załącznik nr 1
do zarządzenia
Rektora Powiślańskiej Szkoły Wyższej w Kwidzynie
z dnia 30.09.2008 r.

Polityka bezpieczeństwa w zakresie danych osobowych w Powiślańskiej Szkole Wyższej

§ 1

Dane osobowe w Powiślańskiej Szkole Wyższej w Kwidzynie przetwarzane są w celu realizacji obowiązków oraz uprawnień określonych przepisami prawa, w szczególności statutowych celów szkoły wyższej. W szczególności dane osobowe przetwarza się:

1) dla zabezpieczenia prawidłowego toku realizacji zadań dydaktycznych, naukowych i organizacyjnych Powiślańskiej Szkoły Wyższej wynikających z przepisów ustawy z dnia 27 lipca 2005 r. Prawo o szkolnictwie wyższym (t.j. Dz. U. z 2012 r. poz. 572, z późn. zm.);
2) w celu zapewnienia prawidłowej, zgodnej z prawem i celami Uczelni, polityki personalnej oraz bieżącej obsługi pracy, a także innych stosunków pracy nawiązywanych przez Uczelnię działającą jako pracodawca w rozumieniu art. 3 ustawy z dnia 26 czerwca 1974 r. Kodeks pracy (t.j. z 1998 r. Dz. U. Nr 21, poz. 94, z późn. zm.) lub strona innych stosunków zatrudnienia;
3) dla realizacji innych celów i zadań Powiślańskiej Szkoły Wyższej, z poszanowaniem praw i wolności osób powierzających Uczelni swoje dane.

§ 2

1. Politykę bezpieczeństwa w zakresie ochrony danych osobowych w PSW stosuje się do danych osobowych przetwarzanych w:

1) zbiorach danych tradycyjnych, w szczególności w kartotekach, skorowidzach, księgach, wykazach, archiwaliach i innych zbiorach ewidencyjnych;
2) systemach informatycznych, także w przypadku przetwarzania danych poza zbiorem danych osobowych. Politykę bezpieczeństwa stosuje się w szczególności do: baz danych, zbiorów plików, poczty elektronicznej, zawartości stron www, skanów dokumentów i dokumentów elektronicznych, archiwaliów elektronicznych.

2. Podstawowe zbiory danych osobowych w PSW, to zbiory obejmujące dane: kandydatów na studia, studentów, doktorantów, absolwentów, kandydatów na pracowników, pracowników, byłych pracowników, członków związków i organizacji, stron umów cywilnoprawnych, kontrahentów, uczestników studiów podyplomowych, uczestników projektów europejskich realizowanych, uczestników kursów, szkoleń i konferencji, osób korzystających z Biblioteki PSW.

§ 3

Realizując politykę bezpieczeństwa PSW wyznacza osoby odpowiedzialne za bieżącą realizację postanowień polityki bezpieczeństwa na terenie Uczelni oraz jej jednostek.
Wyznaczeni zostają w szczególności:

1) pełnomocnik ds. danych osobowych,
2) lokalny administrator danych osobowych, odpowiedzialny za nadzór nad przetwarzaniem danych osobowych w jednostkach podległych i odpowiedzialny za nadzór nad przestrzeganiem zasad ochrony danych osobowych w systemach informatycznych;
3) administrator bezpieczeństwa informacji, odpowiedzialny za nadzór nad przestrzeganiem zasad ochrony danych osobowych w systemach informatycznych;

§ 4

1. PSW realizując politykę bezpieczeństwa w zakresie danych osobowych spełnia wymagane obowiązki informacyjne wobec osób, których dane dotyczą oraz zachowuje szczególną staranność w celu ochrony ich interesów, a szczególności zapewnia, aby dane te były:

1) przetwarzane zgodnie z prawem,
2) zbierane dla oznaczonych, zgodnych z prawem celów i nie poddawane dalszemu przetwarzaniu niezgodnemu z tymi celami,
3) merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane;
4) przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż to jest niezbędne do osiągnięcia celu przetwarzania.

2. Kanclerz przyjmuje wypełniony wniosek - oświadczenie podpisany przez pracownika (załącznik nr 1 do niniejszej Polityki) o nadanie upoważnienia do przetwarzania danych osobowych w PSW.
Kanclerz po podpisaniu upoważnienia (załącznik nr 2 do niniejszej Polityki) przekazuje upoważnienie pracownikowi, a jego kopię do Działu Kadr w celu umieszczenia jej w aktach osobowych upoważnionego pracownika.
3. Osoby, których dane dotyczą, mogą mieć do nich wgląd wyłącznie w obecności upoważnionego pracownika PSW w Kwidzynie.

4. Dostęp do danych osobowych i ich przetwarzanie, bez odrębnego upoważnienia wydanego przez Kanclerza, może mieć miejsce wyłącznie w przypadku działań podmiotów upoważnionych na mocy odpowiednich przepisów prawa do dostępu i przetwarzania danych określonej kategorii, w szczególności takich jak: Państwowa Inspekcja Pracy, organy skarbowe, Policja, Prokuratura, Agencja Bezpieczeństwa Wewnętrznego, Agencja Wywiadu, sądy powszechne, Najwyższa Izba Kontroli, Zakład Ubezpieczeń Społecznych, Generalny Inspektor Danych Osobowych.

5. Podmioty, o których mowa w ust. 4 oraz inne organy, którym przepisy szczegółowe umożliwiają dostęp do przetwarzania danych osobowych na podstawie odrębnych upoważnień, zobowiązane są do złożenia pisemnego wniosku i wskazania przepisu szczególnego dającego im takie prawo lub do wskazania przepisów umożliwiających wykorzystanie innej drogi dostępu do danych osobowych.

§ 5

Zabezpieczenie danych osobowych

1. PSW realizując politykę bezpieczeństwa stosuje odpowiednie środki fizyczne, techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednio do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności zabezpiecza dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.
2. Zgodnie z przepisami wykonawczymi do ustawy o ochronie danych osobowych, uwzględniając kategorie przetwarzanych danych oraz ich zagrożenia, PSW stosuje podstawowy, podwyższony lub wysoki poziom bezpieczeństwa przetwarzania danych osobowych w systemie informatycznym.

§ 6

Ogólne zasady polityki bezpieczeństwa

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

1. W budynkach, pomieszczeniach i częściach pomieszczeń tworzących obszar PSW, w którym przetwarzane są dane osobowe mają prawo przebywać wyłącznie osoby upoważnione do przetwarzania danych osobowych oraz osoby sprawujące nadzór i kontrolę przetwarzania i ochrony tych danych.
2. Osoby nie posiadające upoważnienia do przetwarzania danych osobowych, a mające interes prawny lub faktyczny w uzyskaniu dostępu do danych oraz osoby wykonujące inne czynności niezwiązane z dostępem do danych osobowych, w szczególności takie, jak: sprzątanie, remonty, ochrona budynku, mogą przebywać w budynkach, pomieszczeniach i częściach pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe, wyłącznie w obecności upoważnionego pracownika PSW lub na podstawie wydanego przez administratora danych osobowych dokumentu zezwalającego i określającego warunki przebywania w miejscach przetwarzania danych osobowych. Zezwolenie na przebywanie w w/w miejscach i warunki przebywania mogą wynikać z umowy z podmiotem wykonującym określone usługi dla PSW.
3. Obszar, w którym przetwarzane są dane osobowe obejmuje miejsca, w których wykonuje się wszelkie operacje na danych osobowych, jak również miejsca, w których przechowuje się wszelkie nośniki informacji zawierające dane osobowe (m.in. szafy z dokumentacją papierową, szafy zawierające komputerowe nośniki informacji z kopiami zapasowymi danych, stacje komputerowe, serwery i inne urządzenia komputerowe, w których dane osobowe przetwarzane są na bieżąco).
4. Do obszaru przetwarzania danych należy również zaliczyć pomieszczenia, w których są składowane uszkodzone nośniki komputerowe (taśmy, dyski, komputery, płyty CD, uszkodzone komputery i inne urządzenia z nośnikami zawierającymi dane osobowe.
5. Do obszarów przetwarzania danych osobowych administrator może zaliczyć miejsca wykorzystywane do przechowywania elektronicznych nośników informacji zawierających kopie zapasowe danych przetwarzanych w systemie informatycznym, czy też do składowania innych nośników danych.

6. Pomieszczenia, w których przetwarzane są dane osobowe należy zabezpieczyć przed dostępem osób nieuprawnionych na czas nieobecności w nich osób upoważnionych do przetwarzania danych osobowych.
7. Zabrania się przetwarzania danych osobowych poza obszarem ich przetwarzania (na przenośnych urządzeniach komputerowych). Zabrania się również wynoszenia danych osobowych poza obszar ich przetwarzania na nośnikach elektronicznych.
8. Postanowienia, o którym mowa powyżej nie mają zastosowania w przypadku procedur określonych w innych przepisach.
9. Prowadzenie ewidencji danych dotyczących wykazu budynków, pomieszczeń lub części pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe, należy do obowiązków Administratora Danych Osobowych.
10. Ewidencja, o której mowa w ust. 9 prowadzona jest na formularzu, którego wzór stanowi załącznik nr 3 do niniejszej Polityki.

Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych:

1. Prowadzenie ewidencji danych dotyczących nazwy zbiorów danych oraz stosownych nazw używanych do przetwarzania programów komputerowych należy do obowiązków Administratora Danych Osobowych.
2. W ewidencji danych dotyczących nazwy danych zbiorów podawane są informacje z zakresu dokładnej lokalizacji miejsca (budynek, nazwa komputera lub innego urządzenia), w którym znajdują się zbiory danych osobowych. Ewidencja prowadzona jest na formularzu, którego wzór stanowi załącznik nr 4 do niniejszej Polityki.

Opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania miedzy nimi:

1. Każdy z systemów informatycznych funkcjonujących w PSW powinien posiadać dokumentację techniczną dostarczoną przez jego autorów.
2. Dokumentacja, o której mowa w ust. 1 powinna spełniać wymagania dotyczące struktur baz danych oraz funkcjonalności zarządzających nimi aplikacji zgodnie z ustawą o ochronie danych osobowych.
3. Nowe systemy informatyczne powinny spełnić wymaganie, o którym mowa w ust. 2 przed dopuszczeniem ich do użytkowania.
4. Każdy zidentyfikowany zbiór danych powinien posiadać opis struktury zbioru i zakres informacji gromadzonych w tym zbiorze.
5. Opis poszczególnych pól informacyjnych w strukturze zbioru danych powinien jednoznacznie wskazywać, jakie kategorie są w nich przechowywane.
6. W przypadkach, gdy nie jest możliwa jednoznaczna interpretacja zawartości pola, jego opis powinien wskazywać nie tylko na kategorie danych, ale również na format ich zapisu i określać w danym kontekście ich znaczenie.

Sposób przepływu danych pomiędzy poszczególnymi systemami:

1. Sposób przepływu danych pomiędzy poszczególnymi systemami powinien zostać opisany w dokumentacji technicznej tych systemów, lub dokumentacji technicznej połączenia systemów.
2. Dokumentacja techniczna systemów powinna zawierać również informacje o danych, które przenoszone są pomiędzy systemami w sposób manualny (przy wykorzystaniu

zewnętrznych nośników danych) lub za pomocą teletransmisji wykonywanych w określonych odstępach czasu.

3. W bazach danych, które zlokalizowane są w różnych obiektach PSW i zawierają różne zakresy danych osobowych, należy wskazać zakres przesyłanych danych, podmiotu lub kategorii podmiotów, do których dane są przekazywane oraz ogólne informacje na temat sposobu przesyłania danych. Sposób przesyłania danych np. przez Internet, pocztą elektroniczną, innym sposobem, powinien decydować o rodzaju narzędzi niezbędnych do zapewnienia bezpieczeństwa podczas ich przesyłania.

Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych:

1. Użytkownicy systemów informatycznych PSW powinni zostać przeszkoleni przed rozpoczęciem pracy w systemie.
2. Identyfikatory i hasła dostępu do systemów informatycznych przekazywane są użytkownikom w formie zapewniającej poufność.
3. Systemy informatyczne użytkowane przez PSW powinny być wyposażone w mechanizmy zapewniające:
    a) ochronę dostępu do aplikacji użytkowych,
    b) analizę poprawności przesyłanych danych,
    c) analizę modyfikacji przesyłanych danych,
    d) kontrolę dostępu do aplikacji użytkowych,
    e) kontrolę błędów wprowadzanych danych.

4. Prowadzenie ewidencji osób uprawnionych do przetwarzania danych osobowych w systemach informatycznych należy do obowiązków Administratora Danych Osobowych (wzór załącznik nr 5 do niniejszej Polityki).

§ 7

Bezpieczeństwo danych przetwarzanych w sposób tradycyjny

1. Zgodnie z ustawą ochronie danych osobowych zbiory danych osobowych przetwarzanych w sposób tradycyjny (kartoteki, skorowidze, księgi, wykazy i inne zbiory ewidencyjne) również podlegają ochronie.
2. PSW prowadzi ewidencję budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe w sposób tradycyjny. Obowiązek prowadzenia i aktualizacji ewidencji, o której mowa powyżej powierza się Administratorowi Danych Osobowych. Kopie prowadzonej ewidencji i kopie jej aktualizacji Administrator Danych Osobowych przekazuje Pełnomocnikowi ds. danych osobowych. Kopie przekazywane są raz w miesiącu.

3. Ewidencja zbiorów danych osobowych prowadzonych w sposób tradycyjny zawiera w szczególności:

a) wykaz zbiorów danych osobowych prowadzonych w sposób tradycyjny (załącznik nr 6 do niniejszej Polityki)
b) wykaz osób uprawnionych do przetwarzania danych osobowych w sposób tradycyjny (załącznik nr 7 do niniejszej Polityki),

c) określenie środków technicznych i organizacyjnych niezbędnych do zapewnienia poufności przetwarzanych danych.

4. Obowiązek prowadzenia oraz aktualizację ewidencji, o której mowa w pkt. 3, powierza się Administratora Danych Osobowych lub osobie przez niego wyznaczonej.
5. Przebywanie osób nieuprawnionych w obszarze przetwarzania danych osobowych jest dopuszczalne za zgodą administratora danych lub osoby upoważnionej do przetwarzania danych osobowych.
6. Obszar, w którym są przetwarzane dane osobowe w sposób tradycyjny zabezpiecza się przed dostępem osób nieuprawnionych na czas nieobecności w nim osób upoważnionych do przetwarzania danych osobowych w sposób tradycyjny.
7. Zabrania się wynoszenia wszelkich dokumentów, kartotek, skorowidzów, ksiąg, wykazów i innych zawierających dane osobowe poza obszar ich przetwarzania.

§8

Naruszenie ochrony danych osobowych

Za naruszenie ochrony danych osobowych uznaje się przypadki, w których:
- stwierdzono naruszenie zabezpieczenia systemu teleinformatycznego,
- stan urządzenia, zawartość zbioru danych osobowych, ujawnione metody pracy, sposób działania programu lub jakość komunikacji w sieci teleinformatycznej mogą wskazywać na naruszenie zabezpieczeń tych danych.

Każdy pracownik Szkoły, który stwierdzi lub podejrzewa naruszenie ochrony danych osobowych w systemie teleinformatycznym Szkoły zobowiązany jest do niezwłocznego poinformowania o tym administratora systemu, lokalnego administratora danych osobowych lub w przypadku ich nieobecności administratora bezpieczeństwa informacji.
Administrator baz danych osobowych, który stwierdził lub uzyskał informację wskazującą na naruszenie ochrony tej bazy danych zobowiązany jest do niezwłocznego:
1. Zapisania wszelkich informacji i okoliczności związanych z danym zdarzeniem, a w szczególności dokładnego czasu uzyskania informacji o naruszeniu ochrony danych osobowych lub samodzielnym wykryciu tego faktu.
2. Jeżeli zasoby systemu na to pozwalają, wygenerowania i wydrukowania wszystkich dokumentów i raportów, które mogą pomóc w ustaleniu wszelkich okoliczności zdarzenia, opatrzenia ich datą i opisania.
3. Przystąpienia do zidentyfikowania rodzaju zaistniałego zdarzenia, w tym do określenia skali zniszczeń, metody dostępu osoby niepowołanej do danych itp.
4. Podjęcie odpowiednich kroków w celu powstrzymania lub ograniczenia dostępu osoby niepowołanej, zminimalizowania szkód i zabezpieczenia przed usunięciem śladów naruszenia ochrony danych, w tym m. in.:
   a) fizycznego odłączenia urządzeń i segmentów sieci, które mogły umożliwić dostęp do bazy danych osobie niepowołanej,
   b) wylogowania użytkownika podejrzanego o naruszenie ochrony danych,
   c) zmianę hasła administratora i użytkownika poprzez którego uzyskano nielegalny dostęp w celu uniknięcia ponownej próby uzyskania takiego dostępu,
5. Szczegółowej analizy stanu systemu informatycznego w celu potwierdzenia lub wykluczenia faktu naruszenia danych osobowych.
6. Przywrócenia normalnego działania systemu, przy czym, jeżeli nastąpiło uszkodzenie bazy danych, odtworzenia jej z ostatniej kopii awaryjnej z zachowaniem wszelkich środków

ostrożności mających na celu uniknięcie ponownego uzyskania dostępu przez osobę nieupoważnioną, tą samą drogą.

Po przywróceniu pierwotnego stanu bazy danych osobowych należy przeprowadzić szczegółową analizę (audyt) w celu określenia przyczyn naruszenia naruszenia ochrony danych osobowych lub podejrzenia takiego naruszenia. Należy przedsięwziąć kroki mające na celu wyeliminowanie podobnych zdarzeń w przyszłości.
Jeżeli przyczyną zdarzenia była **infekcja wirusem** należy ustalić źródło jego pochodzenia i wykonać zabezpieczenia antywirusowe i organizacyjne wykluczające powtórzenie się podobnego zdarzenia w przyszłości.
Jeżeli przyczyną zdarzenia był **błąd użytkownika** systemu informatycznego, należy przeprowadzić szkolenie wszystkich osób biorących udział w przetwarzaniu danych.
Jeżeli przyczyną zdarzenia było zaniedbanie ze strony użytkownika systemu należy wyciągnąć konsekwencje dyscyplinarne wynikające z kodeksu pracy oraz ustawy o ochronie danych osobowych.
Administrator bazy danych osobowych, w której nastąpiło naruszenie ochrony danych osobowych, w porozumieniu z pełnomocnikiem ds. danych osobowych przygotowuje szczegółowy raport o przyczynach, przebiegu i wnioskach ze zdarzenia i w terminie 7 dni od daty jego zaistnienia przekazuje administratorowi danych.