PAŃSTWOWA SZKOŁA WYŻSZA
im. Papieża Jana Pawła II
w Białej Podlaskiej
21-500 Biała Podlaska, ul. Sidorska 95/97
tel. 83 344 99 00, fax 83 344 99 50
NIP 537-21-31-853 REGON 030310705

Zarządzenie nr 51/2018
Rektora Państwowej Szkoły Wyższej im. Papieża Jana Pawła II
w Białej Podlaskiej
z dnia 09.10.2018r.

w sprawie: **wprowadzenia w Państwowej Szkole Wyższej im. Papieża Jana Pawła II w Białej Podlaskiej „ Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Państwowej Szkole Wyższej im. Papieża Jana Pawła II w Białej Podlaskiej"**

Na podstawie Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE, Rozporządzenia Ministra Spraw Wewnętrznych i Administracji w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych z dnia 24.04.2004r. (D.U. z 2004r. nr 100, poz. 1024) oraz Rozporządzenia Ministra Administracji i Cyfryzacji z dnia 11 maja 2015r. w sprawie trybu i sposobu realizacji zadań w celu zapewnienia przestrzegania przepisów o ochronie danych osobowych przez Administratora (D.U. z 2015r., poz. 745) zarządzam co następuje:

§ 1

W celu kompleksowego zarządzania bezpieczeństwem w zakresie ochrony danych osobowych wprowadzam:

1. Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Państwowej Szkole Wyższej im. Papieża Jana Pawła II w Białej Podlaskiej.

§ 2

Traci moc Zarządzenie nr 54/2015 Rektora Państwowej Szkoły Wyższej im. Papieża Jana Pawła II w Białej Podlaskiej z dnia 07. 10.2015r. w sprawie zabezpieczenia danych osobowych.

§ 3

Nadzór nad realizacją zarządzenia powierzam: Administratorowi Systemu Informatycznego (ASI) i Inspektorowi ochrony Danych Osobowych (IODO).

§ 4

Zarządzenie wchodzi w życie z dniem podpisania.

dr inż. Agnieszka Smarzewska

Prorektor PSW im. Papieża Jana Pawła II
w Białej Podlaskiej

Załącznik:
Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Państwowej Szkole Wyższej im. Papieża Jana Pawła II w Białej Podlaskiej.

PAŃSTWOWA SZKOŁA WYŻSZA
im. Papieża Jana Pawła II
w Białej Podlaskiej
21-500 Biała Podlaska, ul. Sidorska 95/97
tel. 83 344 99 00, fax 83 344 99 50
NIP 537-21-31-883 REGON 030310705

Załącznik do zarządzenia Nr 51/2018 Rektora
Państwowej Szkoły Wyższej im. Papieża Jana Pawła II
w Białej Podlaskiej z dnia 09.10.2018r.

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM SŁUŻĄCYM DO PRZETWARZANIA DANYCH OSOBOWYCH W PAŃSTWOWEJ SZKOLE WYŻSZEJ IM. PAPIEŻA JANA PAWŁA II W BIAŁEJ PODLASKIEJ

ADMINISTRATOR SYSTEMU INFORMATYCZNEGO

Marcin Stefanowicz .....
Podpis

INSPEKTOR OCHRONY DANYCH OSOBOWYCH

Jan Sroka .....
Podpis

BIAŁA PODLASKA 09.10.2018r.

PAŃSTWOWA SZKOŁA WYŻSZA
im. Papieża Jana Pawła II
w Białej Podlaskiej
21-500 Biała Podlaska, ul. Sidorska 95/97
tel. 83 344 99 00, fax 83 344 99 50
NIP 537-21-31-853 REGON 030310705

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM SŁUŻĄCYM DO PRZETWARZANIA DANYCH OSOBOWYCH W PAŃSTWOWEJ SZKOLE WYŻSZEJ IM. PAPIEŻA JANA PAWŁA II W BIAŁEJ PODLASKIEJ

ROZDZIAŁ I. WPROWADZENIE

§ 1

1. Niniejszy dokument, zwany dalej Instrukcją stanowi „Instrukcję zarządzania systemem informatycznym" służącym do przetwarzania danych osobowych w Państwowej Szkole Wyższej im. Papieża Jana Pawła II w Białej Podlaskiej.

2. Instrukcja określa sposób zarządzania systemem informatycznym wykorzystywanym do przetwarzania danych osobowych w celu zabezpieczenia ich przed zagrożeniami, w tym zwłaszcza przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, nieautoryzowaną zmianą, utratą, uszkodzeniem lub zniszczeniem.

3. W Instrukcji zostały uregulowane:

   1) procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień systemie informatycznym oraz wskazania osób odpowiedzialnych za te czynności;
   2) procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu;
   3) procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania wraz z określeniem sposobu, miejsca i okresu ich przechowywania;
   4) procedury wykonywania przeglądów i konserwacji systemu oraz nośników informacji służących do przetwarzania danych;
   5) Metody i środki uwierzytelniania oraz procedury związane z ich zarządzaniem i użytkowaniem;
   6) sposoby zabezpieczenia systemu informatycznego przed działaniem oprogramowania szkodliwego oraz dostępem do systemu informatycznego osób nieuprawnionych.

4. Instrukcja została opracowana na podstawie § 3 Rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004r. 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) i pozostaje w zgodności z w/wym. aktem , jak również „Polityką Bezpieczeństwa Informacji w Państwowej Szkole Wyższej im. Papieża Jana Pawła II w Białej Podlaskiej".

§ 2

Słownik pojęć

Użyte w instrukcji określenia oznaczają:

1. Administrator Danych Osobowych- Państwowa Szkoła Wyższa im. Papieża Jana Pawła II w Białej Podlaskiej - **REKTOR** decydujący o celach i środkach przetwarzania danych osobowych zwany dalej ADO;

2. Inspektor Ochrony Danych Osobowych - osoba wyznaczona przez ADO,

3. Administrator Systemu Informatycznego - osoba wykonująca zadania w zakresie zarządzania i bieżącego nadzoru nad systemem informatycznym zwany dalej ASI;

4. bezpieczeństwo informacji - stan, w którym informacja jest chroniona przed wieloma różnymi zagrożeniami w taki sposób, aby zapewnić ciągłość prowadzenia działalności, zminimalizować straty i maksymalizować zwrot nakładów na inwestycje i działania o charakterze biznesowym. Bezpieczeństwo informacji oznacza w szczególności zachowanie poufności, integralności, dostępności i rozliczalności;

5. dane osobowe(dane) - wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej;

6. hasło - ciąg znaków literowych, cyfrowych lub innych znany jedynie użytkownikowi;

7. incydent związany z bezpieczeństwem informacji – pojedyncze zdarzenie lub seria niepożądanych lub niespodziewanych zdarzeń, które stwarzają znaczne prawdopodobieństwo zakłócenia działań i zagrażają bezpieczeństwu informacji;

8. identyfikator - ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym;

9. integralność danych - właściwość zapewniająca, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany;

10. IZSI - niniejsza Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, zwana dalej Instrukcją;

11. kopia bezpieczeństwa - kopie plików danych lub plików oprogramowania tworzone na nośnikach wymiennych lub dysku twardym komputera w celu ich odtworzenia w przypadku utraty lub uszkodzenia danych;

12. odbiorca danych - każdy komu udostępniane są dane osobowe z wyłączeniem:
    a) osoby, której dane dotyczą,
    b) osoby upoważnionej do przetwarzania danych,

c) organów państwowych lub organów samorządu terytorialnego, którym dane są udostępniane w związku z prowadzonym postępowaniem;

13. osoba upoważniona do przetwarzania danych osobowych - osoba, która upoważniona została w formie pisemnej do przetwarzania danych osobowych przez ADO (wzór załącznik do PBI PSW);

14. poufność danych - właściwość zapewniająca, że dane nie są udostępniane nieupoważnionym podmiotom;

15. proces zarządzania bezpieczeństwem systemu informatycznego – całość działań organizacyjno-technicznych i prawnych podejmowanych przez Uczelnię mających na celu właściwą ochronę informacji oraz minimalizację skutków w przypadku incydentów bezpieczeństwa;

16. przetwarzanie danych - wykonywanie jakichkolwiek operacji na danych osobowych np. zbieranie, utrwalanie, opracowywanie, udostępnianie, zmienianie, usuwanie i przechowywanie;

17. przetwarzający dane - podmiot, któremu zostało powierzone przetwarzanie danych osobowych na podstawie umowy;

18. rozliczalność - właściwość zapewniająca, że działania podmiotu mogą być przypisane w sposób jednoznaczny tyko temu podmiotowi;

19. RODO - Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych;

20. Serwisant - firma lub pracownik przedsiębiorstwa zajmującego się sprzedażą,

21. Instalacją, naprawą i konserwacją sprzętu komputerowego (software, hardware);

22. system informatyczny – sprzęt komputerowy, oprogramowanie, dane eksploatowane w zespole współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych. W systemie tym pracuje co najmniej jeden komputer centralny i system ten tworzy sieć teleinformatyczną ADO;

23. system zarządzania bezpieczeństwem informacji – całościowy i uporządkowany układ, który tworzą następujące procedury i procesy:

    a) polityka bezpieczeństwa informacji,
    b) określenie zakresu zarządzania bezpieczeństwem informacji,
    c) ocena zagrożeń bezpieczeństwa informacji i zarządzanie ryzykiem;
    d) edukacja pracowników w zakresie bezpieczeństwa informacji;

24. trwałe usunięcie informacji – sposób postępowania z nośnikami informacji mający na celu usunięcie zapisanych na nim informacji tak, aby ich odtworzenie w całości lub części było niemożliwe;

25. uwierzytelnianie – rozumie się przez to działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu;

26. użytkownik – osoba upoważniona do przetwarzania danych osobowych, której nadano identyfikator i hasło;

27. zagrożenie – stan faktyczny, który może spowodować naruszenie bezpieczeństwa informacji;

28. zasada wiedzy koniecznej – oznacza, że dostęp osób zatrudnionych w Państwowej Szkole Wyższej im. Papieża Jana Pawła II w Białej Podlaskiej do zasobów informacyjnych ograniczony jest wyłącznie do informacji, które są im niezbędne do wykonania powierzonych zadań.

§ 3

Obowiązki Administratora Systemu Informatycznego

Do obowiązków Administratora Systemu Informatycznego (ASI) w zakresie ochrony danych osobowych przetwarzanych w systemach informatycznych należy w szczególności:

1. operacyjne zarządzanie systemami informatycznymi w sposób zapewniający ochronę danych osobowych w nich przetwarzanych;

2. przestrzeganie opracowanych procedur operacyjnych i bezpieczeństwa;

3. zarządzanie stosowanymi w systemach informatycznych środkami uwierzytelnienia, w tym rejestrowanie i wyrejestrowywanie użytkowników oraz dokonywanie zmiany uprawnień na podstawie zaakceptowanych wniosków złożonych przez osobę do tego upoważnioną;

4. utrzymanie systemu w należytej sprawności technicznej;

5. regularne tworzenie kopii zapasowych zasobów danych osobowych oraz programów służących do ich przetwarzania;

6. wykonywanie lub nadzór nad wykonywaniem okresowych przeglądów i konserwacji zgodnie z odrębnymi procedurami, sprzętu IT, systemów informatycznych, aplikacji oraz elektronicznych nośników informacji, na których zapisane są dane osobowe;

7. zapewnienie przeszkolenia użytkowników systemów informatycznych ze szczególnym uwzględnieniem przestrzegania zasad bezpieczeństwa i środków podjętych dla ochrony danych przetwarzanych w tych systemach.

Obowiązki użytkowników

Do obowiązków użytkowników systemu informatycznego w zakresie ochrony danych osobowych w systemach informatycznych należy w szczególności:

1. przestrzeganie opracowanych dla systemu zasad przetwarzania danych osobowych;
2. przestrzeganie opracowanych dla systemu procedur operacyjnych i bezpieczeństwa;
3. udostępnianie danych osobowych wyłącznie osobom upoważnionym lub uprawnionym do ich uzyskania;
4. uniemożliwienie dostępu do danych osobowych w systemie lub ich podglądu przez osoby nieupoważnione;
5. informowanie IODO o wszelkich naruszeniach, podejrzeniach naruszenia i nieprawidłowościach w sposobie przetwarzania i ochrony danych osobowych;
6. wykonywania bez zbędnej zwłoki poleceń IODO w zakresie ochrony danych osobowych, jeśli są one zgodne z przepisami prawa powszechnie obowiązującego.

Rozdział II. Procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym

§ 5

1. Dostęp do systemu informatycznego mogą posiadać:
   1) pracownicy – w zależności od wykonywanych czynności służbowych;
   2) wykonawcy usług oraz dostawcy sprzętu lub oprogramowania w zakresie koniecznym do realizowania danej usługi.
2. Pracownicy dostawców sprzętu i oprogramowania wykonują usługę tylko za zgodą i pod nadzorem ASI.

§ 6

1. Do obsługi systemu informatycznego oraz urządzeń wchodzących w jego skład, służących do przetwarzania danych osobowych mogą zostać dopuszczone wyłącznie osoby posiadające upoważnienia wydane przez ADO. Wzór upoważnienia załącznik nr 5 Polityki Bezpieczeństwa PSW w Białej Podlaskiej.
2. Procedury wydawania i anulowania upoważnień do obsługi systemu informatycznego realizowane są według następujących zasad:

1) Kierownicy jednostek organizacyjnych PSW składają wniosek do IODO o wydanie upoważnienia do pracy w systemie informatycznym służącym do przetwarzania danych osobowych.

2) IODO przygotowuje upoważnienie do podpisu przez ADO i po jego podpisaniu a następnie przeszkoleniu osoby upoważnionej do przetwarzania przez IODO w zakresie obowiązujących przepisów osoba upoważniona podpisuje upoważnienie;

3) Oryginał upoważnienia otrzymuje osoba, której upoważnienie zostało wydane a kopia pozostaje w dokumentacji IODO;

4) IODO wypełnia Rejestr osób upoważnionych do przetwarzania danych osobowych, który jeden egzemplarz przekazuje dla ASI a drugi pozostaje w dokumentacji IODO. Wzór Rejestru określa załącznik nr 1 P.B. PSW;

5) ASI po otrzymaniu Rejestru nadaje osobie upoważnionej identyfikator i hasło;

6) W przypadku utraty przez użytkownika uprawnień do obsługi (np. rozwiązanie stosunku pracy, zmiana zakresu czynności) kierownik jednostki organizacyjnej lub kadry występują z wnioskiem o anulowanie upoważnienia do przetwarzania danych osobowych do IODO;

7) IODO przygotowuje odwołanie upoważnienia według załącznika nr 6 do P.B.PSW przekazuje go do podpisu ADO;

8) Podpisany oryginał odwołania IODO włącza do dokumentacji a kopię przekazuje ASI;

9) ASI na podstawie otrzymanej kopi odwołania wyrejestrowuje użytkownika z systemu informatycznego.

Rozdział III. Metody i środki uwierzytelniania

§ 7

Nazwa i hasło użytkownika

1. Uwierzytelnianie użytkownika w systemie informatycznym następuje po podaniu nazwy użytkownika i hasła.

2. Nazwa użytkownika stanowi identyfikator, który w sposób jednoznaczny został przypisany konkretnemu użytkownikowi.

3. Niedopuszczalne jest funkcjonowanie kilku takich samych nazw użytkowników. Raz przypisana nazwa nie podlega zmianie i nie może zostać wykorzystana w przyszłości przez innego użytkownika.

4. Hasło powinno składać się z unikalnego zestawu co najmniej ośmiu znaków, zawierać małe i duże litery oraz cyfry lub znaki specjalne.

5. Hasło nie może:

   1) być identyczne z identyfikatorem użytkownika;
   2) być identyczne z imieniem lub nazwiskiem użytkownika;
   3) odnosić się do innych cech szczególnych użytkownika;
   4) być stosowane przez użytkownika ponownie, jeżeli od ostatniego zastosowania danej kombinacji nie upłynął rok.

6. niedopuszczalne jest zapamiętywanie haseł w systemie.

7. Pierwsze nadane hasło ulega zmianie przez użytkownika.

8. W przypadku gdy system umożliwia limitowanie wprowadzenia błędnego hasła, należy przyjąć próg 3 prób wprowadzonych błędnych haseł. Po przekroczeniu limitu powinna nastąpić automatyczna blokada konta.

9. użytkownik odpowiada za działania wykonywane w systemie przy użyciu jego nazwy oraz zachowanie hasła w tajemnicy.

10. Użytkownik ma obowiązek zmieniać hasło nie rzadziej niż co 30 dni.

11. Okresowe zmiany hasła są wykonywane osobiście przez użytkownika.

12. Hasła administracyjne zapisywane są i przechowywane w rejestrze ASI.

Rozdział IV. Rozwój, utrzymanie i wycofanie systemów informatycznych

§ 8

Rozwój systemów informatycznych

1. Rozwój systemów informatycznych dotyczy wdrożenia nowych lub modernizacji aktualnie eksploatowanych systemów informatycznych a w szczególności zmiany architektury systemów lub ich funkcjonalności.

2. Rozwój systemów informatycznych obejmuje w szczególności następujące działania:

   1) określenie kategorii systemu informatycznego;

   2) analizę ryzyk związanych z wdrożeniem nowego systemu informatycznego lub jego modernizacją, projektowanie architektury i funkcjonalności systemów informatycznych z uwzględnieniem aspektów bezpieczeństwa:

   3) testowanie systemu informatycznego przed jego wdrożeniem do eksploatacji;

   4) przeszkolenie użytkowników.

3. Za rozwój systemów informatycznych w PSW odpowiada Kierownik Działu Teleinformatycznego.

4. ASI sprawuje nadzór merytoryczny nad wdrożeniem mechanizmów właściwych dla kategorii systemu informatycznego.

§ 9

Utrzymanie systemów informatycznych

1. Proces utrzymania systemów informatycznych obejmuje utrzymanie zasobów sprzętowych i programowych w stanie gwarantującym niezakłócone świadczenie usług na rzecz użytkowników.

2. Utrzymanie systemów informatycznych obejmuje następujące działania:

   1) analizę ryzyka związanego z funkcjonowaniem systemu informatycznego;
   2) instalację, konfigurację, serwisowanie oraz administrację zasobami sprzętowymi i oprogramowaniem wchodzącym w skład systemu informatycznego z uwzględnieniem aspektów bezpieczeństwa.

3. Eksploatacja systemów informatycznych obejmuję działania związane z:

   1) użytkowaniem systemu;
   2) okresowym testowaniem i kontrolą zaimplementowanych mechanizmów bezpieczeństwa oraz odpowiednim dokumentowaniem tych działań.

4. Za utrzymaniem systemów informatycznych odpowiada ASI.

5. IODO przy współpracy z ASI sprawuje nadzór merytoryczny nad eksploatacją i utrzymaniem właściwych mechanizmów bezpieczeństwa systemu informatycznego w PSW.

§ 10

Wycofanie systemów informatycznych

1. Systemy informatyczne, nośniki informacji lub inne zasoby informacyjne, które przestały być używane, wycofuje się z eksploatacji na podstawie pisemnego wniosku ASI/IODO.

2. Wycofanie systemu informatycznego z eksploatacji wymaga przestrzegania właściwych procedur bezpieczeństwa obejmujących w szczególności zasady postępowania:

   1) z informacją przetwarzaną w systemie informatycznym i nośnikami informacji;
   2) z dokumentacją bezpieczeństwa zasobu informatycznego

Rozdział V. Procedury rozpoczęcia zawieszenia i zakończenia pracy w systemie informatycznym

§ 11

1. Przed rozpoczęciem pracy użytkownik zobowiązany jest sprawdzić stan urządzeń oraz dokonać oględzin swojego stanowiska pracy w celu wykrycia ewentualnych nieprawidłowości mogących świadczyć o naruszeniu bezpieczeństwa danych osobowych.

2. W pomieszczeniu, w którym są przetwarzane dane osobowe mogą znajdować się osoby postronne tylko za zgodą i w towarzystwie użytkownika lub ASI.

3. Przed osobami postronnymi należy chronić ekranem komputerów (ustawienie monitora powinno uniemożliwiać podgląd), wydruki leżące na biurkach oraz w otwartych szafach;

4. Rozpoczęcie pracy:

   1) włączenie monitora;
   2) zalogowanie się poprzez wprowadzenie nazwy użytkownika i hasła:
   3) uruchomienie programu użytkowego.

5. Zawieszenie pracy w przypadku czasowego opuszczenia stanowiska pracy:

   1) zablokowanie sesji;
   2) w przypadku bezczynności na stacji roboczej przez czas przekraczający 5 minut włącza się wygaszacz ekranu z hasłem umożliwiającym ponowne podjęcie pracy.

6. Zakończenie pracy:

   1) zakończenie pracy programu zgodnie z instrukcją obsługi;
   2) wylogowanie z systemu;
   3) wyłączenie monitora;
   4) wyłączenie z sieci.

7. Krótkotrwała przerwa w pracy podczas, której użytkownik nie opuszcza stanowiska roboczego nie wymaga zamykania aplikacji i wylogowania.

§ 12

Zasady korzystania z komputerów przenośnych

1. Przetwarzanie danych osobowych poza obszarem przetwarzania na komputerze przenośnym wymaga zgody indywidualnej ASI udzielanej w formie pisemnej na wniosek osoby, która będzie dane przetwarzać.

2. O ile to możliwe przy przetwarzaniu danych osobowych na komputerach przenośnych obowiązują procedury określone w niniejszej Instrukcji dotyczące pracy na komputerach stacjonarnych, w tym:

   1) zabezpieczenie dostępu hasłem;
   2) obowiązek zmiany hasła przez użytkownika nie rzadziej niż co 30 dni;
   3) zastosowanie oprogramowania i zabezpieczeń analogicznie do rozwiązań przyjętych na stacjonarnych stacjach roboczych.

3. Pliki zawierające dane osobowe przechowywane na komputerach przenośnych są zaszyfrowane lub opatrzone hasłem dostępu

4. Obowiązuje zakaz używania komputerów przenośnych przez osoby inne niż użytkownicy, którym zostały one powierzone.

5. Obowiązuje zakaz przetwarzania na komputerach przenośnych całych zbiorów danych lub szerokich z nich wypisów, nawet w postaci zaszyfrowanej.

6. Użytkownicy przetwarzający dane osobowe na komputerach przenośnych obowiązani są do systematycznego wprowadzania tych danych w określone miejsce na serwerze ADO a następnie do trwałego usuwania ich z pamięci powierzonych komputerów przenośnych.

7. Osoba wykorzystująca komputer przenośny obowiązana jest do:

   1) wykorzystywania go wyłącznie do określonych celów mieszczących się w zakresie upoważnienia;
   2) nieudostępniania komputera nieupoważnionym osobom;
   3) zachowania szczególnej ochrony przed kradzieżą, zwłaszcza podczas transportu
   4) zaniechania jakichkolwiek zmian oprogramowania, jeżeli takie działania możliwe są poza poziomem ADO

8. W przypadku konieczności zmiany aktualizacji albo naprawy komputera należy zgłosić ten fakt ASI.

9. ADO w razie potrzeby wskazuje w dokumencie powierzenia komputera przenośnego osobie upoważnionej do przetwarzania danych osobowych konieczność i częstotliwość sporządzania kopii zapasowych danych przetwarzanych na komputerze przenośnym oraz określa zasady:

1) postępowania w razie nieobecności w pracy. Jeśli komputer przenośny nie może być zwrócony przed okresem nieobecności to użytkownik tego komputera powinien niezwłocznie powiadomić o tym ASI i uzgodnić z nim zwrot komputera przenośnego ADO;
2) zwrotu komputera w razie ustania stosunku pracy.

Rozdział VI. Sposoby zabezpieczenia systemu informatycznego

§ 13

1. W państwowej Szkole Wyższej im. Papieża Jana Pawła II istnieje bezwzględny wymóg instalacji oprogramowania antywirusowego na każdym stanowisku roboczym, zarówno na komputerach stacjonarnych jak i przenośnych wykorzystywanych do przetwarzania danych osobowych. Osobą odpowiedzialną za instalację programu antywirusowego jest ASI.

2. Sprawdzanie obecności wirusów komputerowych w systemie informatycznym oraz ich usuwanie odbywa się przy wykorzystaniu oprogramowania zainstalowanego na serwerach, komputerach stacjonarnych oraz komputerach przenośnych przez ASI.

3. Oprogramowanie, o którym mowa w ust. 2 sprawuje ciągły nadzór (ciągła praca w tle) nad pracą systemu i jego zasobami oraz serwerem i stacjami roboczymi.

4. Niezależnie od ciągłego nadzoru, o którym mowa w ust. 3 ASI nie rzadziej niż raz na tydzień przeprowadza kontrolę obecności wirusów komputerowych w systemie oraz jego zasobach. Ten fakt odnotowuje w dzienniku administratora, którego wzór określa załącznik nr 1 do Instrukcji.

5. Niedopuszczalne jest wyłączanie lub zmiana ustawień oprogramowania antywirusowego przez użytkowników.

6. Użytkownik jest obowiązany zawiadomić ASI o pojawiających się komunikatach wskazujących na wystąpienie zagrożenia wywołanego szkodliwym oprogramowaniem.

7. Użytkownicy mogą korzystać z zewnętrznych nośników danych tylko na stanowisku wydzielonym w sieci komputerowej ADO po uprzednim sprawdzeniu zawartości nośnika oprogramowaniem antywirusowym.

8. Niedopuszczalne jest otwieranie plików pobranych z Internetu lub korzystanie z zewnętrznych nośników bez uprzedniego przeskanowania zawartości przez program antywirusowy.

9. Przesyłanie danych osobowych pocztą elektroniczną dopuszczalne jest tylko w postaci zaszyfrowanej.

Rozdział VII. Wykonywanie przeglądów, konserwacji, napraw urządzeń systemu oraz nośników

§ 14

Procedura wykonywania przeglądów i konserwacji urządzeń

1. Przegląd i konserwacja urządzeń systemu winna być dokonywana zgodnie z zaleceniami producenta przez ASI , nie rzadziej niż co 3 miesiące.

2. Przeglądu i konserwacji systemu dokonuje ASI, który jest odpowiedzialny za terminowość i rzetelność przeglądów oraz konserwacji urządzeń. ASI odnotowuje ten fakt w książce serwisowej.

3. Zapisy logów systemowych powinny być przeglądane przez ASI codziennie oraz każdorazowo po wykryciu naruszenia zasad bezpieczeństwa.

4. Kontrole prowadzone przez IODO powinny obejmować zarówno dostęp do zasobów systemu, jak i profile oraz uprawnienia poszczególnych użytkowników.

5. Wszelkie nieprawidłowości wykryte podczas tych kontroli powinny być niezwłocznie usunięte a ich przyczyny oraz okoliczności sprzyjające przeanalizowane. O ile to możliwe, stosuje się odpowiednie środki w celu zapobieżenia występowaniu nieprawidłowości w przyszłości.

6. Przegląd programów i narzędzi przeprowadzany jest w przypadku zmiany wersji oprogramowania, zmiany systemu operacyjnego chyba, że zmiany te wynikają z aktualizacji automatycznej.

§ 15

Naprawy urządzeń komputerowych z chronionymi danymi osobowymi

1. Wszelkie naprawy urządzeń komputerowych oraz zmiany w systemie informatycznym przeprowadzane są - o ile to możliwe - przez pracowników Działu Teleinformatycznego pod nadzorem ASI.

2. ASI obowiązany jest do kontroli procesu przebiegu naprawy chyba, że niemożliwe jest jej przeprowadzenie w siedzibie ADO.

3. Naprawy i zmiany w systemie informatycznym przeprowadzane przez serwisanta prowadzone są pod nadzorem ASI w siedzibie ADO (o ile to możliwe) lub poza siedzibą ADO po uprzednim nieodwracalnym usunięciu danych w nich przetwarzanych a jeśli wiązało by się to z nadmiernymi utrudnieniami, to po podpisaniu umów powierzenia przetwarzania danych osobowych lub wymontowaniu dysku.

4. Jeśli nośnik danych (dysk, płyta lub inne) zostanie uszkodzony i nie można go odczytać ani usunąć z niego danych, należy go zniszczyć mechanicznie w niszczarce.

Rozdział VIII. Kopie zapasowe

§ 16

Cel i zasady tworzenia kopii zapasowych

1. W celu zwiększenia poziomu bezpieczeństwa oraz zapewnienia ciągłości działania w PSW tworzy się kopie zapasowe.

2. Kopie zapasowe tworzy się wykorzystując narzędzia programowe oraz narzędzia systemu.

3. Dostęp do kopii zapasowych mają tylko ADO, IODO i ASI.

4. Nośniki zawierające kopie zapasowe należy oznaczać jako „Kopia zapasowa dzienna/tygodniowa/miesięczna wraz z podaniem daty sporządzenia.

5. Kopie ulegają niezwłocznie zniszczeniu w sposób uniemożliwiający ich użycie, jeżeli zostanie stwierdzona ich nieprzydatność albo pojawią się okoliczności wyłączające legalność archiwizowania danych.

6. ASI obowiązany jest do prowadzenia rejestru kopii zapasowych.

§ 17

Procedura tworzenia kopii zapasowych

1. Kopie zapasowe tworzy się codziennie w godzinach nocnych wszystkich danych na sieciowe urządzenia pamięci masowych znajdujące się w innym pomieszczeniu niż serwerownia główna

2. W celu zapewnienia poprawności wykonywanych kopii bezpieczeństwa należy, co najmniej raz w tygodniu poddać testowi cyklicznie wybraną kopię. Próba polega na odtworzeniu danych w warunkach testowych i sprawdzeniu czy jest możliwość odczytania danych.

3. Archiwizacja kopii zapasowych przeprowadzana jest automatycznie w godzinach

4. nocnych przy pomocy wbudowanych w system funkcji.

5. harmonogram wykonywanych archiwizacji:

   1) kopie aktualnych baz danych oraz istotnych elementów systemu operacyjnego serwera są wykonywane codziennie;
   2) kopie baz archiwalnych są wykonywane codziennie.

6. ASI otrzymuje wiadomość o wykonaniu programu archiwizującego oraz okresowo

7. sprawdza możliwość odtworzenia danych z kopii zapasowych.

§ 18

Nośniki danych wykorzystywanych do sporządzania kopii zapasowych

1. Kopie zapasowe baz danych są nagrywane na zewnętrzne nośniki, takie jak: pamięć USB, sieciowe dyski pamięci.

2. W przypadku stosowania zewnętrznych nośników pamięci nośniki te wymieniane są okresowo i nie mogą być stosowane do więcej niż:

   1) taśmy magnetyczne – 2 cykli kopiowania;
   2) dyski CD - RW - 1 cyklu kopiowania;
   3) inne – zgodnie z zaleceniami producenta.

§ 19

Przechowywanie kopii zapasowych

1. Wszystkie nośniki bez względu na ich rodzaj są zabezpieczane przed nieautoryzowaną zmianą, zniszczeniem i dostępem.

2. Odpowiedzialność za zabezpieczenie, o którym mowa w ust. 1 ponosi ASI.

3. kopię zapasowe przechowuje się w zamkniętym pomieszczeniu w Dziale Teleinformatycznym. Dostęp do kopii zapasowych posiada wyłącznie ASI i upoważnieni przez ASI pracownicy.

4. Zabrania się przechowywania kopii zapasowych w pomieszczeniach przeznaczonych do przechowywania zbiorów danych pozostających w bieżącym użytkowaniu.

5. Wynoszenie nośników poza wskazany obszar jest niedopuszczalne z wyłączeniem wyjątkowych okoliczności za uprzednią zgodą ASI.

§ 20

Przechowywanie elektronicznych nośników informacji zawierających dane osobowe

1. Zbiory danych osobowych przechowywane są na serwerze obsługującym system informatyczny ADO. Wszelkie dane przetwarzane w pamięci stacji roboczych oraz komputerów przenośnych są niezwłocznie umieszczane w odpowiednich miejscach na serwerze, przydzielonych każdemu użytkownikowi przez ASI.

2. Zakazuje się przetwarzania danych osobowych na zewnętrznych nośnikach magnetycznych oraz ich przesyłania pocztą elektroniczną bez uprzedniego zaszyfrowania.

3. W przypadku posługiwania się nośnikiem danych pochodzącym od podmiotu zewnętrznego użytkownik jest zobowiązany do sprawdzenia go programem antywirusowym na wyznaczonym w tym celu stanowisku komputerowym oraz do oznakowania tego nośnika.

4. Nośniki magnetyczne raz użyte do przetwarzania danych osobowych nie mogą być wykorzystywane do innych celów mimo usunięcia danych i podlegają ochronie w trybie niniejszej Instrukcji.

5. Nośniki Informatyczne przechowywane są w miejscach do, których dostęp mają wyłącznie osoby upoważnione do przetwarzania danych osobowych.

§ 21

Likwidacja nośników zawierających kopie

1. Nośniki, które uległy uszkodzeniu lub zawierają nieaktualne kopie danych powinny zostać bezzwłocznie zniszczone.

2. W przypadku nośników jednorazowych takich jak płyty CD-R, DVD-R, likwidacja polega na ich fizycznym zniszczeniu w taki sposób, by nie można było odczytać ich zawartości.

3. Nośniki wielorazowego użytku takie jak dyski twarde, dyskietki, płyty CD - RW, DVD - RW można wykorzystać ponownie do celów przechowywania kopii bezpieczeństwa po uprzednim usunięciu ich zawartości.

4. Nośniki wielorazowego użytku nienadające się do ponownego użycia należy zniszczyć fizycznie.

5. Proces niszczenia kopii wykonywany jest przez ASI lub za jego zgodą przez wyspecjalizowany podmiot.

§ 22

Sposób zabezpieczenia systemu informatycznego przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego.

1. Sprawdzenie obecności wirusów komputerowych w systemie informatycznym oraz ich usuwanie odbywa się przy wykorzystaniu oprogramowania zainstalowanego na serwerach, stacjach roboczych oraz komputerach przenośnych automatycznie.

2. Oprogramowanie ,o którym mowa w pkt. 1 sprawuje ciągły nadzór (ciągła praca w tle) nad pracą systemu i jego zasobami oraz serwerami i stacjami roboczymi.

3. Do obowiązków administratora systemu należy monitorowanie aktualizacji oprogramowania antywirusowego oraz określenie częstotliwości automatycznych aktualizacji definicji wirusów dokonywanych przez to oprogramowanie.

4. Użytkownik niezwłocznie powiadamia ASI o pojawiających się komunikatach wskazujących na wystąpienie zagrożenia wywołanego szkodliwym oprogramowaniem.

§ 23

Postępowanie w przypadku stwierdzenia naruszenia bezpieczeństwa systemu informatycznego

Użytkownik zobowiązany jest zawiadomić IODO lub ASI o każdym naruszeniu lub podejrzeniu naruszenia bezpieczeństwa systemu. Szczegółowy opis znajduje się w Instrukcji postępowania w przypadku naruszenia ochrony danych osobowych w Państwowej Szkole Wyższej im. Papieża Jana Pawła II w Białej Podlaskiej

§ 25

Postanowienia końcowe

1. Instrukcja jest dokumentem wewnętrznym w Państwowej Szkole Wyższej im. Papieża Jana Pawła II w Białej Podlaskiej i jest obowiązkiem zachowania poufności przez wszystkie osoby, którym zostanie ujawniona.

2. W sprawach nieokreślonych niniejszą Instrukcja należy stosować instrukcje obsługi i zalecenia producentów aktualnie eksploatowanych urządzeń i programów.

3. każda osoba upoważniona do przetwarzania danych osobowych zobowiązana jest zapoznać się przed dopuszczeniem do przetwarzania danych z Instrukcją.

4. Niezastosowanie się do procedur określonych w Instrukcji przez pracowników upoważnionych do przetwarzania danych osobowych może być potraktowane jako naruszenie obowiązków pracowniczych skutkujące rozwiązaniem stosunku pracy bez wypowiedzenia na podstawie art. 52 Kodeksu pracy.

5. Instrukcja wchodzi w życie z dniem podpisania Zarządzenia wprowadzającego.

6. Do Instrukcji załącza się:

Załącznik nr 1 - Dziennik Administratora Systemu.
Załącznik nr 2 - Rejestr użytkowników posiadających wymienne nośniki danych.
Załącznik nr 3 - Rejestr wykonanych kopii danego systemu.
Załącznik - Instrukcja postępowania w przypadku naruszenia ochrony D.O. W PSW.

PAŃSTWOWA SZKOŁA WYŻSZA
im. Papieża Jana Pawła II
w Białej Podlaskiej
21-500 Biała Podlaska, ul. Sidorska 95/97
tel. 83 344 99 00, fax 83 344 99 50
NIP 537-21-31-853 REGON 050310705

Załącznik nr 1 do Zarządzenia Rektora nr 51/2018
Dotyczący Instrukcji zarządzania systemem informatycznym w PSW

DZIENNIK ADMINISTRATORA SYSTEMU

.....
nazwa systemu

Lp.	Data	Opis wydarzenia w systemie	Podpis ASI	Uwagi

PAŃSTWOWA SZKOŁA WYŻSZA
im. Papieża Jana Pawła II
w Białej Podlaskiej
21-500 Biała Podlaska, ul. Sidorska 95/97
tel. 83 344 99 00, fax 83 344 99 50
NIP 537-21-31-853 REGON 030310705

Załącznik nr 2 do Zarządzenia Rektora nr 51/2018 dotyczący Instrukcji zarządzania systemem informatycznym w PSW

REJESTR UŻYTKOWNIKÓW POSIADAJĄCYCH WYMIENNE NOŚNIKI DANYCH

Lp.	Imię i nazwisko użytkownika	Rodzaj wymiennego nośnika danych	Uwagi

PAŃSTWOWA SZKOŁA WYŻSZA
im. Papieża Jana Pawła II
w Białej Podlaskiej
21-500 Biała Podlaska, ul. Sidorska 95/97
tel. 83 344 99 00, fax 83 344 99 50
NIP 537-21-31-853 REGON 030310705

Załącznik nr 3 do Zarządzenia Rektora nr 51/2018
dotyczący Instrukcji zarządzania systemem informatycznym w PSW

REJESTR WYKONANYCH KOPII DANYCH SYSTEMU

Data	Nazwa i nr kopii przechowywanej na serwerze	Nazwa i nr kopii przechowywanej na nośniku zewnętrznym	Dysk twardy Dedykowanego urządzenia	Podpis osoby wykonującej kopię

PAŃSTWOWA SZKOŁA WYŻSZA
im. Papieża Jana Pawła II
w Białej Podlaskiej
21-500 Biała Podlaska, ul. Sidorska 95/97
tel. 83 344 99 00, fax 83 344 99 50
NIP 537-21-31-853 REGON 030310705

INSTRUKCJA

POSTĘPOWANIA W PRZYPADKU NARUSZENIA OCHRONY DANYCH OSOBOWYCH W PAŃSTWOWEJ SZKOLE WYŻSZEJ W BIAŁEJ PODLASKIEJ

1. Za naruszenie ochrony danych osobowych zgodnie z art.4 pkt 12 rodo uznaje się 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, w których stwierdzono naruszenie:
   1). zabezpieczenia systemu teleinformatycznego m.in.:
   - brak możliwości uruchomienia przez przetwarzającego aplikacji pozwalającej na dostęp do danych osobowych;
   - brak możliwości zalogowania się do tej aplikacji;
   - ograniczone w stosunku od normalnej sytuacji, uprawnienia przetwarzającego w aplikacji (na przykład brak możliwości wykonywania pewnych operacji normalnie dostępnych przetwarzającemu) lub uprawnienia poszerzone w stosunku do normalnej sytuacji;
   - wygląd aplikacji inny niż normalnie;
   - inny zakres danych niż dostępny dla przetwarzającego – dużo więcej lub dużo mniej danych;
   - znaczne spowolnienie działania systemu informatycznego;
   - pojawienie się niestandardowych komunikatów generowanych przez system Informatyczny;
   - podejrzenie nieautoryzowanej modyfikacji danych osobowych przetwarzanych w systemie informatycznym.
   2). zawartości bazy danych, przetwarzanych poza systemem teinformatycznym:
   - ślady włamania lub prób włamania do obszaru, w którym przetwarzane są dane osobowe;
   - ślady włamania lub prób włamania do pomieszczeń, w których odbywa się przetwarzanie danych osobowych, w szczególności do serwerowni oraz do pomieszczeń, w których przechowywane są nośniki kopi zapasowych;
   - włamanie lub próby włamania do szaf, w których przechowywane są w postaci elektronicznej lub papierowej nośniki danych osobowych;
   - zagubienie lub kradzież nośnika danych osobowych;
   - kradzież sprzętu informatycznego, którym przechowywane były dane osobowe;
   - informacja z systemu antywirusowego o zainfekowaniu systemu Informatycznego wirusami;
   - fizyczne zniszczenie lub podejrzenie zniszczenia elementów systemu

informatycznego przetwarzającego dane osobowe na skutek przypadkowych lub celowych działań albo zaistnienia działania siły wyższej.

2. Każda osoba biorąca udział w przetwarzaniu danych osobowych w systemie informatycznym lub tradycyjnym Uczelni, która stwierdzi lub podejrzewa naruszenie ochrony danych osobowych zobowiązana jest do natychmiastowego poinformowania Inspektora Ochrony Danych Osobowych Uczelni, którym jest *Jan Sroka*

3. Po otrzymaniu zgłoszenia o wystąpieniu symptomów wskazujących na możliwość zaistnienia naruszenia bezpieczeństwa danych osobowych Inspektor Ochrony jest zobowiązany do podjęcia kroków w celu:

   1). wyjaśnienia zdarzenia – we szczególności czy miało miejsce naruszenie ochrony danych osobowych;

   2). wyjaśnienia przyczyn naruszenia bezpieczeństwa danych osobowych i zebranie ewentualnych dowodów – szczególnie, gdy zdarzenie było związane z celowym działaniem pracowników lub osób trzecich;

   3). zabezpieczenia systemu informatycznego przed dalszym rozprzestrzenianiem się zagrożenia;

   4). usunięcia skutków incydentu i przywróceniu pierwotnego stanu systemu informatycznego (to jest stanu sprzed incydentu);

   5). ewentualnego ukarania sprawców incydentu.

4. Inspektor Ochrony Danych podejmuje działania w celu zapewnienia, by każda osoba działająca z upoważnienia Administratora (Rektor), która ma dostęp do danych osobowych przetwarzała je wyłącznie na polecenie Administratora.

5. Inspektor Ochrony Danych wspólnie z Administratorem Systemu Informatycznego podejmują działania zmierzające do wyjaśnienia zgłoszonego zdarzenia. W zależności od rodzaju zgłoszonego zdarzenia mogą dokonać w szczególności:

   1). wizji lokalnej w zakresie adekwatnym do rodzaju zgłoszonego zdarzenia;

   2). przeprowadzenie wywiadów z pracownikami w celu ustalenia zaistniałych faktów;

   3).przeprowadzenie analizy poprawności funkcjonowania systemu informatycznego, jeżeli zgłoszone zdarzenie było związane nieprawidłowym jego funkcjonowaniem;

   4). przeprowadzenie analizy zapisu zdarzeń w systemie informatycznym uwzględnieniem zapisu operacji realizowanych przez użytkowników;

   5). sporządzenie dokumentacji fotograficznej lub filmowej (w razie potrzeby);

   6). zabezpieczenie danych przetwarzanych w systemie informatycznym

dotkniętym incydentem, w szczególności danych konfiguracyjnych tego systemu;

7). zebranie innych materiałów pozwalających na wyjaśnienie przyczyn zaistnienia incydentu, jego charakteru i potencjalnych skutków;

8). rozważyć w miarę możliwości techniczno-organizacyjnych odłączenie systemu dotkniętego incydentem od pozostałej części infrastruktury informatycznej;

6. Administrator Danych (Inspektor Ochrony Danych) fakt naruszenia ochrony danych osobowych zgodnie a art. 33 rodo zgłasza do organu nadzorczego nie później niż w terminie 72 godzin po stwierdzeniu naruszenia chyba, że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw i wolności osób fizycznych (wzór zał. nr1).

7. Administrator Systemu Informatycznego przystępuje do usuwania skutków incydentu i przywrócenia prawidłowego przebiegu procesu przetwarzania danych osobowych W szczególności mogą one obejmować:

1). przeprowadzenie naprawy sprzętu informatycznego;

2). rekonfigurację sprzętu informatycznego;

3). wprowadzenie poprawek do oprogramowania;

4). odtworzenie danych z kopii awaryjnych;

5). modyfikację danych w celu odtworzenia ich integralności;

6). wycofanie z użycia materiału kryptograficznego.

8. Administrator może odstąpić od usuwania skutków incydentu, jeśli został on spowodowany działaniem celowym a całkowite wyjaśnienie zdarzenia i wyciągnięcie konsekwencji wobec sprawców jest istotniejsze niż przerwa w działaniu systemu. Istniejący stan systemu informatycznego nie powinien być zmieniany w celach dowodowych do czasu wyjaśnienia incydentu.

9. Przy usuwaniu skutków incydentu z wykorzystaniem odtwarzania danych z kopii awaryjnych, Administrator Systemu Informatycznego obowiązany jest upewnić się że odtwarzane dane zostały zapisane przed wystąpieniem incydentu – w szczególności dotyczy to przypadków odtwarzania systemu po infekcji wirusowej.

10. System informatyczny, którego prawidłowe działanie zostało odtworzone należy poddać szczegółowej obserwacji w celu stwierdzenia całkowitego usunięcia symptomów incydentu.

11. Opisane powyżej działania związane z usuwaniem skutków incydentu i wyjaśnieniem jego przyczyn mogą być realizowane przez osoby upoważnione przez Inspektora Danych Osobowych.

12. Inspektor Ochrony Danych Osobowych prowadzi ewidencję naruszeń ochrony danych osobowych, która obejmuje następujące informacje:

    1). imię i nazwisko osoby zgłaszającej incydent;

    2). imię i nazwisko osoby przyjmującej zgłoszenie incydentu;

    3). datę zgłoszenia incydentu;

    4). opis zgłoszonego incydentu;

    5). przeprowadzone badania wyjaśniające przyczyny zaistnienia incydentu;

    6). wyniki przeprowadzonych badań;

    7). podjęte akcje naprawcze i ich skuteczność.

13. Inspektor Ochrony Danych Osobowych odpowiedzialny jest za przeprowadzenie raz w roku analizy zaistniałych incydentów w celu:

    1). określenia skuteczności podejmowanych działań wyjaśniających i naprawczych;

    2). określenia wymaganych działań zwiększających bezpieczeństwo systemu informatycznego i minimalizujących ryzyko zaistnienia incydentu;

    3). określenia potrzeb w zakresie szkoleń użytkowników systemu informatycznego przetwarzających dane osobowe.

Inspektor Ochrony Danych Osobowych

.....
JAN SROKA

Administrator Systemu Informatycznego

.....
MARCIN STEFANOWICZ