Publiczna Szkoła Podstawowa nr 6
im. Marii Skłodowskiej - Curie
ul. Pawła Stalmacha 20
47 - 220 KĘDZIERZYN - KOŹLE
NIP 749-16-34-428 ; Regon 000698271
tel. 77 483 29 52 , 77 486 56 32
psp6@kedzierzynkozle.pl

Zarządzenie Dyrektora nr 04/09/2017-2018

Publicznej Szkoły Podstawowej nr 6 im. Marii Skłodowskiej-Curie w Kędzierzynie-Koźlu

z dnia 1 września 2017 r.

w sprawie powołania Administratora Systemu Informatycznego

Na podstawie art.36a ust.6 ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (tj. Dz. U z 2016 r. poz. 922.) w celu obsługi i zabezpieczenia systemu informatycznego Administrator danych

powołuję

z dniem 1 września 2017 r.

Pana Tomasza Puk

ADMINISTRATOREM SYSTEMU INFORMATYCZNEGO

w Publicznej Szkole Podstawowej nr 6 im. Marii Skłodowskiej-Curie w Kędzierzynie-Koźlu.

§ 1

Zakres czynności dla Administratora Systemu Informatycznego stanowi załącznik do niniejszego zarządzenia.

§ 2

Zarządzenie wchodzi w życie z dniem podjęcia.

DYREKTOR SZKOŁY
mgr Małgorzata Nowacka

.....
(pieczątka, data, podpis)

Załącznik nr 1 do Zarządzenia
Nr 04/09/2017-2018 Dyrektora
PSP nr 6 w Kędzierzynie-Koźlu
z dnia 01.09.2017 r.

Zakres czynności Administratora Systemu Informatycznego w Publicznej Szkole Podstawowej nr 6 w Kędzierzynie-Koźlu:

1. Prowadzenie monitoringu przetwarzania danych osobowych.
2. Administrowanie systemem informatycznym.
3. Nadawanie haseł użytkownikom.
4. Stosowanie środków ochrony w ramach oprogramowania użytkowego, systemów operacyjnych, urządzeń teletransmisyjnych, programów antywirusowych oraz ochrony sprzętowej.
5. Kontrola mechanizmów uwierzytelniania użytkowników w systemie informatycznym przetwarzającym dane osobowe oraz kontrola dostępu do danych osobowych.
6. Kontrola systemu antywirusowego.
7. Kontrola awaryjnego zasilania komputerów.
8. Kontrola i wykonywanie kopii awaryjnych.
9. Konserwacja oraz uaktualnienia systemów informatycznych
10. Prowadzenie ewidencji sprzętu teleinformatycznego oraz oprogramowania.
11. Informowanie na bieżąco ADO i ABI o przypadkach awarii programów wynikających z posługiwania się przez użytkowników nieautoryzowanym oprogramowaniem, nie przestrzegania zasad używania programów antywirusowych, niewłaściwego wykorzystywania sprzętu komputerowego.
12. Przeprowadzenie wraz z ABI co najmniej raz w roku auditu teleinformatycznego na załączniku nr 2 w postaci kompleksowej analizy przetwarzania danych osobowych w systemie informatycznym oraz ewentualnych potrzeb w zakresie bezpieczeństwa.

Załącznik nr 2 do Zarządzenia
Nr 04/09/2017-2018 Dyrektora PSP nr 6 w Kędzierzynie-Koźlu
z dnia 01.09.2017 r.

KARTA AUDYTU TELEINFORMATYCZNEGO

L.p.	Wymaganie	Pytania audytowe	Czy spełniane są wymagania	
			TAK	NIE
1	Przetwarzanie danych osobowych jest dopuszczalne wtedy, gdy osoba której dane dotyczą, wyrazi na to zgodę, chyba że przetwarzanie danych jest niezbędne dla ochrony żywotnych interesów osoby której dane dotyczą a uzyskanie jej zgody jest niemożliwe. Dane można przetwarzać do czasu gdy uzyskanie zgody tej osoby będzie możliwe.	Czy osoba której dane dotyczą, wyraziła zgodę na ich przetwarzanie, lub przetwarzanie tych danych jest niezbędne dla ochrony żywotnych interesów tej osoby?		
2	Przetwarzanie danych osobowych jest niezbędne do zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa.	Czy przetwarzanie danych osobowych jest niezbędne do zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa?		
3	Przetwarzanie danych osobowych jest konieczne do realizacji umowy, gdy osoba której te dane dotyczą jest jej stroną łub gdy jest to niezbędne do podjęcia działań przed zawarciem umowy na żądanie osoby, której dane dotyczą.	Czy są realizowane umowy, z udziałem osoby będącej stroną w umowie lub przetwarzanie danych jest niezbędne do podjęcia działań przed zawarciem umowy na żądanie osoby, której dane dotyczą?		
4	Przetwarzanie danych osobowych jest niezbędne do wykonania określonych prawem zadań realizowanych dla dobra publicznego.	Czy przetwarzanie danych osobowych jest niezbędne do wykonania określonych prawem zadań realizowanych dla dobra publicznego?		
5	Przetwarzanie danych osobowych jest niezbędne dla wypełniania prawnie usprawiedliwionych celów realizowanych przez administratorów danych albo odbiorców danych, a przetwarzanie nie narusza prawa i wolności osoby, której dane dotyczą.	Czy przetwarzanie danych osobowych jest niezbędne dla wypełniania prawnie usprawiedliwionych celów realizowanych przez administratorów danych albo odbiorców danych, a przetwarzanie nie narusza prawa i wolności osoby, której dane dotyczą?		
6	Administrator poinformował osobę o adresie swojej siedziby i pełnej nazwie, a w przypadku gdy administratorem jest osoba fizyczna - o miejscu swego zamieszkania oraz imieniu i nazwisku.	Czy administrator poinformował osobę o adresie swojej siedziby i pełnej nazwie, a w przypadku gdy administratorem jest osoba fizyczna - o miejscu swego zamieszkania oraz imieniu i nazwisku ?		
7	Administrator poinformował osobę o celu zbierania danych, a w szczególności o znanych mu w czasie udzielania informacji lub przewidywanych odbiorcach lub kategoriach odbiorców danych.	Czy administrator poinformował osobę o celu zbierania danych, a w szczególności o znanych mu w czasie udzielania informacji lub przewidywanych odbiorcach lub kategoriach odbiorców danych?		
8	Administrator poinformował osobę o prawie dostępu do swoich danych oraz ich poprawiania.	Czy administrator poinformował osobę o prawie dostępu do swoich danych oraz ich poprawiania?		
9	Administrator poinformował osobę o dobrowolności albo obowiązku podania danych, a jeżeli taki obowiązek istnieje, o jego podstawie prawnej.	Czy administrator poinformował osobę o dobrowolności albo obowiązku podania danych, a jeżeli taki obowiązek istnieje, o jego podstawie prawnej?		

10	Administrator poinformował osobę bezpośrednio po utrwaleniu zebranych danych o źródle danych.	Czy administrator poinformował osobę o źródle danych?		
11	Administrator poinformował osobę bezpośrednio po utrwaleniu zebranych danych o uprawnieniu do wniesienia w określonych ustawowo przypadkach pisemnie umotywowanego żądania zaprzestania przetwarzania jej danych ze względu na jej szczególną sytuację	Czy administrator poinformował osobę o uprawnieniu do wniesienia w określonych ustawowo przypadkach pisemnie umotywowanego żądania zaprzestania przetwarzania jej danych ze względu na jej szczególną sytuację?		
12	Administrator poinformował osobę bezpośrednio po utrwaleniu zebranych danych o prawie wniesienia sprzeciwu wobec przetwarzania jej danych w określonych ustawowo przypadkach, gdy administrator ma zamiar przetwarzać je w celach marketingowych lub wobec przekazywania jej danych osobowych innemu administratorowi danych.	Czy administrator poinformował osobę o prawie wniesienia sprzeciwu wobec przetwarzania jej danych w określonych ustawowo przypadkach, gdy administrator ma zamiar przetwarzać je w celach marketingowych lub wobec przekazywania jej danych osobowych innemu administratorowi danych?		
13	Administrator zapewnia przetwarzanie danych zgodnie z prawem.	Czy administrator zapewnia przetwarzanie danych zgodnie z prawem?		
14	Administrator zapewnia, że dane są zbierane dla oznaczonych, zgodnych z prawem celów i nie poddawane dalszemu przetwarzaniu niezgodnemu z tymi celami.	Czy administrator zapewnia, że dane są zbierane dla oznaczonych, zgodnych z prawem celów i nie poddawane dalszemu przetwarzaniu niezgodnemu z tymi celami?		
15	Administrator zapewnia merytoryczną poprawność danych i adekwatność w stosunku do celów, w jakich są przetwarzane.	Czy administrator zapewnia merytoryczna poprawność danych i adekwatność w stosunku do celów, w jakich są przetwarzane?		
16	Administrator zapewnia, że dane przechowywane są w postaci umożliwiającej identyfikację osób których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania.	Czy administrator zapewnia, że dane przechowywane są w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania?		
17	Administrator danych stosuje środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną.	Czy administrator danych stosuje środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną?		
18	Administrator danych zabezpiecza dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.	Czy administrator danych zabezpiecza dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem?		
19	Administrator danych prowadzi dokumentację opisującą sposób przetwarzania danych oraz ich środki ochrony.	Czy administrator danych prowadzi dokumentację opisującą sposób przetwarzania danych oraz ich środki ochrony?		
20	Dokumentacja zawiera politykę bezpieczeństwa.	Czy dokumentacja zawiera politykę bezpieczeństwa?		
21	Polityka bezpieczeństwa zawiera w szczególności wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe.	Czy polityka bezpieczeństwa zawiera w szczególności wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe?		
22	Polityka bezpieczeństwa zawiera w szczególności wykaz zbiorów danych osobowych wraz z wskazaniem programów zastosowanych do przetwarzania tych danych.	Czy polityka bezpieczeństwa zawiera w szczególności wykaz zbiorów danych osobowych wraz z wskazaniem programów zastosowanych do przetwarzania tych danych?		

23	Polityka bezpieczeństwa zawiera w szczególności opis struktury zbiorów danych wskazujących zawartość poszczególnych pól informacyjnych i powiązania między nimi.	Czy polityka bezpieczeństwa zawiera w szczególności opis struktury zbiorów danych wskazujących zawartość poszczególnych pól informacyjnych i powiązania między nimi?		
24	Polityka bezpieczeństwa zawiera w szczególności sposób przepływu danych pomiędzy poszczególnymi systemami.	Czy polityka bezpieczeństwa zawiera w szczególności sposób przepływu danych pomiędzy poszczególnymi systemami?		
25	Polityka bezpieczeństwa zawiera w szczególności określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych.	Czy polityka bezpieczeństwa zawiera w szczególności określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozdzielczości przetwarzanych danych?		
26	Dokumentacja zawiera instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.	Czy dokumentacja zawiera instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych?		
27	Instrukcja zawiera w szczególności procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie Informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności.	Czy instrukcja zawiera w szczególności procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te		
28	Instrukcja zawiera w szczególności stosowane metody i środki uwierzytelniania oraz procedury związane z ich zarządzaniem i użytkowaniem	Czy instrukcja zawiera w szczególności stosowane metody i środki uwierzytelniania oraz procedury związane z ich zarządzaniem i użytkowaniem ?		
29	Instrukcja zawiera w szczególności procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu.	Czy instrukcja zawiera w szczególności procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu?		
30	Instrukcja zawiera w szczególności procedury tworzenia kopn zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania.	Czy instrukcja zawiera w szczególności procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania?		
31	Instrukcja zawiera w szczególności sposób, miejsce i okres przechowywania elektronicznych nośników informacji zawierających dane osobowe.	Czy instrukcja zawiera w szczególności sposób, miejsce i okres przechowywania elektronicznych nośników informacji zawierających dane osobowe?		
32	Instrukcja zawiera w szczególności sposób, miejsce i okres przechowywania kopii zapasowych.	Czy instrukcja zawiera w szczególności sposób, miejsce i okres przechowywania kopii zapasowych?		
33	Instrukcja zawiera w szczególności sposób zabezpieczania systemu informatycznego przed działalnością o programowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego.	Czy instrukcja zawiera w szczególności sposób zabezpieczania systemu informatycznego przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego?		
34	Instrukcja zawiera w szczególności sposób realizacji wymogów dotyczących odnotowania informacji o odbiorcach, którym dane osobowe zostały udostępnione, dacie i zakresie tego udostępnienia.	Czy instrukcja zawiera w szczególności sposób realizacji wymogów dotyczących odnotowania informacji o odbiorcach, którym dane osobowe zostały udostępnione, dacie i zakresie tego udostępnienia?		
35	Instrukcja zawiera w szczególności procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych.	Czy instrukcja zawiera w szczególności procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych?		
36	Dokumentacja jest prowadzona w formie pisemnej.	Czy dokumentacja jest prowadzona w formie pisemnej?		
37	Dokumentację wdraża administrator danych.	Czy dokumentację wdraża administrator danych?		

38	Do przetwarzania danych dopuszczane są wyłącznie osoby posiadające upoważnienie nadane przez administratora danych.	Czy do przetwarzania danych dopuszczane są wyłącznie osoby posiadające upoważnienie nadane przez administratora danych?		
39	Administrator danych zapewnia kontrolę nad tym, jakie dane osobowe, kiedy i przez kogo zostały wprowadzone do zbioru oraz komu są przekazywane.	Czy administrator danych zapewnia kontrolę nad tym, jakie dane osobowe i kiedy i przez kogo zostały wprowadzone do zbioru oraz komu są przekazywane?		
40	Administrator danych prowadzi ewidencję osób upoważnionych do ich przetwarzania.	Czy administrator danych prowadzi ewidencję osób upoważnionych do ich przetwarzania?		
41	Ewidencja zawiera imię i nazwisko osoby upoważnionej.	Czy ewidencja zawiera imię i nazwisko osoby upoważnionej?		
42	Ewidencja zawiera datę nadania i ustania oraz zakres upoważnienia do przetwarzania danych osobowych.	Czy ewidencja zawiera datę nadania ustania oraz zakres upoważnienia do przetwarzania danych osobowych?		
43	Ewidencja zawiera identyfikator, jeżeli dane są przetwarzane w systemie Informatycznym.	Czy ewidencja zawiera identyfikator, dane są przetwarzane w systemie informatycznym?		
44	Obszar(budynki, pomieszczenia lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe), zabezpiecza się przed dostępem osób nieuprawnionych na czas nieobecności w nim osób upoważnionych do przetwarzania danych osobowych.	Czy obszar, w którym przetwarzane są dane osobowe, zabezpiecza się przed dostępem osób nieuprawnionych na czas nieobecności w nim osób upoważnionych do przetwarzania danych osobowych?		
45	Przebywanie osób nieuprawnionych w obszarze(budynki, pomieszczenia lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe) jest dopuszczalne za zgodą administratora danych lub w obecności osoby upoważnionej do przetwarzania danych osobowych.	Czy przebywanie osób nieuprawnionych w obszarze, w którym przetwarzane są dane osobowe jest dopuszczalne za zgodą administratora danych lub w obecności osoby upoważnionej do przetwarzania danych osobowych?		
46	W systemie informatycznym służącym do przetwarzania danych osobowych stosuje się mechanizmy kontroli dostępu do tych danych.	Czy w systemie informatycznym służącym do przetwarzania danych osobowych stosuje się mechanizmy kontroli dostępu do tych danych?		
47	Jeżeli dostęp do danych przetwarzanych w systemie informatycznym posiadają co najmniej dwie osoby, wówczas zapewnia się, aby w systemie tym rejestrowany był dla każdego użytkownika odrębny identyfikator.	Czy zapewnia się, aby w systemie informatycznym rejestrowany był dla każdego użytkownika odrębny identyfikator?		
48	Jeżeli dostęp do danych przetwarzanych w systemie informatycznym posiadają co najmniej dwie osoby, wówczas zapewnia się, aby dostęp do danych był możliwy wyłącznie po wprowadzeniu identyfikatora i dokonaniu uwierzytelnienia.	Czy zapewnia się, aby dostęp do danych był możliwy wyłącznie po wprowadzeniu identyfikatora i dokonaniu uwierzytelnienia?		
49	System informatyczny służący do przetwarzania danych osobowych zabezpiecza się, przed działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego	Czy system informatyczny służący do przetwarzania danych osobowych zabezpiecza się, przed działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego?		
50	System informatyczny służący do przetwarzania danych osobowych zabezpiecza się, przed utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej.	Czy system informatyczny służący do przetwarzania danych osobowych zabezpiecza się, przed utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej?		
51	Identyfikator użytkownika, który utracił uprawnienia do przetwarzania danych, nie może być przydzielony innej osobie.	Czy identyfikator użytkownika, który utracił uprawnienia do przetwarzania danych, nie może być przydzielony innej osobie?		

52	W przypadku gdy do uwierzytelniania użytkowników używa się hasła, jego zmiana następuje nie rzadziej niż co 30 dni.	Czy w przypadku gdy do uwierzytelniania użytkowników używa się hasła, jego zmiana następuje nie rzadziej niż co 30 dni?.		
53	Hasło składa się co najmniej z 8 znaków.	Czy hasło składa się co najmniej z 8 znaków?		
54	Dane osobowe przetwarzane w systemie informatycznym zabezpiecza się przez wykonywanie kopii zapasowych zbiorów danych oraz programów służących do przetwarzania danych.	Czy dane osobowe przetwarzane w systemie informatycznym zabezpiecza się przez wykonywanie kopii zapasowych zbiorów danych oraz programów służących do przetwarzania danych?		
55	Kopie zapasowe przechowuje się w miejscach zabezpieczających je przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem lub zniszczeniem	Czy kopie zapasowe przechowuje się w miejscach zabezpieczających je przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem lub zniszczeniem?		
56	Kopie zapasowe usuwa się niezwłocznie po ustaniu ich użyteczności.	Czy kopie zapasowe usuwa się niezwłocznie po ustaniu ich użyteczności?		
57	Osoba użytkują komputer przenośny zawierający dane osobowe zachowuje szczególną ostrożność podczas jego transportu, przechowywania i użytkowania poza obszarem przetwarzania	Czy osoba użytkująca komputer przenośny zawierający dane osobowe zachowuje szczególną ostrożność podczas jego transportu, przechowywania i użytkowania poza obszarem, w którym przetwarzane są dane osobowe?		
58	Osoba użytkująca komputer przenośny zawierający dane osobowe, podczas jego transportu stosuje środki ochrony kryptograficznej wobec przetwarzanych danych osobowych.	Czy osoba użytkująca komputer przenośny zawierający dane osobowe, podczas jego transportu stosuje środki ochrony kryptograficznej wobec przetwarzanych danych osobowych?		
59	Urządzenia, dyski lub inne elektroniczne nośniki informacji, zawierające dane osobowe, przeznaczone do likwidacji —pozbawia się wcześniej zapisu tych danych, a w przypadku gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie;	Czy urządzenia, dyski lub inne elektroniczne nośniki informacji, zawierające dane osobowe, przeznaczone do likwidacji — pozbawia się wcześniej zapisu tych danych, a w przypadku gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie?		
60	Urządzenia, dyski lub inne elektroniczne nośniki informacji, zawierające dane osobowe, przeznaczone do przekazania podmiotowi nieuprawnionemu do przetwarzania danych —pozbawia się wcześniej zapisu tych danych, w sposób uniemożliwiający ich odzyskanie	Czy urządzenia, dyski lub inne elektroniczne nośniki informacji, zawierające dane osobowe, przeznaczone do przekazania podmiotowi nieuprawnionemu do przetwarzania danych -pozbawia się wcześniej zapisu tych danych, w sposób uniemożliwiający ich odzyskanie?		
61	Urządzenia, dyski lub inne elektroniczne nośniki informacji, zawierające dane osobowe, przeznaczone do naprawy-pozbawia się wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie albo naprawia się je pod nadzorem osoby upoważnionej przez administratora danych.	Czy urządzenia, dyski lub inne elektroniczne nośniki informacji, zawierające dane osobowe, przeznaczone do naprawy - pozbawia się wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie albo naprawia się je pod nadzorem osoby upoważnionej przez administratora danych?		
62	Administrator danych monitoruje wdrożone zabezpieczenia systemu informatycznego	Czy Administrator danych monitoruje wdrożone zabezpieczenia systemu informatycznego?		
63	W przypadku stosowania haseł do uwierzytelniania użytkowników, hasła te składają się co najmniej z 8 znaków, zawierają małe i wielkie litery oraz cyfry lub znaki specjalne.	Czy w przypadku stosowania haseł do uwierzytelniania użytkowników, hasła te składają się co najmniej z 8 znaków, zawierają małe i wielkie litery oraz cyfry lub znaki specjalne?		
64	Urządzenia i nośniki zawierające dane osobowe przekazywane poza obszar w którym przetwarzane są dane osobowe, zabezpiecza się w sposób zapewniający poufność i integralność tych danych.	Czy urządzenia i nośniki zawierające dane osobowe przekazywane poza obszar w którym przetwarzane są dane osobowe, zabezpiecza się w sposób zapewniający poufność i integralność tych danych?		

65	Instrukcję zarządzania systemem informatycznym rozszerza się o sposób stosowania środków bezpieczeństwa dla poziomu podwyższonego.	Czy instrukcję zarządzania systemem informatycznym rozszerza się o sposób stosowania środków bezpieczeństwa określonych dla poziomu podwyższonego?		
66	Administrator danych stosuje na poziomie podwyższonym środki bezpieczeństwa określone dla poziomu podstawowego, o ile zasady określone dla poziomu podwyższonego nie stanowią inaczej.	Czy administrator danych stosuje na poziomie podwyższonym środki bezpieczeństwa określone dla poziomu podstawowego, o ile zasady określone dla poziomu podwyższonego nie stanowią inaczej?		
67	Wdrożono fizyczne lub logiczne zabezpieczenia chroniące, przed nieuprawnionym dostępem z s1ec1 publicznej, system informatyczny służący do przetwarzania danych osobowych.	Czy wdrożono fizyczne lub logiczne zabezpieczenia chroniące, przed nieuprawnionym dostępem z sieci publicznej, system informatyczny służący do przetwarzania danych osobowych?		
68	W przypadku zastosowania logicznych zabezpieczeń obejmują one kontrolę przepływu informacji pomiędzy systemem informatycznym administratora danych a siecią publiczną.	Czy w przypadku zastosowania logicznych zabezpieczeń obejmują one kontrolę przepływu informacji pomiędzy systemem informatycznym administratora danych a siecią publiczną?		
69	W przypadku zastosowania logicznych zabezpieczeń obejmują one kontrolę działań inicjowanych z sieci publicznej i systemu informatycznego administratora baz danych?	Czy w przypadku zastosowania logicznych zabezpieczeń obejmują one kontrolę działań inicjowanych z sieci publicznej i systemu informatycznego administratora baz danych?		
70	Administrator danych stosuje środki kryptograficznej ochrony wobec danych wykorzystywanych do uwierzytelniania, które są przesyłane w sieci publicznej	Czy administrator danych stosuje środki kryptograficznej ochrony wobec danych wykorzystywanych do uwierzytelniania, które są przesyłane w sieci publicznej		
71	Administrator danych stosuje środki bezpieczeństwa środki określone dla poziomu podstawowego i bezpieczeństwa określone dla poziomu podwyższonego, o ile zasady określone dla poziomu nie stanowią inaczej?	Czy administrator danych stosuje środki bezpieczeństwa środki określone dla poziomu podstawowego i bezpieczeństwa określone dla poziomu podwyższonego, o ile zasady określone dla poziomu nie stanowią inaczej?		
72	System informatyczny służący do przetwarzania danych osobowych zapewnia odnotowanie daty pierwszego wprowadzenia danych do systemu	Czy system informatyczny służący do przetwarzania danych osobowych zapewnia odnotowanie daty pierwszego wprowadzenia danych do systemu		
73	System informatyczny służący do przetwarzania danych osobowych zapewnia odnotowanie identyfikatora użytkownika wprowadzającego dane do systemu	Czy system informatyczny służący do przetwarzania danych osobowych zapewnia odnotowanie identyfikatora użytkownika wprowadzającego dane do systemu		
74	System informatyczny służący do przetwarzania danych osobowych zapewnia odnotowanie źródła, w przypadku zbierania danych nie od osoby, której owe dane dotyczą.	Czy system informatyczny służący do przetwarzania danych osobowych zapewnia odnotowanie źródła, w przypadku zbierania danych nie od osoby, której owe dane dotyczą.		
75	System informatyczny służący do przetwarzania danych osobowych zapewnia odnotowanie informacji o odbiorcach, którem dane zostały udostępnione, dacie i zakresie tego udostępniania , chyba że system informatyczny używany jest w zakresie przetwarzania danych w zbiorach jawnych	Czy system informatyczny służący do przetwarzania danych osobowych zapewnia odnotowanie informacji o odbiorcach, którem dane zostały udostępnione, dacie i zakresie tego udostępniania , chyba że system informatyczny używany jest w zakresie przetwarzania danych w zbiorach jawnych		
76	System informatyczny służący do przetwarzania danych osobowych zapewnia odnotowanie sprzeciwu wobec przetwarzania danych przez osobę której te dane dotyczą.	Czy system informatyczny służący do przetwarzania danych osobowych zapewnia odnotowanie sprzeciwu wobec przetwarzania danych przez osobę której te dane dotyczą?		

77	Odnotowanie informacji dotyczących daty pierwszego wprowadzenia danych do systemu i identyfikatora użytkownika wprowadzającego te dane następuje automatycznie po zatwierdzeniu przez użytkownika operacji wprowadzania danych.	Czy odnotowanie informacji dotyczących daty pierwszego wprowadzenia danych do systemu i identyfikatora użytkownika wprowadzającego te dane następuje automatycznie po zatwierdzeniu przez użytkownika operacji wprowadzania danych?		
78	System umożliwia tworzenie i drukowanie raportów zawierających odnotowane informacje w przystępnej formie dla każdej osoby, której dane są przetwarzane.	Czy system umożliwia tworzenie i drukowanie raportów zawierających odnotowane informacje w przystępnej formie, dla każdej osoby, której dane są przetwarzane?		
79	Wyznaczona przez Administratora danych osoba, nadzorująca przestrzeganie zasad ochrony danych osobowych	Czy powołano Administratora Bezpieczeństwa Informacji?		
		Czy określono zakres obowiązków Administratora Bezpieczeństwa Informacji?		
		Czy określono Instrukcję postępowania w przypadku naruszenia ochrony danych osobowych?		
		Czy korespondencja w zakresie procedur kadrowo-płacowych prowadzona jest za pomocą listów poleconych?		
		Czy pracownicy (użytkownicy) dopuszczeni do przetwarzania danych osobowych zapoznali się z polityką bezpieczeństwa?		
		Czy pracownicy (użytkownicy) dopuszczeni do przetwarzania danych osobowych zapoznali się z instrukcją zarządzania systemami informatycznym.?		
		Czy pracownicy zachowują ostrożność udzielając informacji dot. danych osobowych przez telefon i poza instytucją ?		
		Czy pracownicy zachowują ostrożność udzielając informacji osobom nieuprawnionym ?		
		Czy pracownicy reagują na obecność nieznanych osób przebywających w pobliżu miejsca przetwarzania danych i zachowujące się podejrzanie?		
		Czy pracownicy są świadomi konieczności zgłaszania incydentów bezpieczeństwa Administratorowi bezpieczeństwa informacji?		
		Czy pracownicy podpisali oświadczenia?		
		Czy zakres udostępnionych danych osobowych osobie upoważnionej do przetwarzania danych osobowych jest pisemnie potwierdzony przez Administratora Danych Osobowych?		
		Czy przestrzegany jest zakaz niepodawania swojego hasła, pod rygorem naruszenia zasad bezpieczeństwa informacji?		
		Czy hasło posiada ilość znaków, zgodnie z poziomem bezpieczeństwa?		
		Czy hasła nie są zapisywane na kartkach , w pobliżu komputera, w innych widocznych miejscach?		
		Czy użytkownik jest świadom zakazu udostępniania swojego hasła innym użytkownikom?		

		Czy sprawdzane jest podczas logowania się, czy ktoś się nie próbował włamać do systemu?		
		Czy użytkownik loguje się zawsze na swój login i hasło?		
		Czy użytkownik blokuje dostęp do swojego komputera po odejściu od stanowiska pracy za pomocą wygaszacza z hasłem ?		
		Czy po zakończeniu pracy użytkownik wylogowuje się a następnie zamyka komputer?		
		Czy w razie awarii komputera lub sprzętu przetwarzającego dane osobowe, użytkownik powiadamia informatyka, do którego kontakt jest znany?		
		Czy laptop pozostawiany jest bez opieki w pomieszczeniu, jeśli pomieszczenie nie jest zamknięte na klucz?		
		Czy ekrany monitorów ustawiono w taki sposób, żeby uniemożliwić odczyt wyświetlanych danych osobowych osobom nieupoważnionym?		
		Czy określono politykę korzystania z Internetu?		
		Czy określono politykę korzystania z poczty firmowej ?		
		Czy zarząd / kierownictwo najwyższego szczebla jest świadome odpowiedzialności karnej za naruszenie Ochrony Danych Osobowych?		
		Czy dokumenty w postaci papierowej lub elektronicznej zawierające dane osobowe po zakończeniu pracy są zamknięte (klucze w szafach) ?		
		Czy dokumenty papierowe i CD zawierające dane osobowe niszczone są w niszczarkach?		
		Czy stosuje się system kontroli dostępu?		
		Czy konfiguracja systemu umożliwia użytkownikom końcowym dostęp do danych osobowych jedynie za pośrednictwem aplikacji?		
		Czy używane jest tylko licencjonowane oprogramowanie do przetwarzania danych osobowych?		
		Czy urządzenia wchodzące w skład systemu informatycznego podłączone są do odrębnego obwodu elektrycznego, zabezpieczonego na wypadek zaniku napięcia albo awarii w sieci zasilającej?		
		Czy sieć lokalna podłączona jest do Internetu za pomocą odrębnego komputera?		

.....
(data, podpis administratora bezpieczeństwa informacji)