Zarządzenie nr 15/2016
Rektora Wyższej Szkoły Gospodarki Euroregionalnej
im. Alcide De Gasperi w Józefowie
z dnia 5 września 2016 roku

w sprawie wprowadzenia w Wyższej Szkoły Gospodarki Euroregionalnej im. Alcide De Gasperi w Józefowie „Polityki bezpieczeństwa i instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych"

Działając na podstawie §29 ust. 1 pkt. 12 Statutu Wyższej Szkoły Gospodarki Euroregionalnej im. Alcide De Gasperi w Józefowie w zw. z art. 36 ust. 2 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. nr 101, poz. 926, z późn. zm.) i §3 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz.U. Nr 100, poz. 1024), zarządza się co następuje:

§ 1

W Wyższej Szkoły Gospodarki Euroregionalnej im. Alcide De Gasperi w Józefowie wprowadza się „Politykę bezpieczeństwa i instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych", stanowiące załącznik do niniejszego zarządzenia.

§ 2

Zobowiązuje się kierowników jednostek organizacyjnych Uczelni do zapoznania pracowników z Instrukcją zarządzania systemem informatycznym ochrony danych osobowych.

§3

Zarządzenie wchodzi w życie z dniem podpisania z mocą obowiązująca od roku akademickiego 2016/2017.

Rektor
Wyższej Szkoły Gospodarki Euroregionalnej
im. Alcide De Gasperi w Józefowie

.....
dr Tadeusz Graca

Załącznik
do zarządzenia nr 15/2016
Rektora Wyższej Szkoły Gospodarki Euroregionalnej
im. Alcide De Gasperi w Józefowie
z dnia 5 września 2016 roku

„Polityka bezpieczeństwa i instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych" w Wyższej Szkoły Gospodarki Euroregionalnej im. Alcide De Gasperi w Józefowie

Wstęp

Władze Wyższej Szkoły Gospodarki Euroregionalnej im. Alcide De Gasperi w Józefowie świadome wagi zagrożeń prywatności, w tym zwłaszcza zagrożeń danych osobowych przetwarzanychw związku z wykonywaniem zadań administratora danych, deklarują podejmowanie wszelkich możliwych działań koniecznych do zapobiegania zagrożeniom.

W celu zapewnienia ochrony danych osobowych przetwarzanych w Uczelni przed wszelkiego rodzaju zagrożeniami, tak wewnętrznymi jak i zewnętrznymi, świadomymi lub nieświadomymi, wprowadza się niniejszą „Politykę bezpieczeństwa i instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych" w Wyższej Szkoły Gospodarki Euroregionalnej im. Alcide De Gasperi w Józefowie.

Dokument został opracowany przy uwzględnieniu regulacji zawartych w § 4 i 5 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024). Dokument uwzględnia m.in. zestaw procedur opisujących zasady bezpieczeństwa danych osobowych przetwarzanych w zbiorach papierowych i w systemach informatycznych.

I. Definicje

Przez użyte określenia należy rozumieć:

1) Uczelnia, WSGE – Wyższa Szkoła Gospodarki Euroregionalnej im. Alcide De Gasperi w Józefowie;
2) polityka – „Polityka bezpieczeństwa i instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych" w Wyższej Szkoły Gospodarki Euroregionalnej im. Alcide De Gasperi w Józefowie;
3) Administrator Bezpieczeństwa Informacji i Danych Osobowych (ABIDO) – osoba wyznaczona przez Rektora, odpowiedzialna za organizację ochrony danych osobowych i decydująca o celachi środkach przetwarzania danych osobowych;
4) ustawa – ustawa z dnia 29 sierpnia 1997 r. ochronie danych osobowych (Dz. U. z 2002 roku nr 101 poz. 926, z późn. zm.);
5) rozporządzenie – rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024);
6) dane osobowe (dane) – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej;
7) zbiór danych – zestaw danych osobowych posiadający określoną strukturę, prowadzony według określonych kryteriów oraz celów;
8) usuwanie danych – zniszczenie danych osobowych lub taka ich modyfikacja, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą;
9) zgoda osoby, której dane dotyczą – oświadczenie woli, którego treścią jest zgoda na przetwarzanie danych osobowych tego, kto składa oświadczenie; zgoda nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści;
10) baza danych osobowych – zbiór uporządkowanych powiązanych ze sobą tematycznie danych zapisanych np. w pamięci zewnętrznej komputera; złożona z elementów o określonej strukturze - rekordów lub obiektów, w których są zapisane dane osobowe;
11) przetwarzanie danych – wykonywanie jakichkolwiek operacji na danych osobowych, np. zbieranie, utrwalanie, opracowywanie, udostępnianie, zmienianie, usuwanie;
12) system informatyczny (system) – zespół współpracujących ze sobą urządzeń, danych eksploatowanych w tym zespole, programów, procedur przetwarzania informacji i narzędzi

programowych; w systemie tym pracuje co najmniej jeden komputer centralny i system ten tworzy sieć teleinformatyczną administratora danych;

13) administrator systemu – osoba nadzorująca pracę systemu informatycznego oraz wykonująca w nim czynności wymagające specjalnych uprawnień;
14) użytkownik – upoważniony do przetwarzania danych osobowych pracownik Uczelni, któremu nadano identyfikator i przyznano hasło, uprawniony do pracy w systemie informatycznym zgodnie z zakresem obowiązków służbowych.
15) zabezpieczenie systemu informatycznego – wdrożenie stosownych środków administracyjnych, technicznych i fizycznych w celu zabezpieczenia zasobów technicznych oraz ochrony przed modyfikacją, zniszczeniem, nieuprawnionym dostępem i ujawnieniem lub pozyskaniem danych osobowych, a także ich utratą;
16) hasło – ciąg znaków literowych, cyfrowych lub innych, znany jedynie użytkownikowi;
17) identyfikator – ciąg znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym;
18) uwierzytelnianie – działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu;
19) integralność danych – właściwość zapewniająca, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany;
20) poufność danych – właściwość zapewniająca, że dane nie są udostępniane nieupoważnionym podmiotom;
21) rozliczalność – właściwość zapewniająca, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi;
22) sieć telekomunikacyjna – sieć telekomunikacyjna w rozumieniu art. 2 pkt 35 ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz. U. z 2014 r. poz. 243, z późn. zm.);
23) publiczna sieć telekomunikacyjna – sieć publiczna w rozumieniu art. 2 pkt 29 ustawy z ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz. U. z 2014 r. poz. 243, z późn. zm.);
24) teletransmisja – przesyłanie informacji za pośrednictwem sieci telekomunikacyjnej;
25) nośnik komputerowy (wymienny) – nośnik służący do zapisu i przechowywania informacji, np. płyty CD/DVD, dyski twarde, pamięci przenośne.

II. Zadania Administratora Bezpieczeństwa Informacji i Danych Osobowych.

1. ABIDO powołuje Rektor.
2. Do najważniejszych obowiązków ABIDO należy:
   1) organizacja bezpieczeństwa i ochrony danych osobowych zgodnie z wymogami Ustawy,
   2) zapewnienie przetwarzania danych zgodnie z uregulowaniami Polityki.
   2) wydawanie i anulowanie upoważnień do przetwarzania danych osobowych,
   3) prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych,
   4) prowadzenie postępowania wyjaśniającego w przypadku naruszenia ochrony danych osobowych, prowadzenie postępowania wyjaśniającego w przypadku naruszenia ochrony danych osobowych,
   5) nadzór nad bezpieczeństwem danych osobowych,
   6) kontrola działań komórek organizacyjnych pod względem zgodności przetwarzania danych z przepisami o ochronie danych osobowych,
   7) inicjowanie i podejmowanie przedsięwzięć w zakresie doskonalenia ochrony danych osobowych.
3. ABIDO ma prawo:
   1) wyznaczania, rekomendowania i egzekwowania wykonania zadań związanych z ochroną danych osobowych w całej Uczelni,
   2) wstępu do pomieszczeń w których zlokalizowane są zbiory danych i przeprowadzenia niezbędnych badań lub innych czynności kontrolnych w celu oceny zgodności przetwarzania danych z Ustawą,

3) żądać złożenia pisemnych lub ustnych wyjaśnień w zakresie niezbędnym do ustalenia stanu faktycznego,
4) żądać okazania dokumentów i wszelkich danych mających bezpośredni związek z problematyką kontroli,
5) żądać udostępnienia do kontroli urządzeń, nośników oraz systemów informatycznych służących do przetwarzania danych.

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

Wykaz budynków i pomieszczeń wchodzących w skład obszaru przetwarzania danych osobowych	
Adres: Wyższa Szkoła Gospodarki Euroregionalnej im. Alcie De Gasperi w Józefowie, ul. Sienkiewicza 4	Pomieszczenia: dziekanat (parter, numery pomieszczeń: 4) rektorat (parter, numery pomieszczeń: 12) Biuro Współpracy Zagranicznej (2. piętro, numery pomieszczeń: 27) księgowość (2. piętro, numery pomieszczeń: 28)
Adres: Zamiejscowy Wydział Nauk Społecznych w Mińsku Mazowieckim	Pomieszczenia: połączenie VPN z Józefowem
Adres: punkty rekrutacyjne	Pomieszczenia: połączenie VPN z Józefowem

IV. Opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi

1. Dane osobowe są przetwarzane przy zastosowaniu systemów informatycznych oraz tradycyjnych, w zbiorach ewidencyjnych oraz poza zbiorami.
2. W Uczelni przetwarzane są następujące zbiory danych:
   1) dane osobowe studentów,
   2) dane osobowe byłych studentów, w tym absolwentów,
   3) dane osobowe kandydatów na studia,
   4) dane osobowe pracowników,
   5) dane osobowe kandydatów do pracy,
   6) dane osobowe stażystów,
   7) dane osobowe byłych stażystów,
   8) dane osobowe byłych pracowników,
   9) dane osobowe osób, z którymi zawarto umowy cywilno-prawne,
   10) dane osobowe osób, które posiadały umowy cywilno-prawne,
   11) dane osobowe osób korzystających z Biblioteki,
   12) dane osobowe osób, które korzystały z Biblioteki,
   13) dane osobowe słuchaczy,
   14) dane osobowe byłych słuchaczy i absolwentów studiów podyplomowych,
   15) dane osobowe uczestników kursów,
   16) dane osobowe byłych uczestników kursów.
3. Uczelnia posługuje się systemami informatycznymi wymienionymi w poniższej tabeli.

Wykaz zbiorów danych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych				
Lp.	**Zbiór danych**	**Programy zastosowane do przetwarzania / Nazwa zasobu**	**Lokalizacja zbioru/zasobu**	**Miejsce przetwarzania danych**
1.	Baza danych programu	Proakademia, wirtualny	Sewer APR/	WSGE

	ProAkademia	dziekanat	serwerownia	
2.	Baza programu Biblioteka	Biblioteka + www	Serwer/ serwerownia	WSGE
3.	księgowość	Ramzes, raksgl	księgowość	WSGE

V. Sposób przepływu danych pomiędzy poszczególnymi systemami

1. Przetwarzanie danych osobowych odbywa się z wykorzystaniem systemów informatycznych wykonanych w różnych technologiach, przechowujących informacje w różnych systemach zarządzania bazą danych.
2. Schematy przepływu danych pomiędzy systemami informatycznymi, zastosowanymi w celu przetwarzania danych osobowych wykonuje ABIDO, zgodnie z relacjami występującymi pomiędzy tymi systemami.
3. Przepływ danych pomiędzy systemami zastosowanymi w celu przetwarzania danych osobowych może odbywać się w postaci przepływu jednokierunkowego lub przepływu dwukierunkowego.
4. Przesyłanie danych pomiędzy systemami może odbywać się w sposób manualny, przy wykorzystaniu nośników zewnętrznych (w szczególności dyskietki, płyty CD i DVD, dysku wymiennego, pamięci przenośnych) lub w sposób półautomatyczny, przy wykorzystaniu funkcji eksportu (importu) danych za pomocą teletransmisji (w szczególności poprzez wewnętrzną sieć teleinformatyczną).
5. Przetwarzanie danych osobowych w uczelni realizowane jest w różnych systemach informatycznych, dostępnych również poza podstawowym obszarem przetwarzania danych. W związku z dostępnością niektórych systemów z sieci publicznej stosuje się wysoki poziom zabezpieczenia systemów informatycznych służących do przetwarzania danych osobowych.

VI. Środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych

1. Zabezpieczenia organizacyjne
   a) wyznaczono ABIDO nadzorującego przestrzeganie zasad ochrony przetwarzanych danych osobowych oraz została opracowana i wdrożona „Polityka bezpieczeństwa i instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych";
   b) do przetwarzania danych zostały dopuszczone wyłącznie osoby posiadające upoważnienia nadane przez ABIDO (Załącznik nr 1);
   c) prowadzona jest ewidencja osób upoważnionych do przetwarzania danych (Załącznik nr 2);
   d) osoby zatrudnione przy przetwarzaniu danych zostały zaznajomione z przepisami dotyczącymi ochrony danych osobowych oraz w zakresie zabezpieczeń systemu informatycznego;
   e) osoby zatrudnione przy przetwarzaniu danych osobowych obowiązane zostały do zachowania ich w tajemnicy;
   f) przetwarzanie danych osobowych dokonywane jest w warunkach zabezpieczających dane przed dostępem osób nieupoważnionych;
   g) przebywanie osób nieuprawnionych w pomieszczeniach, gdzie przetwarzane są dane osobowe jest dopuszczalne tylko w obecności osoby zatrudnionej przy przetwarzaniu danych osobowych oraz w warunkach zapewniających bezpieczeństwo danych;
   h) stosuje się pisemne umowy powierzenia przetwarzania danych dla współpracy z podwykonawcami przetwarzającymi dane osobowe.
2. Zabezpieczenia ochrony fizycznej danych osobowych.
3. Zabezpieczenia sprzętowe infrastruktury informatycznej i telekomunikacyjnej.
4. Zabezpieczenia stosuje się dla fizycznych elementów systemu, ich połączeń oraz systemów operacyjnych.

5. Zabezpieczenia narzędzi programowych i baz danych.
6. Zabezpieczenia (techniczne i programowe) stosuje się dla procedur, aplikacji, programów i innych narzędzi programowych przetwarzających dane osobowe.

VII. Polityka kluczy

1. Ogólne zasady.
   a) Polityka kluczy obejmuje obszary przetwarzania danych osobowych.
   b) Klucze zapasowe przechowywane są w odpowiednio zabezpieczonym miejscu.
2. Nadawanie upoważnień.
   a) Upoważnienia do pobierania kluczy do pomieszczeń, w których przetwarzane są dane osobowe mają wyłącznie osoby upoważnione przez kierowników jednostek, w których dane te są przetwarzane.
   b) Udzielenie/anulowanie upoważnienia wymaga wprowadzenia osoby do ewidencji, prowadzonej w postaci Załącznika nr 2.
3. Wydawanie i zdawanie kluczy.
   a) Klucze do pomieszczeń, w których przetwarzane są dane osobowe są wydawane za potwierdzeniem. Klucze do pomieszczeń pozostają pod osobistym nadzorem osób upoważnionych. Wydający klucze ma prawo weryfikacji tożsamości pobierającego z ewidencją osób upoważnionych.
   b) Klucze do serwerowni są wydawane za potwierdzeniem. Klucze te pozostają pod osobistym nadzorem osób upoważnionych. Wydający klucze ma prawo weryfikacji tożsamości pobierającego z ewidencją osób upoważnionych. Dostęp osób trzecich odbywa się pod ścisłym nadzorem pracowników Działu IT.
   c) Pracownicy upoważnieni zobowiązani są do odnotowania pobrania i zdania kluczy.
4. Wydawanie i zdawanie kluczy w trybie nadzwyczajnym.
   a) Wydawanie kluczy zapasowych upoważnionym pracownikom może odbywać się tylko w uzasadnionych sytuacjach oraz przypadkach awaryjnych za zgodą przełożonego.
   b) Klucze zapasowe po ich wykorzystaniu należy niezwłocznie zwrócić do miejsca ich przechowywania.
5. Bieżące postępowanie w trakcie dnia pracy.
   a) W godzinach pracy klucze pozostają pod nadzorem pracowników, którzy ponoszą pełną odpowiedzialność za ich należyte zabezpieczenie.
   b) Zabrania się pozostawiania kluczy w biurkach i szafach podczas chwilowej nieobecności osób upoważnionych w pomieszczeniu.
   c) Po zakończeniu pracy, klucze służące do zabezpieczenia biurek i szaf muszą być przechowywane w bezpiecznym miejscu określonym przez kierownika jednostki organizacyjnej.
   d) Po zakończeniu pracy, pracownicy są zobowiązani do:
      - wyłączenia i zabezpieczenia urządzeń elektronicznych oraz elektrycznych,
      - wyłączenia oświetlenia,
      - zabezpieczenia i zamknięcia okien i drzwi.
   e) Za przestrzeganie ww. zasad odpowiada kierownik jednostki organizacyjnej.

VIII. Zabezpieczenia infrastruktury informatycznej i telekomunikacyjnej

1. Zabezpieczenia infrastruktury przed skutkami awarii zasilania.
   a) UPS-y podtrzymujące zasilanie serwera i pozostałych kluczowych elementów systemu IT,
   b) listwy przepięciowe.
2. Zabezpieczenia stanowisk komputerowych wykorzystywanych do przetwarzania danych osobowych.

a) Programy zainstalowane na komputerach obsługujących przetwarzanie danych osobowych są użytkowane z zachowaniem praw autorskich i posiadają aktualne licencje.

3. Zabezpieczenia przed nieuprawnionym dostępem do danych osobowych, w tym środków zapewniających rozliczalność wykonywanych operacji.
   a) Lokalizacja urządzeń komputerowych (komputerów, drukarek itp.) uniemożliwia osobom niepowołanym (np. pracownikom lub studentom) dostęp do nich.
   b) Dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem (identyfikatora użytkownika oraz hasła.
4. Zabezpieczenia sprzętowe i programowe służące ochronie poufności danych przesyłanych drogą elektroniczną (środków ochrony transmisji).
   a) Zastosowano środki kryptograficznej ochrony danych dla danych osobowych przekazywanych drogą teletransmisji z użyciem VPN.
   b) Dostęp do środków teletransmisji zabezpieczono za pomocą mechanizmów uwierzytelnienia.
5. Zabezpieczenia sprzętowe i programowe przed szkodliwym oprogramowaniem i nieuprawnionym dostępem do przetwarzanych danych.
   a) Zastosowano programy antywirusowe chroniące przed szkodliwym oprogramowaniem takim, jak np. robaki, wirusy, konie trojańskie, rootkity.
   b) Użyto systemu Firewall oraz IDS/IPS do ochrony dostępu do sieci .

IX. Zabezpieczenia baz danych i oprogramowania przetwarzającego dane osobowe

1. Dostęp do zbioru danych osobowych (do bazy danych i do programu) wymaga uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła. Zastosowano mechanizm wymuszający okresową zmianę haseł dostępu do zbioru danych osobowych.
2. Zastosowano mechanizm umożliwiający automatyczną rejestrację identyfikatora użytkownika i datę pierwszego wprowadzenia danych osobowych.
3. Zastosowano środki umożliwiające określenie praw dostępu do wskazanego zakresu danych w ramach przetwarzanego zbioru danych osobowych.
4. Zastosowano systemowe środki pozwalające na określenie odpowiednich praw dostępu do zasobów informatycznych, w tym zbiorów danych osobowych dla poszczególnych użytkowników systemu informatycznego.
5. Zainstalowano wygaszacze ekranów na stanowiskach, na których przetwarzane są dane osobowe.
6. Zastosowano mechanizm automatycznej blokady dostępu do systemu informatycznego służącego do przetwarzania danych osobowych w przypadku dłuższej nieaktywności pracy użytkownika (automatyczny wygaszacz ekranu).
7. Zastosowano oprogramowanie antywirusowe na stanowiskach, na których przetwarzane są dane osobowe.

X. Procedura dostępu podmiotów zewnętrznych

1. ABIDO prowadzi rejestr podmiotów zewnętrznych, którym udostępnia dane osobowe oraz podmiotów, którym powierzono przetwarzanie danych osobowych w formie usługi zewnętrznej. (Załącznik nr 3)
2. ABIDO powierza do przetwarzania dane osobowe będące w jego obszarze fizycznym podmiotom zewnętrznym w oparciu o umowę poufności, nakładając obowiązki:
   a) Podmiot zewnętrzny zobowiązany jest do zachowania poufności powierzonych danych i przetwarzania ich zgodnie z celem umowy.
   b) Podmiot zewnętrzny zobowiązany jest do przetwarzania danych zgodnie z zakresem i celem określonym w umowie powierzenia przetwarzania danych osobowych.

c) Podmiot zewnętrzny zobowiązany jest do stosowania zabezpieczeń określonych w rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz.U. Nr 100, poz. 1024).

XI. Procedura korzystania z Internetu

1. Zabrania się zgrywania na dysk twardy komputera oraz uruchamiania jakichkolwiek nielegalnych programów oraz plików pobranych z niewiadomego źródła.
2. Użytkownik ponosi odpowiedzialność za szkody spowodowane przez oprogramowanie instalowane z Internetu.
3. Zabrania się wchodzenia na strony, na których prezentowane są informacje o charakterze przestępczym, hakerskim, pornograficznym, lub innym zakazanym przez prawo (na większości stron tego typu jest zainstalowane szkodliwe oprogramowanie, infekujące w sposób automatyczny system operacyjny komputera szkodliwym oprogramowaniem).
4. Nie należy w opcjach przeglądarki internetowej włączać opcji autouzupełniania formularzy i zapamiętywania haseł.
5. W przypadku korzystania z szyfrowanego połączenia przez przeglądarkę, należy zwracać uwagę na pojawienie się odpowiedniej ikonki (kłódka) oraz adresu www rozpoczynającego się frazą "https:".

XII. Procedura korzystania z poczty elektronicznej

1. Przesyłanie danych osobowych z użyciem e-maila poza Uczelnię może odbywać się tylko przez osoby do tego upoważnione
2. W przypadku zabezpieczenia plików hasłem, obowiązuje minimum 8 znaków: wielkie i małe litery oraz cyfry lub znaki specjalne, a hasło należy przesłać odrębnym e-mailem lub inną metodą, np. telefonicznie lub SMS-em.
3. Użytkownicy powinni zwracać szczególną uwagę na poprawność adresu odbiorcy dokumentu.
4. Zaleca się, aby użytkownik podczas przesyłania danych osobowych e-mailem zawarł w treści prośbę o potwierdzenie otrzymania i zapoznania się z informacją przez adresata.
5. Podczas wysyłania maili do wielu adresatów jednocześnie należy użyć metody „Ukryte do wiadomości – UDW".

XIII. Procedura nadawania uprawnień do przetwarzania danych osobowych

1. Zarządzane uprawnieniami użytkowników.
   a) Przyznanie, anulowanie upoważnienia do przetwarzania danych osobowych w systemie informatycznym lub w zbiorze papierowym realizowane jest na podstawie upoważnienia przygotowanego przez ABIDO.
   b) Przed nadaniem upoważnienia, ABIDO zobowiązany jest do sprawdzenia, czy osoba upoważniona:
      - odbyła szkolenie z zakresu przestrzegania zasad bezpieczeństwa danych osobowych lub została zapoznana z „Polityką bezpieczeństwa i instrukcją zarządzania systemem informatycznym służącym do przetwarzania danych osobowych";
      - podpisała oświadczenie o zachowaniu poufności;
      - będzie przetwarzać dane osobowe w zakresie i celu określonym upoważnieniem.
   c) ABIDO jest zobowiązany do aktualizacji upoważnień i ich zakresu (np. z powodu zatrudnienia, urlopu, dostępu do zbiorów lub zmiany stanowiska pracy).

d) Zakres uprawnień w systemach informatycznych dla danej osoby określa upoważnienie.
e) Po akceptacji upoważnienia, ABIDO nadaje identyfikator oraz uprawnienia użytkownika w systemach informatycznych i aplikacjach.
f) Identyfikator użytkownika po wyrejestrowaniu z systemu informatycznego nie może być przydzielany innej osobie.
g) ABIDO odpowiada za przechowywanie i aktualizację wszystkich upoważnień.
h) ABIDO opowiada za prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych.

2. Zarządzanie uprawnieniami administratorów.
   a) Hasła do wszystkich systemów znane są tylko ABIDO.
   b) W przypadkach awaryjnych (np. nieobecność ABIDO) hasło może być przekazane osobie zastępującej ABIDO za jego zgodą i wiedzą.

XIV. Metody i środki uwierzytelnienia

1. Ogólne zasady postępowania z hasłami.
   a) ABIDO informuje e-mailem lub ustnie użytkownika o nadaniu pierwszego hasła do systemu.
   b) Użytkownik systemu zobowiązany jest do niezwłocznej zmiany tego hasła.
   c) Użytkownik systemu w trakcie pracy w aplikacji może zmienić swoje hasło.
   d) Hasła nie mogą być powszechnie używanymi słowami. W szczególności nie należy jako haseł wykorzystywać: dat, imion, nazwisk, inicjałów, numerów rejestracyjnych samochodów, numerów telefonów.
   e) Użytkownik zobowiązuje się do zachowania hasła w poufności, nawet po utracie przez nie ważności.
   f) Zabronione jest zapisywanie haseł w sposób jawny oraz przekazywanie ich innym osobom.
2. Hasła do programów przetwarzających dane osobowe.
   a) Hasło dostępu do programów składają się co najmniej 8 znaków.
   b) Hasło składa się z wielkich i małych liter oraz z cyfr lub znaków specjalnych.
   c) Zaleca się zmianę hasła raz na 30 dni lub zmianę hasła wymusza system.

XV. Procedura rozpoczęcia, zawieszenia i zakończenia pracy

1. Użytkownik rozpoczyna pracę z systemem informatycznym przetwarzającym dane osobowe z użyciem identyfikatora i hasła.
2. Użytkownik jest zobowiązany do powiadomienia ABIDO o próbach logowania się do systemu osoby nieupoważnionej, jeśli system to sygnalizuje.
3. Użytkownik jest zobowiązany do uniemożliwienia osobom niepowołanym (np. nieupoważnionym pracownikom innych działów, studentom) wglądu do danych wyświetlanych na monitorach komputerowych.
4. Przed czasowym opuszczeniem stanowiska pracy, użytkownik zobowiązany jest wylogować się z systemu.
5. Po zakończeniu pracy, użytkownik zobowiązany jest:
   a) wylogować się z systemu, a następnie wyłączyć sprzęt komputerowy,
   b) zabezpieczyć stanowisko pracy, w szczególności wszelką dokumentację oraz nośniki elektroniczne i tradycyjne, na których znajdują się dane osobowe.

XVI. Sposób, miejsce i okres przechowywania elektronicznych nośników informacji i wydruków

1. Zabezpieczenie elektronicznych nośników informacji.
   a) Nośniki danych są przechowywane w sposób uniemożliwiający dostęp do nich osób nieupoważnionych, jak również zabezpieczający je przed zagrożeniami środowiskowymi (np. zalanie, pożar, wpływ pól elektromagnetycznych).
   b) Zabrania się wynoszenia poza obszar Uczelni wymiennych nośników informacji, a w szczególności twardych dysków z zapisanymi danymi osobowymi bez zgody ABIDO.
   c) W sytuacji przekazywania nośników z danymi osobowymi poza obszar Uczelni należy stosować następujące zasady bezpieczeństwa:
      - adresat powinien zostać powiadomiony o przesyłce,
      - nadawca powinien sporządzić kopię przesyłanych danych,
      - dane przed wysłaniem powinny zostać zaszyfrowane, a hasło podane adresatowi inną drogą,
      - stosować bezpieczne koperty depozytowe,
      - adresat powinien powiadomić nadawcę o otrzymaniu przesyłki.
   d) Użytkownicy są zobowiązani do niezwłocznego i trwałego usuwania/kasowania danych osobowych z nośników informacji po ustaniu powodu ich przechowywania.
   e) Podlegające likwidacji uszkodzone lub przestarzałe nośniki, w szczególności twarde dyski z danymi osobowymi są komisyjnie niszczone w sposób fizyczny (Załącznik nr 4).
   f) Nośniki informacji zamontowane w sprzęcie IT, a w szczególności twarde dyski z danymi osobowymi, powinny być wymontowane lub wyczyszczone specjalistycznym oprogramowaniem, zanim zostaną przekazane poza obszar Uczelni.
2. Zabezpieczenie dokumentów i wydruków.
   a) Dokumenty i wydruki trwałe z danymi osobowymi przechowuje się w archiwum lub w zabezpieczonych fizycznie pomieszczeniach, biurkach i szafach.
   b) Pracownicy są zobowiązani do zabezpieczania dokumentów (np. zamykanie dokumentów na klucz w szafach, biurkach) przed dostępem osób nieupoważnionych podczas swojej nieobecności w pomieszczeniach lub po zakończeniu pracy.
   c) Zabrania się pozostawiania wydruków oraz ksero na drukarkach, skanerach i kserokopiarkach.
   d) Pracownicy są zobowiązani do niszczenia dokumentów i tymczasowych wydruków niezwłocznie po ustaniu celu ich przetwarzania.
   e) Za zapewnienie bezpieczeństwa dokumentów i wydruków odpowiedzialni są kierownicy jednostek organizacyjnych oraz podległe im osoby przetwarzające dane osobowe.

XVII. Procedura zabezpieczenia systemu informatycznego

1. Ochrona antywirusowa.
   a) System antywirusowy zainstalowano na stacjach roboczych.
   b) System antywirusowy zapewnia ochronę: systemu operacyjnego, przechowywanych plików, poczty elektronicznej.
   c) Użytkownicy zobowiązani są do skanowania plików programem antywirusowym.
   d) ABIDO zapewniają stałą aktywność programu antywirusowego, tzn. program antywirusowy musi być aktywny podczas pracy systemu informatycznego przetwarzającego dane osobowe.
   e) Aktualizacja definicji wirusów odbywa się automatycznie.
   f) W przypadku stwierdzenia pojawienia się wirusa, każdy użytkownik winien powiadomić ABIDO.
2. Ochrona przed nieautoryzowanym dostępem do sieci lokalnej.
   a) Firewall sprzętowy.
   b) Mechanizmy kontroli dostępu do sieci oraz technika NAT.

3. Aktualizacje oprogramowania.
   a) Dział IT odpowiada za aktualizację oprogramowania zgodnie z zaleceniami producentów oraz opinią o bezpieczeństwie i stabilności nowych wersji (np. aktualizacje, service packi).
   b) Dział IT odpowiada za zapewnienie licencjonowanego oprogramowania do przetwarzania danych osobowych.

XVIII. Instrukcja alarmowa

1. Instrukcja definiuje katalog zagrożeń i incydentów zagrażających bezpieczeństwu danych osobowych oraz opisuje sposób reagowania na nie, a jej celem jest minimalizacja skutków wystąpienia incydentów bezpieczeństwa, ograniczenie ryzyka powstania zagrożeń i występowania incydentów w przyszłości.
2. Każdy pracownik Uczelni, w przypadku stwierdzenia zagrożenia lub naruszenia ochrony danych osobowych, zobowiązany jest poinformować bezpośredniego przełożonego oraz ABIDO.
3. Do typowych zagrożeń bezpieczeństwa danych osobowych należą:
   a) niewłaściwe zabezpieczenie fizyczne pomieszczeń, urządzeń i dokumentów;
   b) niewłaściwe zabezpieczenie sprzętu komputerowego, oprogramowania przed wyciekiem, kradzieżą i utratą danych osobowych;
   c) nieprzestrzeganie zasad ochrony danych osobowych przez pracowników.
4. 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, 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).
5. W przypadku stwierdzenia wystąpienia zagrożenia, ABIDO prowadzi postępowanie wyjaśniające w toku, którego:
   a) ustala zakres i przyczyny zagrożenia oraz jego ewentualne skutki;
   b) inicjuje ewentualne działania dyscyplinarne;
   c) rekomenduje działania prewencyjne (zapobiegawcze) zmierzające do eliminacji podobnych zagrożeń w przyszłości.
6. W przypadku stwierdzenia incydentu (naruszenia), ABIDO prowadzi postępowanie wyjaśniające w toku, którego:
   a) ustala czas wystąpienia naruszenia, jego zakres, przyczyny, skutki oraz wielkość szkód, które zaistniały;
   b) zabezpiecza ewentualne dowody;
   c) ustala osoby odpowiedzialne za naruszenie;
   d) podejmuje działania naprawcze (usuwa skutki incydentu i ogranicza szkody);
   e) inicjuje działania dyscyplinarne;
   f) wyciąga wnioski i rekomenduje działania korygujące zmierzające do eliminacji podobnych incydentów w przyszłości;
   g) dokumentuje prowadzone postępowania.

XIX. Procedura działań korygujących i zapobiegawczych

1. Procedura działań korygujących i zapobiegawczych obejmuje wszystkie te procesy, w których incydenty bezpieczeństwa lub zagrożenia mogą wpłynąć na zgodność z wymaganiami Ustawy, jak również na poprawne funkcjonowanie systemu ochrony danych osobowych.

2. Osobą odpowiedzialną za nadzór nad procedurą jest ABIDO.
3. ABIDO jest odpowiedzialny za analizę incydentów bezpieczeństwa lub zagrożeń ochrony danych osobowych.
4. W przypadku, gdy ABIDO stwierdzi konieczność podjęcia działań korygujących lub zapobiegawczych, określa źródło powstania incydentu lub zagrożenia, zakres działań korygujących lub zapobiegawczych, termin realizacji, osobę odpowiedzialną.
5. ABIDO jest odpowiedzialny za nadzór nad poprawnością i terminowością wdrażanych działań korygujących lub zapobiegawczych.
6. Po przeprowadzeniu działań korygujących lub zapobiegawczych, ABIDO jest zobowiązany do oceny efektywności ich zastosowania.

XX. Szkolenia użytkowników

1. Każdy użytkownik przed dopuszczeniem do pracy z systemem informatycznym przetwarzającym dane osobowe lub zbiorami danych osobowych w wersji papierowej winien być zapoznany z Polityką.
2. Po zapoznaniu się z Polityką, użytkownik zobowiązany jest do podpisania Oświadczenia o poufności (Załącznik nr 5).
3. Dokument ten jest przechowywany w aktach osobowych użytkowników (kopia dokumentu przechowywana jest w dokumentacji ABIDO) i stanowi podstawę do podejmowania działań w celu nadania im uprawnień do korzystania z systemu informatycznego przetwarzającego dane osobowe.
4. W przypadku przeprowadzenia szkolenia wewnętrznego z zasad ochrony danych osobowych zdarzenie powyższe dokumentuje się za pomocą planu szkolenia.

XXI. Postanowienia końcowe

1. Kierownicy jednostek organizacyjnych są obowiązani zapoznać każdego pracownika z treścią Polityki.
2. Wszystkie regulacje dotyczące systemów informatycznych, określone w Polityce dotyczą również przetwarzania danych osobowych w bazach prowadzonych w jakiejkolwiek innej formie.
3. Użytkownicy zobowiązani są do stosowania przy przetwarzaniu danych osobowych postanowień zawartych w niniejszym dokumencie.
4. Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu potraktowane będą jako naruszenie obowiązków pracowniczych.
5. Wobec osoby, która w przypadku naruszenia zabezpieczeń systemu informatycznego lub uzasadnionego domniemania takiego naruszenia nie podjęła działania określonego w niniejszym dokumencie, a w szczególności nie powiadomiła odpowiedniej osoby zgodnie z określonymi zasadami, a także gdy nie zrealizowała stosownego działania dokumentującego ten przypadek, można wszcząć postępowanie dyscyplinarne.
6. W sprawach nieuregulowanych w niniejszym dokumencie mają zastosowanie przepisy ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych oraz wydanych na jej podstawie aktów wykonawczych.

Załącznik nr 1 do
„Polityki bezpieczeństwa i instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych"

UPOWAŻNIENIE/ANULOWANIE UPOWAŻNIENIA*

do przetwarzania danych osobowych
w systemie informatycznym lub w zbiorze w wersji papierowej

Z dniem ..... upoważniam/anuluję* upoważnienie

Użytkownik		

Imię i nazwisko użytkownika:	Jednostka organizacyjna:
Miejsce przetwarzania/Pokój:	Stanowisko:

Opis zakresu uprawnień użytkownika w systemie informatycznym:
P – przeglądanie/drukowanie; Z – zmiana; D – dopisanie; U – usuwanie; N – zakładanie nowych kont/aktualizacja Planu Kont; O/Z – otwarcie/zamknięcie miesiąca/roku; A – archiwizowanie
zakreślić odpowiednio krzyżykiem

Uprawnienia	P	Z	D	U	N	O/Z	A
Moduły programu							
Inne programy							

Uwagi: .....

Zobowiązuję Użytkownika do przestrzegania przepisów dotyczących ochrony danych osobowych oraz wprowadzonych i wdrożonych do stosowania przez ABIDO „Polityki bezpieczeństwa i instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych".

Data i podpis ABIDO:

Załącznik nr 2 do
„Polityki bezpieczeństwa i instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych"

Ewidencja osób upoważnionych do przetwarzania danych osobowych

Zakres upoważnienia		Nazwisko i imię użytkownika	Identyfikator użytkownika	Data nadania upoważnienia	Data ustania upoważnienia
Nazwa zbioru danych	Rodzaj uprawnień				

Legenda:

Uprawnienia: (WG) wgląd, (W) wprowadzanie, (M) modyfikacja, (U) usuwanie, (A) archiwizacja

Dane aktualne na dzień: ...../...../.....

.....
podpis ABIDO

Załącznik nr 3 do
„Polityki bezpieczeństwa i instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych"

Rejestr podmiotów zewnętrznych, którym udostępnia się dane osobowe oraz podmiotów, którym powierzono przetwarzanie danych osobowych w formie usługi zewnętrznej

Lp.	Nazwa firmy	Zakres świadczonych usług	Numer umowy	Uwagi
1.				
2.				
3.				
4.				
5.				

.....
Opracował

.....
Zatwierdził

Załącznik nr 4 do
„Polityki bezpieczeństwa i instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych"

Józefów, dnia.....

Protokół
zniszczenia nośników komputerowych

Dnia ..... komisja powołana przez Administratora Bezpieczeństwa Informacji i Danych Osobowych w składzie:

1. Przewodniczący: .....
2. Członkowie: .....

.....

dokonała trwałego zniszczenia nośników komputerowych:

Lp.	Nazwa	Sposób zniszczenia	Uwagi
1.			
2.			
3.			

Dokonanie ww. czynności zostaje potwierdzone własnoręcznymi podpisami komisji:

.....

.....

.....

Załącznik nr 5 do
„Polityki bezpieczeństwa i instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych"

Oświadczenie
o zachowaniu poufności i zapoznaniu się z przepisami o ochronie danych osobowych

Józefów, dnia.....

.....
(imię i nazwisko)

.....
(stanowisko, jednostka organizacyjna)

Ja niżej podpisany/-a oświadczam, że znana mi jest treść przepisów:

1. Ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych;
2. Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 roku w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych;
3. Zarządzenia nr 9/2016 Rektora Wyższej Szkoły Gospodarki Euroregionalnej im. Alcide De Gasperi w Józefowie z dnia 24 maja 2016 roku w sprawie wprowadzenia w Wyższej Szkoły Gospodarki Euroregionalnej im. Alcide De Gasperi w Józefowie „Polityki bezpieczeństwa i instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych"

i zobowiązuję się

nie ujawniać nikomu w żaden sposób i nie wykorzystywać informacji związanych z przetwarzanymi danymi osobowymi, z którymi się zapoznałem/-am w związku z wykonywaną pracą, oraz zachować w tajemnicy sposoby ich zabezpieczenia.

.....
(podpis pracownika)

.....
(potwierdzenie ważności podpisu, ABIDO)