone jest otwieranie wiadomości poczty elektronicznej i załączników od „niezaufanych" nadawców.

Stosowane zabezpieczenia mają na celu zabezpieczenie systemów informatycznych przed nieautoryzowanym dostępem do sieci lokalnej np. przez programy szpiegujące, hackerów.

1. Dokonuje się aktualizacji oprogramowania (firmware / sterowniki) urządzeń sieciowych oraz innych (np. w urządzeniach jak: routery, switche, access pointy, firewalle, drukarki, skanery).
2. Dokonuje się konfiguracji urządzeń sieciowych oraz innych (routery, switche, access pointy, firewalle, 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 / CMS (Wordpress, Joomla) / Dedykowany CMS / Adobe / Flash / Java / inne). Aktualizacja dokonywana jest zgodnie z zaleceniami producentów oraz opinią rynkową co do bezpieczeństwa i stabilności nowych wersji (np. aktualizacje, service pack-i, łatki).
4. Usługi sieciowe są monitorowane (np. DHCP, DNS, SSH, http, telnet, FTP, SMTP, SNMP) celem utrzymania niezbędnych usług a deaktywacji tych nieużywanych.
5. Zastosowano system antywirusowy na stacjach roboczych (ESET ENDPOINT ANTIVIRUS).
6. Zastosowano filtr antyspamowy.
7. Stosowany jest Ubiquiti UniFi Security Gateway PRO 4 (sprzętowy firewall zintegrowany z routerem) oraz programowe firewalle na serwerach i stacjach roboczych.
8. Zastosowano technikę NAT.
9. Zastosowano Sewer proxy oraz dedykowane przełączniki sieciowe dla chronionego segmentu sieci (Kwestura oraz Dział Obsługi Studentów).
10. Sieć bezprzewodową zabezpieczono technologią WPA2 PSK.
11. Separacja sieci wewnętrznej Ethernet od sieci WIFI.
12. Separacja sieci wewnętrznej Ethernet pracowników administracji od sieci przeznaczonej dla studentów i wykładowców oraz gości.

8.3. Zabezpieczenia infrastruktury IT

1. Serwer „USOS" wyposażono w macierz dyskową w celu ochrony danych osobowych przed skutkami awarii pamięci dyskowej.
2. Zastosowano wirtualizację serwera.
3. Zabezpieczono hasłem dostęp do portów fizycznych (gniazd - np. szeregowych, USB, Ethernet) celem uniemożliwienia zmian konfiguracji przez osoby nieupoważnione.
4. Dokonano dezaktywacji nieużywanych gniazd sieciowych (np. przez wypięcie przewodów lub wyłączenie portów na switchu).
5. Dopuszczono do użycia wyłącznie zakwalifikowane pendrive wraz z blokadą dopuszczenia pozostałych.
6. Przed czasowym opuszczeniem stanowiska pracy, użytkownik zobowiązany jest wywołać blokowany hasłem wygaszacz ekranu (WINDOWS + L) lub wylogować się z systemu bądź z programu.
7. Ustawienie monitorów uniemożliwiające wgląd w dane przez osoby postronne.

8.4. 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. Kluczowe aplikacje/bazy z danymi osobowym zabezpieczono przed eksportem danych do plików (np. tekstowych, .csv, .xls).
4. Zabezpieczono interfejsy programistyczne poprzez zmianę domyślnych loginów i haseł / wyłączenie dostępu zdalnego, gdy nie jest wymagany.
5. Zabezpieczenie testowych wersji aplikacji poprzez zmianę domyślnych loginów i haseł / wyłączenie dostępu zdalnego, gdy nie jest wymagany.
6. Szyfrowanie baz danych.
7. W kluczowych aplikacjach stosuje się terminację sesji.
8. Stosuje się szyfrowanie poczty wychodzącej (SSL).
9. Dla aplikacji webowych stosowane jest szyfrowanie połączeń internetowych z użyciem protokołu SSL.
10. Formularze kontaktowe na stronach www zabezpieczono protokołem SSL.
11. URL Aplikacji webowych są skrócone/pozbawione końcówek alfanumerycznych.
12. Zabezpiecza się logi systemowe przed sfałszowaniem.

9. Procedura wykonywania przeglądów i konserwacji

1. Wszelkie prace związane z naprawami i konserwacją systemu informatycznego lub komputera, na którym przetwarzane są dane osobowe wykonywane są wyłącznie przez Administratora systemu.
2. Administrator systemu okresowo sprawdza możliwość odtworzenia danych z kopii zapasowej.
3. Za terminowość przeprowadzania przeglądów i konserwacji oraz ich prawidłowy przebieg odpowiada administrator systemu.
4. Nieprawidłowości w działaniu systemu informatycznego oraz oprogramowania są usuwane przez administratora systemu, a ich przyczyny analizowane w celu uniknięcia podobnych zdarzeń w przyszłości.
5. Stosowany jest system wykrywania słabości i zagrożeń (Skanery podatności).
6. Stosowane jest oprogramowanie do inwentaryzacji infrastruktury IT / zainstalowanego oprogramowania na stacjach roboczych (serwerach) oraz do kontroli procesu aktualizacji (patche / łatki).
7. Stosowany jest system do monitoringu aktywności użytkowników.
8. Administrator SI jest odpowiedzialny za monitoring/przegląd logów aktywności aplikacji /baz.
9. Administrator SI jest odpowiedzialny za monitoring/przegląd logów aktywności oraz uprawnień użytkowników i administratorów.
10. Administrator SI odpowiada za optymalizację zasobów serwerowych, wielkości pamięci i dysków, optymalizację baz danych.
11. Administrator SI odpowiada za sprawdzanie poprawności działania systemu IT, w tym: stacji roboczych, serwerów, drukarek, baz danych, aplikacji, poczty email.

12. Administrator SI odpowiada za identyfikację i przyjmowanie zgłoszeń o nieprawidłowościach w działaniu systemu informatycznego oraz oprogramowania celem ich niezwłocznego usunięcia.
13. 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.
14. 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).
15. 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.
16. Rekomendowane jest korzystanie z serwisu, który dokonuje napraw u klienta (umowy gwarancyjne on-site).
17. Czynności konserwacyjne i naprawcze wykonywane przez osoby nieposiadające upoważnień do przetwarzania danych (np. specjalistów z firm zewnętrznych) muszą być wykonywane pod nadzorem osób upoważnionych.
18. 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.

REKTOR

dr Aleksander Prokopiuk

Załącznik nr 1

Polityka kluczy

1. Polityka kluczy obejmuje Budynki przy ul. Zwycięstwa 14/3 (budynek główny uczelni) oraz budynek przy ul. Zwycięstwa 14/2 (budynek przedszkola).
2. Z uwagi na specyfikę pracy uczelni, budynek główny uczelni funkcjonuje w sposób ciągły, przez siedem dni w tygodniu, budynek przedszkola od poniedziałku do piątku.
3. Upoważnieni do pobierania kluczy do pomieszczeń są wyłącznie pracownicy pracujący w tych pomieszczeniach i osoby upoważnione przez kierowników jednostek.
4. Klucze do pomieszczeń pozostają pod osobistym nadzorem osób upoważnionych. Klucze do pomieszczeń wydawane są z pomieszczenia portierni z odnotowaniem w zeszycie pobrań kluczy i zdawane do pomieszczenia portierni.
5. Klucze do pomieszczeń szczególnie chronionych np. serwerowni, archiwum wydawane są osobom upoważnionym i pozostają pod ich osobistym nadzorem.
6. Dostęp osób trzecich do tych pomieszczeń odbywa się pod ścisłym nadzorem osób upoważnionych.
7. Klucze zapasowe przechowywane są w oddzielnym, zamkniętym na klucz pomieszczeniu, w zamkniętej na klucz gablocie. 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.
8. Klucze służące do zabezpieczenia biurek i szaf muszą być jednoznacznie opisane.
9. W godzinach pracy klucze pozostają pod nadzorem pracowników, którzy ponoszą pełną odpowiedzialność za ich należyte zabezpieczenie.
10. Po zakończeniu pracy, klucze służące do zabezpieczenia biurek i szaf muszą być przechowywane w zabezpieczonym miejscu.
11. 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, ew. aktywacji alarmu.
12. Naruszenie zasad polityki kluczy może spowodować wyciągnięcie konsekwencji wynikających z art. 52 kodeksu pracy oraz z art. 363 § 1. kodeksu cywilnego.

Załącznik nr 2

Wzór Rejestru upoważnień

Rejestr osób przetwarzających dane osobowe w Wyższej Szkole Ekonomicznej w Białymstoku					
L.p.	**Imię i nazwisko**	**Stanowisko służbowe**	**Data nadania upoważnienia**	**Data ustania upoważnienia**	**Uwagi**

Załącznik nr 3

Protokół zniszczenia uszkodzonych nośników komputerowych

Białystok, dnia .....r.

Protokół nr .....
zniszczenia uszkodzonych nośników komputerowych
.....
(jednostka organizacyjna)

Dnia ..... komisja powołana przez .....

(data) (imię, nazwisko i stanowisko osoby powołującej komisję)

w składzie:
1. Przewodniczący: .....
2. Członkowie: .....
.....

dokonała trwałego zniszczenia nośników komputerowych:

L.p.	Nazwa	Nr ewidencyjny	Sposób zniszczenia	Uwagi

Dokonanie w/w czynności zostaje potwierdzone własnoręcznymi podpisami komisji:

.....
.....
.....

Jednostka organizacyjna

ADMINISTRATOR SI
.....

Załącznik nr 4

Regulamin użytkowania komputerów przenośnych

1. Każdy Użytkownik komputera przenośnego winien zapoznać się z Regulaminem użytkowania komputerów przenośnych oraz pisemnie zobowiązać się do jego przestrzegania.

2. Użytkownicy nie mogą wynosić poza obiekty WSE urządzeń (w tym również komputerów przenośnych) oraz nośników danych zawierających dane osobowe bez pisemnej zgody Rektora.

3. W przypadku przechowywania na komputerze przenośnym danych osobowych lub stanowiących tajemnicę Pracodawcy, Użytkownik zobowiązany jest do ich przechowywania na dysku szyfrowanym, zabezpieczonym co najmniej 8 znakowym hasłem (duże, małe litery, znaki specjalne lub cyfry).

4. 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.

5. Użytkownik zobowiązany jest do zabezpieczenia komputera przenośnego w czasie transportu, a w szczególności:
a) zaleca się przenoszenie go w specjalnym futerale. *Dobrym sposobem na zmylenie potencjalnego złodzieja jest przenoszenie komputera przenośnego w zwykłej teczce-aktówce. Sugeruje to przenoszenie dokumentów a ukrywa fakt transportu komputera przenośnego.*
b) zabrania się pozostawiania komputera przenośnego w samochodzie podczas postoju w miejscu publicznym bez nadzoru. *W chwili obecnej złodzieje dysponują aparaturą umożliwiającą wykrywanie nawet ukrytych komputerów przenośnych.*
c) podczas jazdy samochodem zaleca się przechowywanie komputera przenośnego pod tylnym siedzeniem kierowcy. *Zabrania się przewożenia go np. na siedzeniach, co może skutkować kradzieżą na skrzyżowaniach, przejściach dla pieszych lub w korkach.*

6. W przypadku, gdy komputer przenośny pozostawiony jest w miejscu dostępnym dla osób nieupoważnionych, Użytkownik jest zobowiązany do stosowania kabla zabezpieczającego. W szczególności dotyczy to zabezpieczenia komputera na stanowisku pracy, podczas konferencji, prezentacji, szkoleń, targów itp

7. W przypadku pozostawiania komputerów przenośnych w biurze zaleca się umieszczanie ich po zakończeniu pracy w zamykanych szafkach

8. Użytkownik komputera przenośnego jest zobowiązany do regularnego tworzenia kopii bezpieczeństwa danych na serwerze lub na określonych nośnikach (pendrive, CD, DVD). Nośniki z takimi kopiami powinny być przechowywane w bezpiecznym miejscu, z uwzględnieniem ochrony przed dostępem osób niepowołanych.

9. Pracując na komputerze przenośnym w miejscach publicznych i środkach transportu, Użytkownik zobowiązany jest chronić wyświetlane na monitorze informacje przed wglądem osób nieupoważnionych.

Zapoznałem się z treścią Regulaminu użytkowania komputerów przenośnych i zobowiązuję się do przestrzegania zasad w nim zawartych

Czytelny podpis Użytkownika

.....

Wyższa Szkoła Ekonomiczna
w Białymstoku
15-703 Białystok, ul. Zwycięstwa 14/3
tel./fax (85) 652-00-24, tel. (85) 652-09-97
REGON 050383717, NIP 542-17-21-656

Załącznik Nr 9
do dokumentu Polityka Ochrony danych osobowych w Wyższej Szkole Ekonomicznej w Białymstoku

Regulamin Ochrony Danych Osobowych w Wyższej Szkole Ekonomicznej w Białymstoku

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

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 zabezpieczenia przed zniszczeniem lub uszkodzeniem. Za sprzęt IT rozumie się: komputery stacjonarne, monitory, drukarki, skanery, ksera, laptopy, służbowe tablety i smartfony.
2. Użytkownik jest zobowiązany zgłosić zagubienie, utratę lub zniszczenie powierzonego mu sprzętu IT.
3. Samowolne instalowanie otwieranie (demontaż) sprzętu IT, instalowanie dodatkowych urządzeń (np. twardych dysków, pamięci) do lub podłączanie jakichkolwiek niezatwierdzonych urządzeń do systemu informatycznego jest zabronione.
4. 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).
5. 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 młotkiem) jeśli nie, zobowiązany jest do przekazania Administratorowi SI nośników przeznaczonych do zniszczenia.
6. Użytkownicy komputerów przenośnych, na których znajdują się dane osobowe zobowiązani są do stosowania zasad bezpieczeństwa zawartych w **Regulaminie użytkowania komputerów przenośnych.**

2 ZARZĄDZANIE UPRAWNIENIAMI - PROCEDURA ROZPOCZĘCIA, ZAWIESZENIA I ZAKOŃCZENIA PRACY

1. Każdy użytkownik (np. komputera stacjonarnego, laptopa, dysku sieciowego, programów, w których użytkownik pracuje, poczty elektronicznej) musi posiadać swój własny indywidualny identyfikator (login) do logowania się.
2. Tworzenie kont użytkowników wraz z uprawnieniami (np. komputera stacjonarnego, laptopa, dysku sieciowego, programów w których użytkownik pracuje, poczty elektronicznej) odbywa się na polecenie Rektora WSE lub kierowników jednostek organizacyjnych a wykonywane przez Administratora SI.
3. Użytkownik nie może samodzielnie zmieniać swoich uprawnień.
4. Każdy użytkownik musi posiadać indywidualny identyfikator. Zabronione jest umożliwianie innym osobom pracy na koncie innego użytkownika.
5. Zabrania się pracy wielu użytkowników na wspólnym koncie.
6. Użytkownik (np. komputera stacjonarnego, laptopa, dysku sieciowego, programów w których użytkownik pracuje, poczty elektronicznej) rozpoczyna pracę z użyciem identyfikatora i hasła.
7. Użytkownik jest zobowiązany do powiadomienia Administratora SI o próbach logowania się do systemu osoby nieupoważnionej, jeśli system to sygnalizuje.
8. W przypadku, gdy użytkownik podczas próby zalogowania się zablokuje system, zobowiązany jest powiadomić o tym Administratora SI.

9. Użytkownik jest zobowiązany do uniemożliwienia osobom niepowołanym (np. studentom, klientom, pracownikom innych działów) wglądu do danych wyświetlanych na monitorach – tzw. **Polityka czystego ekranu.**
10. Przed czasowym opuszczeniem stanowiska pracy, użytkownik zobowiązany jest wywołać blokowany hasłem wygaszacz ekranu (WINDOWS + L) lub wylogować się z systemu bądź z programu.
11. Zabrania się uruchamiania jakiejkolwiek aplikacji lub programu na prośbę innej osoby, dotyczy to zwłaszcza programów przesłanych za pomocą poczty elektronicznej lub wskazanych w formie odnośnika internetowego.
12. Po zakończeniu pracy, użytkownik zobowiązany jest:
    a) wylogować się z systemu informatycznego, a następnie wyłączyć sprzęt komputerowy
    b) zabezpieczyć stanowisko pracy, w szczególności wszelką dokumentację oraz nośniki elektroniczne, na których znajdują się dane osobowe.

3 POLITYKA HASEŁ

1. Hasła powinny składać się z co najmniej 8 znaków.
2. Hasła powinny zawierać duże litery + małe litery + cyfry (lub znaki specjalne).
3. 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.
4. 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.
5. W przypadku ujawnienia hasła – należy natychmiast je zmienić.
6. Hasła muszą być zmieniane co 60 / 90 dni.
7. Jeżeli system nie wymusza zmiany haseł, użytkownik zobowiązany jest do samodzielnej zmiany hasła.
8. Użytkownik systemu w trakcie pracy w aplikacji może zmienić swoje hasło.
9. Użytkownik zobowiązuje się do zachowania hasła w poufności, nawet po utracie przez nie ważności.
10. Zabrania się używania w serwisach internetowych takich samych lub podobnych haseł jak w systemie komputerowym uczelni.
11. Zabrania się stosowania tego samego hasła jako zabezpieczenia w dostępie do różnych systemów.
12. Zabrania się definiowania haseł, w których jeden człon pozostaje niezmienny, a drugi zmienia się według przewidywalnego wzorca (np. Anna001, Anna002, Anna003 itd.). Nie powinno się też stosować haseł, w których któryś z członów stanowi imię, nazwę lub numer miesiąca lub inny możliwy do odgadnięcia klucz.

4 ZABEZPIECZENIE DOKUMENTACJI PAPIEROWEJ Z DANYMI OSOBOWYMI

1. Upoważnieni pracownicy są zobowiązani do stosowania tzw. „**Polityki czystego biurka**". Polega ona na zabezpieczaniu (zamykaniu) dokumentów oraz nośników np. w szafach,

biurkach, pomieszczeniach przed kradzieżą lub wglądem osób nieupoważnionych po godzinach pracy lub podczas ich nieobecności w trakcie godzin pracy.
2. Upoważnieni pracownicy / współpracownicy zobowiązani są do niszczenia dokumentów i wydruków w niszczarkach. Zabrania się pozostawiania dokumentów z danymi osobowymi poza zabezpieczonymi pomieszczeniami, np. w korytarzach, w kserokopiarkach, drukarkach, w pomieszczeniach konferencyjnych.
3. Zabrania się wyrzucania niezniszczonych dokumentów na śmietnik lub porzucania ich na zewnątrz, np., na terenach publicznych, miejskich lub w lesie.

5 ZASADY WYNOSZENIA NOŚNIKÓW Z DANYMI POZA SIEDZIBĘ WSE

1. Użytkownicy nie mogą wynosić na zewnątrz uczelni wymiennych elektronicznych nośników informacji z zapisanymi danymi osobowymi bez zgody Rektora. Do takich nośników zalicza się: wymienne twarde dyski, pen-drive, płyty CD, DVD, pamięci typu Flash
2. Dane osobowe wynoszone poza uczelnię muszą być zaszyfrowane (szyfrowane dyski, zabezpieczone hasłem pliki).
3. Należy zapewnić bezpieczne przewożenie dokumentacji papierowej w plecakach, teczkach.
4. W przypadku, gdy dokumenty przewozi pracownik/współpracownik, zobowiązany jest do zabezpieczenia przewożonych dokumentów przed zagubieniem i kradzieżą.

6 ZASADY KORZYSTANIA Z INTERNETU

1. 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 Administratora SI i tylko w uzasadnionych przypadkach.
2. Zabrania się wchodzenia na strony, 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).
3. Nie należy w opcjach przeglądarki internetowej włączać opcji autouzupełniania formularzy i zapamiętywania haseł.
4. 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.
5. Należy zachować szczególną ostrożność w przypadku podejrzanego żądania lub prośby zalogowania się na stronę (np. na stronę banku, portalu społecznościowego, e-sklepu, poczty mailowej) lub podania naszych loginów i haseł, PIN-ów, numerów kart płatniczych przez Internet. Szczególnie tyczy się to żądania podania takich informacji przez rzekomy bank.
6. Zabrania się samowolnego podłączania do komputerów modemów, telefonów komórkowych i innych urządzeń dostępowych (np.: typu BlueConnect, iPlus, OrangeGo).

Zabronione jest też łączenie się przy pomocy takich urządzeń z Internetem w chwili, gdy komputer użytkownika podłączony jest do sieci.

7 ZASADY KORZYSTANIA Z POCZTY ELEKTRONICZNEJ

1. Przesyłanie danych osobowych z użyciem maila poza organizację może odbywać się tylko przez osoby do tego upoważnione.
2. W przypadku przesyłania danych osobowych poza uczelnię należy wysyłać pliki zaszyfrowane/spakowane (np. programem 7 zip, winzipem, winrarem) i zabezpieczone hasłem, gdzie hasło powinno być przesłane do odbiorcy telefonicznie lub SMS.
3. W przypadku zabezpieczenia plików hasłem, obowiązuje minimum 8 znaków: duże i małe litery i cyfry lub znaki specjalne a hasło należy przesłać odrębnym mailem lub inną metodą, np. telefonicznie lub SMS-em
4. Użytkownicy powinni zwracać szczególną uwagę na poprawność adresu odbiorcy dokumentu.
5. Zaleca się, aby użytkownik podczas przesyłania danych osobowych mailem zawarł w treści prośbę o potwierdzenie otrzymania i zapoznania się z informacją przez adresata.
6. **WAŻNE:** Nie otwierać załączników (.zip, .xlsm, .pdf, .exe) w mailach!!!!! Są to zwykle „wirusy", które infekują komputer oraz często pozostałe komputery w sieci. WYSOKIE RYZYKO UTRATY BEZPOWROTNEJ UTRATY DANYCH.
7. **WAŻNE:** Nie wolno „klikać" na hiperlinki w mailach, gdyż mogą to być hiperlinki do stron z „wirusami". Użytkownik „klikając" na taki hiperlink infekuje komputer oraz inne komputery w sieci. WYSOKIE RYZYKO UTRATY BEZPOWROTNEJ UTRATY DANYCH.
8. Należy zgłaszać Administratorowi SI przypadki podejrzanych emaili.
9. Użytkownicy nie powinni rozsyłać „niezawodowych" emaili w formie „łańcuszków szczęścia", np. Życzenia Świąteczne adresowane do 230 osób.
10. Podczas wysyłania maili do wielu adresatów jednocześnie, należy użyć metody „Ukryte do wiadomości – UDW". Zabronione jest rozsyłanie maili do wielu adresatów z użyciem opcji „Do wiadomości"!
11. Użytkownicy powinni okresowo kasować niepotrzebne maile.
12. Konta pocztowe służbowe są odseparowane od poczty prywatnej.
13. Mail służbowy jest przeznaczony wyłącznie do wykonywania obowiązków służbowych.
14. Zaleca się ograniczenie do niezbędnego minimum wysyłanie korespondencji służbowej na prywatne skrzynki pocztowe pracowników lub innych osób.
15. Użytkownicy mają prawo korzystać z poczty mailowej dla celów prywatnych wyłącznie okazjonalnie i powinno być to ograniczone do niezbędnego minimum.
16. Zabrania się użytkownikom poczty elektronicznej konfigurowania swoich kont pocztowych do automatycznego przekierowywania wiadomości na adres zewnętrzny.
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. Przy korzystaniu z maila, Użytkownicy mają obowiązek przestrzegać prawa własności przemysłowej i prawa autorskiego.

19. Użytkownicy nie mają prawa korzystać z maila w celu rozpowszechniania treści o charakterze obraźliwym, niemoralnym lub niestosownym wobec powszechnie obowiązujących zasad postępowania.

8 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 administratora SI lub bezpośredniego przełożonego.

9 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 informatyka, 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 organizacji 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, pen-drive 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.

10 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 ma 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. Osoba dopuszczona do przetwarzania odbywa szkolenie z zasad ochrony danych osobowych oraz musi być zapoznana z treścią niniejszego Regulaminu.
3. Osoby zapoznane z treścią niniejszego Regulaminu ODO lub przeszkolone zobowiązane są podpisać stosowne 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.
6. Zabrania się ujawniania na grupach dyskusyjnych, forach internetowych, blogach itp. szczegółów dotyczących funkcjonowania uczelni i placówek, dla których jest ona organem prowadzącym, w tym informacji na temat sprzętu i oprogramowania, z jakiego korzysta uczelnia i placówki przez nią prowadzone, oraz informacji kontaktowych innych, niż ogólnodostępne w materiałach zewnętrznych.
7. Zabrania się wywieszania w miejscach ogólnodostępnych (np. gablotach na korytarzach) jakichkolwiek list lub innych dokumentów zawierających dane osobowe. Wyjątkiem są przypadki wynikające z przepisów prawa określających jawność danego procesu (np. zawierające tylko **imię i nazwisko** listy z wynikami rekrutacji na studia, listy

studentów z podziałem na grupy ćwiczeniowe, laboratoryjne itp., wyniki postępowań w ramach zamówień publicznych, w których zwycięzcami są osoby fizyczne,).

8. Dopuszcza się możliwość publikowania na stronach internetowych WSE lub w jakiejkolwiek innej formie następujących danych osobowych pracowników: imię, nazwisko, stopień/tytuł naukowy, stanowisko, służbowy numer telefonu, służbowy adres e-mail. Zabrania się publikowania na stronach internetowych WSE lub w jakiejkolwiek innej formie innych danych pracowników (w tym prywatnych numerów telefonów, prywatnych adresów e-mail, adresów prywatnych stron WWW)
9. Publikacja wizerunku pracownika na stronie internetowej WSE jest dozwolona tylko po uzyskaniu zgody pracownika udzielonej na piśmie.
10. Zabronione jest publikowanie na stronach internetowych i w mediach społecznościowych klubu dziecięcego, przedszkola i szkoły podstawowej danych osobowych dzieci i rodziców. Dopuszcza się możliwość publikowania imienia i nazwiska dziecka w związku z jego udziałem w konkursach lub wydarzeniach, po wyrażeniu zgody rodzica w formie pisemnej.
11. Publikacja wizerunku dziecka dopuszczalna jest jedynie po wyrażeniu zgody rodzica w formie pisemnej.

11 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.

REKTOR

dr Aleksander Prokopiak

Wyższa Szkoła Ekonomiczna
w Białymstoku
15-703 Białystok, ul. Zwycięstwa 14/3
tel./fax (85) 652-00-24, tel. (85) 652-09-97
REGON 050383717, NIP 542-17-21-656

Załącznik Nr 10 *do dokumentu Polityka Ochrony danych osobowych w Wyższej Szkole Ekonomicznej w Białymstoku*

OŚWIADCZENIE O POUFNOŚCI

1) Zobowiązuję się do zachować w tajemnicy dane osobowe, z którymi zapoznałam/em się w trakcie wykonywania swoich obowiązków służbowych, zarówno w czasie trwania stosunku pracy/umowy zlecenia/współpracy jak i po jego zakończeniu.
2) Zobowiązuję się chronić dane osobowe przed dostępem do nich osób do tego nieupoważnionych, zabezpieczać je przed zniszczeniem i nielegalnym ujawnieniem.
3) Zostałam/em poinformowana/y o obowiązujących w Wyższej Szkole Ekonomicznej w Białymstoku procedurach przetwarzania danych osobowych ustanowionych w dokumentach: **Polityka bezpieczeństwa przetwarzania danych osobowych w Wyższej Szkole Ekonomicznej w Białymstoku,** załącznik Nr 8 – **Instrukcja zarządzania RODO** oraz załącznik Nr 9 – **Regulamin ochrony danych osobowych.** Zobowiązuję się do przestrzegania wszelkich standardów przetwarzania danych osobowych uregulowanych w przedmiotowych dokumentach.
4) Zostałam/em poinformowana/y o wynikających z obowiązujących przepisów prawa powszechnego obowiązkach nałożonych na osobę upoważnioną do przetwarzania danych osobowych oraz administratorów tych danych, t. j. z postanowieniami Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) oraz Ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. 2018 poz. 1000).
5) Jestem świadoma/y sankcji grożących za wszelkie naruszenia przyjętych standardów przetwarzania danych, w tym odpowiedzialności karnej określonej przepisami ustawy o ochronie danych osobowych oraz odpowiedzialności dyscyplinarnej związanej z ciężkim naruszeniem podstawowych obowiązków pracowniczych.

Białystok, dnia .....

.....
Podpis Pracownika

Załącznik Nr 11

do dokumentu Polityka Ochrony danych osobowych w Wyższej Szkole Ekonomicznej w Białymstoku

Wyższa Szkoła Ekonomiczna
w Białymstoku
15-703 Białystok, ul. Zwycięstwa 14/3
tel./fax (85) 652-00-24, tel. (85) 652-09-97
REGON 050383717, NIP 542-17-21-656

REJESTR NARUSZEŃ OCHRONY DANYCH OSOBOWYCH ORAZ INCYDENTÓW NARUSZEŃ BEZPIECZEŃSTWA DANYCH

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