

Polityka Bezpieczeństwa Danych Osobowych
ZESPÓŁ SZKÓŁ AGROTECHNICZNYCH w SŁUPSKU

Spis treści

1.	Wstęp	2
2.	Definicje	4
3.	Zadania i uprawnienia Administratora Bezpieczeństwa Informacji (ABI)	7
4.	Wykaz pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe	8
5.	Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych	8
6.	Opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi	8
7.	Sposób przepływu danych pomiędzy poszczególnymi systemami	9
8.	Środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności i rozliczności przetwarzanych danych	10
9.	Instrukcja alarmowa (postępowania w przypadku naruszenia ochrony danych osobowych)	13
9.1.	Zdarzenia zagrażające bezpieczeństwu danych osobowych	13
9.2.	Procedura postępowania w przypadkach naruszenia bezpieczeństwa danych osobowych	14
9.3.	Procedura postępowania w przypadkach zagrożeń (stwierdzenia słabości systemu)	14
10.	Procedura działań korygujących i zapobiegawczych	15
11.	Kontrola systemu ochrony danych osobowych i przegląd zarządzania	17
12.	Lokalizacja sprzętu komputerowego	17
13.	Plan ciągłości działania	18
14.	Postanowienia końcowe	18
15.	Załączniki	20

1. Wstęp

Celem Polityki Bezpieczeństwa jest zapewnienie Ochrony Danych Osobowych przetwarzanych przez Zespół Szkół Agrotechnicznych w Słupsku przed wszelakiego rodzaju zagrożeniami, tak wewnętrznymi jak i zewnętrznymi, świadomymi lub nieświadomymi.

Polityka określa obowiązki administratora danych w zakresie zabezpieczenia danych osobowych, o których mowa w art. 3 Ustawy o Ochronie Danych Osobowych z dnia 29 sierpnia 1997 roku (Dz. U. z 2002 r. Nr 101 z późniejszymi zmianami).

Polityka określa reguły dotyczące procedur zapewnienia bezpieczeństwa danych osobowych w postaci papierowej oraz zawartych w systemach informatycznych w Zespole Szkół Agrotechnicznych w Słupsku.

Jako załącznik do niniejszej polityki opracowano i wdrożono "Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych", zwaną dalej "Instrukcją zarządzania systemem informatycznym". Określa ona sposób zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych, ze szczególnym uwzględnieniem zapewnienia ich bezpieczeństwa.

Polityka została opracowana zgodnie z wymogami określonymi w § 4 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. z 2004 r. Nr 100, poz. 1024).

Polityka obowiązuje wszystkich pracowników w Zespole Szkół Agrotechnicznych w Słupsku oraz dostawców, podmiotów współpracujących na zasadzie umów, mających jakikolwiek kontakt z danymi osobowymi objętymi ochroną.

Ochrona danych osobowych jest realizowana poprzez: zabezpieczenia fizyczne, procedury organizacyjne, oprogramowanie systemowe, aplikacje oraz przez użytkowników.

Zastosowane zabezpieczenia mają służyć osiągnięciu powyższych celów i zapewnić:

1. Poufność danych - rozumianą jako właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym osobom.
2. Integralność danych - rozumianą jako właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany.
3. Rozliczność danych - rozumianą jako właściwość zapewniającą, że działania osoby mogą być przypisane w sposób jednoznaczny tylko tej osobie.
4. Integralność systemu - rozumianą jako nienaruszalność systemu, niemożność jakiegokolwiek manipulacji, zarówno zamierzonej, jak i przypadkowej.

Niniejszy dokument jest zgodny z następującymi aktami prawnymi:

- Ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002r. Nr 101 z późniejszymi zmianami).
- 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. z 2004 r. Nr 100, poz. 1024).
- Akty wykonawcze wydane na podstawie w/w. ustaw.

2. Definicje

Przez użyte w Polityce określenia należy rozumieć:

1. Polityka - rozumie się przez to Politykę bezpieczeństwa danych osobowych w Zespole Szkół Agrotechnicznych w Słupsku.
2. Administrator Danych Osobowych – Dyrektor Zespołu Szkół Agrotechnicznych w Słupsku (zwanym dalej ADO), decydujący o celach i środkach przetwarzania danych osobowych.
3. Administrator Bezpieczeństwa Informacji (ABI) – pracownik Zespołu Szkół Agrotechnicznych w Słupsku, wyznaczony przez ADO, odpowiedzialny za organizację ochrony danych osobowych.
4. Administrator Systemu Informatycznego (ASI) - Informatyk nadzorujący pracę systemu informatycznego oraz wykonujący w nim czynności wymagające specjalnych uprawnień.
5. Ustawa - ustawa z dnia 29 sierpnia 1997r. o ochronie danych osobowych (Dz. U. z 2002r. Nr 101, poz.92 z późniejszymi zmianami).
6. Rozporządzenie -Rozporządzenie Ministra Spraw Wewnętrznych Administracji i 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. z 2004 r. Nr 100, poz. 1024).
7. Baza danych osobowych- zbiór uporządkowanych powiązanych ze sobą tematycznie danych zapisanych np. w pamięci zewnętrznej komputera. Baza danych jest złożona z elementów o określonej strukturze -rekordów lub obiektów.
8. Dane osobowe (dane) - wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej.
9. Hasło -ciąg znaków literowych, cyfrowych lub innych, znanych jedynie osobie uprawnionej do pracy w systemie informatycznym.
10. Identyfikator użytkownika - ciąg znaków literowych, jednoznacznie identyfikujący osobę upoważnioną do danych osobowych w systemie informatycznym.

11. Integralność danych -właściwość zapewniająca, że dane nie zostały zmienione lub zniszczone w sposób nieautoryzowany.
12. Nośnik komputerowy -nośnik służący do zapisu i przechowywania informacji, np. taśmy, płytki CD/DVD, dyski twarde etc.
13. Odbiorca danych - każdy, komu udostępnia się dane osobowe, z wyłączeniem:
 - osoby, której dane dotyczą;
 - osoby upoważnionej do przetwarzania danych;
 - podmiotu, o którym mowa w art. 31 Ustawy;
 - przedstawiciela, o którym mowa w art. 31a Ustawy;
 - organów państwowych lub organów samorządu terytorialnego, którym dane są udostępniane w związku z prowadzonym postępowaniem.
14. Poufność danych - właściwość zapewniająca, że dane nie są udostępniane nieupoważnionym podmiotom.
15. Przetwarzanie danych -wykonywanie jakichkolwiek operacji na danych osobowych, np. zbieranie, utrwalanie, opracowywanie, udostępnianie, zmienianie, usuwanie.
16. Rozliczalność - właściwość zapewniająca, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi.
17. Raport - przygotowane przez system informatyczny zestawienia zakresu i treści przetwarzanych danych.
18. Sieć publiczna -sieć publiczna w rozumieniu Ustawy z dnia 16 lipca 2004 r. - Prawo telekomunikacyjne (Dz. U. Nr 171 poz. 1800).
19. Sieć Telekomunikacyjna-sieć telekomunikacyjna w rozumieniu Ustawa z dnia 16 lipca 2004 r. - Prawo telekomunikacyjne (Dz. U. Nr 171 poz. 1800).
20. System informatyczny - zespół (nazwa szkoły)zeń, programów i procedur przetwarzania informacji w celu przetwarzania danych.
21. Teletransmisja - przesyłanie informacji za pośrednictwem sieci telekomunikacyjnej.
22. Usuwanie danych – zniszczenie danych osobowych, lub taką ich modyfikację , która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą.
23. Uwierzytelnianie - działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu.

24. Użytkownik – pracownik Zespołu Szkół Agrotechnicznych w Słupsku posiadający uprawnienia do przetwarzania danych osobowych w zakresie obowiązujących przepisów o ochronie danych osobowych.
25. Zabezpieczenie danych w systemie informatycznym -wdrożenie i eksploatacja stosowanych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem.
26. Zbiór danych - zestaw danych osobowych posiadający określoną strukturę, prowadzony w/g określonych kryteriów oraz celów np. zbiór pracowników Zespołu Szkół Agrotechnicznych w Słupsku, zbiór interesantów Zespołu Szkół Agrotechnicznych w Słupsku.
27. 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.

3. **Zadania i uprawnienia Administratora Bezpieczeństwa Informacji (ABI)**

Do najważniejszych obowiązków Administratora Bezpieczeństwa Informacji należy:

1. Organizacja bezpieczeństwa i ochrony danych osobowych zgodnie z wymogami „Ustawy o Ochronie Danych Osobowych”.
2. Zapewnienie przetwarzania danych zgodnie z uregulowaniami niniejszej polityki.
3. Rejestracja zbiorów danych oraz wszelkich zmian z nimi związanych.
4. Prowadzenie "Ewidencji osób upoważnionych do przetwarzania danych osobowych".
5. Prowadzenie postępowania wyjaśniającego w przypadku naruszenia ochrony danych osobowych.
6. Nadzór nad bezpieczeństwem danych osobowych.
7. Kontrola działań komórek organizacyjnych pod względem zgodności przetwarzania danych z przepisami o ochronie danych osobowych.
8. Inicjowanie i podejmowanie przedsięwzięć w zakresie doskonalenia ochrony danych osobowych w Zespole Szkół Agrotechnicznych w Słupsku.

Administrator Bezpieczeństwa Informacji ma prawo :

1. 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.
2. Żądać złożenia pisemnych lub ustnych wyjaśnień w zakresie niezbędnym do ustalenia stanu faktycznego.
3. Żądać okazania dokumentów wszelkich danych mających bezpośredni związek z problematyką kontroli.
4. Żądać udostępnienia do kontroli (nazwa szkoły)zeń, nośników oraz systemów informatycznych służących do przetwarzania danych.

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

Szczegółowe rozmieszczenie zbiorów dokumentacji papierowej i elektronicznej, zawierającej dane osobowe, opisane jest w Załączniku A - "Wykaz zbiorów danych osobowych" w postaci papierowej i elektronicznej.

5. **Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych**

Wykaz zbiorów danych osobowych w postaci dokumentacji papierowej i elektronicznej wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych, opisany jest w Załączniku A - "Wykaz zbiorów danych osobowych".

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

Wykaz zbiorów danych osobowych zawierających informację o rodzaju danych osobowych opisany jest w Załączniku B - "Struktura baz danych osobowych w Zespole Szkół Agrotechnicznych w Słupsku.

Programy z zakresem przetwarzanych danych osobowych zawiera Załącznik B - „Struktura baz danych osobowych w Zespole Szkół Agrotechnicznych w Słupsku.

7. Sposób przepływu danych pomiędzy poszczególnymi systemami

System / Moduł "A"	System / Moduł "B"	Kierunek przepływu danych osobowych	Sposób przesyłania danych osobowych
Program Płace	Program Płatnik	Jednokierunkowo z programu Płace do Programu Płatnik	Manualnie przez wskazanie wygenerowanego pliku, Internet
Program WF GANG	Płatnik	Jednokierunkowo WF GANG-Płatnik	import automatyczny
Kseon Optivum Vulcan	Vulcan Plus	Jednokierunkowo KOV-VP	Manualnie - wskazanie wygenerowanego pliku
Program SIO	Organ prowadzący	Jednokierunkowo	Manualnie - wskazanie wygenerowanego pliku, Internet
Program HERMES	OKE	Jednokierunkowo	Manualnie - wskazanie wygenerowanego pliku, Internet

8. Środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności i rozliczności przetwarzanych danych

A. Środki ochrony fizycznej:

1. Podstawowe zabezpieczenia fizyczne opisane są w Załączniku A - "Wykaz zbiorów danych osobowych".
2. Przetwarzanie danych osobowych dokonywane jest w warunkach zabezpieczających dane przed dostępem osób nieupoważnionych.
3. Przebywanie osób nieuprawnionych w pomieszczeniach, gdzie przetwarzane są dane osobowe jest dopuszczalne tylko w obecności osoby zatrudnionej przy przetwarzaniu danych osobowych
4. Kopie zapasowe/archiwalne zbioru danych osobowych w formie elektronicznej przechowywane są w sejfie znajdującym się w gabinecie Dyrektora Zespołu Szkół Agrotechnicznych w Słupsku.

B. Środki sprzętowe, informatyczne i telekomunikacyjne:

1. Pomieszczenia, w którym przetwarzane są dane osobowe zabezpieczone są przed skutkami pożaru. Gaśnice rozmieszczone w korytarzu zgodnie z przepisami ochrony przeciwpożarowej.
2. Dokumenty zawierające dane osobowe po ustaniu przydatności są niszczone przez pocięcie w niszczarce.
3. Sprzęt komputerowy służący do przetwarzania danych osobowych połączony jest z siecią publiczną (Internetem) za pośrednictwem dwóch dostawców internetowych (Telekomunikacja Polska S.A, Systemy DK). Dostęp do sieci publicznej warunkują certyfikowane i zabezpieczone routery pełniących rolę bramy zabezpieczającej przed niepowołanym dostępem.
4. Lokalizacja urządzeń komputerowych (komputerów typu PC, laptop, drukarki) uniemożliwia osobom niepowołanym dostęp do nich oraz w miarę możliwości wglądu do danych wyświetlanych na monitorach komputerowych.
5. Komputery przenośne, wykorzystywane do przetwarzania danych osobowych, po zakończonej pracy są przechowywane w warunkach zapewniających ich bezpieczeństwo.

C. Środki ochrony w ramach oprogramowania (nazwa szkoły)zeń teletransmisji:

1. W razie wystąpienia konieczności wymiany danych pomiędzy Urzędem, a jednostkami zależnymi zastosowano system zapewniający poufność i integralność przesyłanych danych (szyfrowanie SSL, szyfrowanie WPA2).
2. Do połączenia z serwerem poczty wykorzystywane jest połączenie

z wykorzystaniem algorytmu SSL zapewniające poufność danych używanych do autoryzacji i uwierzytelniania.

3. Dostęp do Internetu realizowany jest za pomocą certyfikowanych, zabezpieczonych urządzeń technicznych (router) zapewniających ochronę przed nieautoryzowanym dostępem z zewnątrz.

D. Środki ochrony w ramach oprogramowania systemu

1. Dostęp do zbioru danych osobowych przetwarzanych za pomocą komputera zabezpieczony jest za pomocą hasła.
2. Zastosowano system operacyjny pozwalający na określenie odpowiednich praw dostępu do zasobów informatycznych dla poszczególnych użytkowników systemu informatycznego.
3. Zastosowano oprogramowanie umożliwiające wykonanie kopii zapasowych zbiorów danych osobowych na nośniku danych.

E. Środki ochrony w ramach narzędzi baz danych i innych narzędzi programowych:

1. Dostęp do zbioru danych osobowych zabezpieczony jest za pomocą procesu autoryzacji i uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła na poziomie aplikacji systemu służącego do przetwarzania zbioru.
2. Zastosowano identyfikator i hasło dostępu do danych na poziomie aplikacji.
3. Dla każdego użytkownika systemu jest ustalony odrębny identyfikator.
4. O ile aplikacja to umożliwia, zastosowano mechanizm wymuszający okresową zmianę haseł dostępu do zbioru danych osobowych.

F. Środki ochrony w ramach systemu operacyjnego stacji roboczych:

1. Zastosowano zabezpieczone hasłem wygaszanie ekranu w przypadku dłuższej nieaktywności użytkownika (30 minut).
2. Zastosowano działający w "tle" program antywirusowy na komputerach użytkowników firmy Kaspersky Internet Security 2015

G. Środki organizacyjne:

1. Wyznaczono Administratora Bezpieczeństwa Informacji w osobie Pana Jacka Wolikowskiego - nauczyciel
2. Wyznaczono Administratora Systemów Informatycznych oraz Zarządzającego Oprogramowaniem w osobie Pana Michała Gargasa - nauczyciel
3. Opracowano i wdrożono Politykę bezpieczeństwa i Instrukcję zarządzania systemem informatycznym.
4. Wdrożono odpowiedni podział obowiązków i kontroli.
5. ABI upoważnia w imieniu Administratora Danych pracowników do przetwarzania danych osobowych. Wzór upoważnienia w załączniku nr 2 do Instrukcji zarządzania

systemem informatycznym. Kopie upoważnienia przechowuje ABI.

6. W razie jakichkolwiek zmian lub cofnięcia upoważnień należy natychmiast powiadomić ABI i ASI.
7. Do danych osobowych mają dostęp jedynie osoby posiadające upoważnienie nadane przez Administratora Danych lub ABI.
8. Zespół Szkół Agrotechnicznych w Słupsku zatrudniając Stażystów lub Praktykantów musi podpisać z nimi upoważnienia na okres nie dłuższy niż 30 dni wskazując dokładnie jakie zbiory będą przetwarzać. Kopie upoważnień dostarczają ABI. Przedłużając upoważnienia muszą zachować tą samą powyższą procedurę.
9. ABI prowadzi "Ewidencję osób upoważnionych do przetwarzania danych osobowych".
10. Wprowadzono mechanizmy uwierzytelnienia i autoryzacji i zabezpieczeń przed dostępem osób trzecich.
11. Wprowadzono procedury alarmowe i informacyjne.
12. Osoby upoważnione do przetwarzania danych osobowych przed dopuszczeniem do tych danych są szkolone w zakresie obowiązujących przepisów o ochronie danych osobowych, procedur przetwarzania danych oraz informowane o podstawowych zagrożeniach związanych z przetwarzaniem danych osobowych. Osoby te są zobowiązane do podpisania stosownego oświadczenia.
13. Osoby zatrudnione przy przetwarzaniu danych osobowych obowiązane są do zachowania ich w tajemnicy.
14. Monitory komputerów, na których przetwarzane są dane osobowe ustawione są w miarę możliwości w sposób uniemożliwiający wgląd osobom postronnym.
15. Komputery przenośne mogą opuszczać teren Zespołu Szkół Agrotechnicznych w Słupsku po wydaniu zgody przez Administratora Danych lub Administratora Bezpieczeństwa Informacji.
16. Komputery przenośne spełniają wymogi bezpieczeństwa przy przetwarzaniu danych.
17. Tymczasowe wydruki z danymi osobowymi są po ustaniu ich przydatności niszczone w niszczarce.
18. Korespondencja w zakresie procedur kadrowo-płacowych prowadzona jest za pomocą listów poleconych.
19. Zapewnia się bezpieczne przechowywanie lub niszczenie uszkodzonych nośników zawierających dane osobowe (np. dysk twardy), szczególnie, gdy sprzęt, w którym zamontowany jest dany nośnik przekazywany jest do naprawy do firmy zewnętrznej.

20. ABI i ASI zobowiązani są do prowadzenia dziennika administratora w którym umieszczają wpisy związane z bezpieczeństwem informacji, systemów teleinformatycznych, awariach oraz aktualizacjach baz danych i programów je obsługujących.

21. Zobowiązano użytkowników do należytego zabezpieczenia dokumentów zawierających dane osobowe po zakończeniu pracy.

9. Instrukcja alarmowa (postępowania w przypadku naruszenia ochrony danych osobowych)

Procedury reagowania na zdarzenia zagrażające bezpieczeństwu danych osobowych określające:

czyż są zagrożenia i naruszenia danych osobowych;

- sposób reagowania, gdy wystąpią one w rzeczywistości;
- sposób postępowania po wystąpieniu naruszenia.

9.1. Zdarzenia zagrażające bezpieczeństwu danych osobowych

Do zdarzeń zagrażających bezpieczeństwu danych osobowych należą:

1. Próby naruszenia ochrony danych:

- zewnętrzne;
- wewnętrzne;

2. Programy destrukcyjne:

- wirusy,
- konie trojańskie,
- makra,
- bomby logiczne,

3. Awarie sprzętu lub uszkodzenie oprogramowania,

4. Zabór sprzętu lub nośników z ważnymi danymi,

5. Inne skutkujące utratą danych osobowych, bądź wejściem w ich posiadanie osób nieuprawnionych.

9.2. Procedura postępowania w przypadkach naruszenia bezpieczeństwa danych osobowych

1. W przypadku stwierdzenia faktu nieuprawnionego przetwarzania, ujawnienia lub nienależytego zabezpieczenia przed osobami nieuprawnionymi danych osobowych, jak również stwierdzenia istnienia przesłanek wskazujących na prawdopodobieństwo naruszenia ochrony danych osobowych, każdy pracownik Zespołu Szkół Agrotechnicznych w Słupsku zobowiązany jest poinformować o zdarzeniu Administratora Bezpieczeństwa Informacji, a ten Administratora Danych Osobowych.
2. W sytuacji, określonej w pkt. 1, Administrator Bezpieczeństwa Informacji prowadzi postępowanie wyjaśniające w toku, którego:
 - a. ustala czas wystąpienia naruszenia, jego zakres, przyczyny, skutki oraz wielkość szkód, które zaistniały,
 - b. ustala osoby odpowiedzialne za naruszenie,
 - c. podejmuje działania w kierunku ograniczenia szkód oraz przeciwdziałania podobnym przypadkom w przyszłości,
 - d. sporządza pisemną notatkę z przeprowadzonego postępowania.
3. Administrator Bezpieczeństwa Informacji powiadamia o wynikach postępowania wyjaśniającego Administratora Danych Osobowych.
4. W przypadku zaistnienia zdarzenia, określonego w ust. 1, decyzje dyscyplinarne w stosunku do winnych oraz w sprawie wniosku o pociągnięcie ich do odpowiedzialności karnej podejmuje Administrator Danych Osobowych.

9.3. Procedura postępowania w przypadkach zagrożeń (stwierdzenia słabości systemu)

1. W przypadku jakiegokolwiek nieprawidłowości w działaniu systemu, uszkodzenia lub podejrzenia o uszkodzenie sprzętu, oprogramowania lub danych należy bezzwłocznie powiadomić Administratora Bezpieczeństwa Informacji.
2. W przypadku włamania lub podejrzenia o włamanie do systemu Administrator Systemu Informatycznego podejmuje działania w celu zabezpieczenia systemu i danych:
 - a. zmienia hasła administracyjne, określa rodzaj i sposób włamania,
 - b. podejmuje działania w celu uniemożliwienia ponownego włamania tego samego typu,
 - c. szacuje straty w systemie,
 - d. przywraca stan systemu sprzed włamania.
3. W przypadku uszkodzenia sprzętu lub programów z danymi Administrator Systemu Informatycznego podejmuje działania w celu:

- a. określenia przyczyny uszkodzenia,
 - b. oszacowania strat wynikłych z w/w uszkodzenia,
 - c. naprawy uszkodzeń, a w szczególności naprawy sprzętu, ponownego zainstalowania danego programu, odtworzenie jego pełnej konfiguracji oraz wczytania danych z ostatniej kopii zapasowej.
4. W przypadku uszkodzenia danych Administrator Systemu Informatycznego podejmuje następujące działania:
 - a. ustala przyczynę uszkodzenia danych,
 - b. określa wielkość i jakość uszkodzonych danych,
 - c. podejmuje działania w celu odtworzenia danych z ostatniej kopii zapasowej.
5. W przypadku stwierdzenia nieprawidłowości w funkcjonowaniu sieci telekomunikacyjnej każdy użytkownik zobowiązany jest niezwłocznie powiadomić Administratora Systemu Informatycznego, który podejmuje działania w celu ustalenia przyczyn zaistniałej sytuacji oraz wyeliminowania nieprawidłowości.

W przypadku zidentyfikowania osób odpowiedzialnych za wystąpienie któregoś ze zdarzeń zagrażających bezpieczeństwu danych Administrator Bezpieczeństwa Informacji zobowiązany jest powiadomić Administratora Danych Osobowych.

10. Procedura działań korygujących i zapobiegawczych

1. Celem procedury jest uporządkowanie i przedstawienie czynności związanych z inicjowaniem oraz realizacją działań korygujących i zapobiegawczych wynikających z zaistnienia incydentów naruszenia bezpieczeństwa lub słabości systemu ochrony danych osobowych.
2. Procedura działań korygujących i zapobiegawczych obejmuje wszystkie te procesy, w których incydenty bezpieczeństwa, zagrożenia lub słabości systemu ochrony danych osobowych mogą wpłynąć na zgodność z wymaganiami Ustawy, jak również na poprawne funkcjonowanie systemu ochrony danych osobowych.
3. Osobą odpowiedzialną za nadzór nad procedurą jest Administrator Bezpieczeństwa Informacji. Przy czym czynności związane z realizacją poszczególnych zadań, zabezpieczeń zatwierdza Administrator Danych Osobowych.
4. Definicje
 - a. Niezgodność - niespełnienie wymagania, czyli potrzeby lub oczekiwania, które zostało ustalone, przyjęte zwyczajowo lub jest obowiązkowe.

- b. Incydent - naruszenie bezpieczeństwa informacji ze względu na poufność, dostępność i integralność.
 - c. Zagrożenie- potencjalna możliwość wystąpienia incydentu.
 - d. Słabość systemu - zdarzenie, stan rzeczy zwiększający ryzyko wystąpienia incydentu.
 - e. Działanie korygujące - jest to działanie przeprowadzane w celu wyeliminowania przyczyny wykrytej niezgodności i incydentu lub innej niepożądaney sytuacji.
 - f. Działanie zapobiegawcze - jest to działanie, które należy przedsięwziąć, aby wyeliminować przyczyny potencjalnej niezgodności i incydentu lub innej potencjalnej sytuacji niepożądaney.
 - g. Korekcja - działanie w celu wyeliminowania wykrytej niezgodności lub incydentu.
 - h. Kontrola (Audyt) - systematyczny, niezależny i udokumentowany proces oceny skuteczności systemu ochrony danych osobowych, na podstawie określonych kryteriów, wymagań, polityk i procedur.
5. Opis czynności Administratora Bezpieczeństwa Informacji (ABI)
- a. ABI jest odpowiedzialny za analizę incydentów naruszenia bezpieczeństwa, zagrożeń lub słabości systemu ochrony danych osobowych. Typowymi źródłami informacji o incydentach, zagrożeniach lub słabościach są:
 - zgłoszenia od pracowników;
 - alarmy z systemów informatycznych;
 - analizy incydentów;
 - wyniki audytów i kontroli.
 - b. Gdy ABI stwierdzi konieczność podjęcia działań korygujących lub zapobiegawczych, określa:
 - źródło powstania incydentu i zagrożenia lub słabości;
 - zakres działań korygujących lub zapobiegawczych;
 - termin realizacji;
 - osobę odpowiedzialną.
 - c. ABI jest odpowiedzialny za nadzór nad poprawnością i terminowością wdrażanych działań korygujących lub zapobiegawczych.
 - d. Po przeprowadzeniu działań korygujących lub zapobiegawczych, ABI jest zobowiązany do oceny efektywności ich zastosowania.
 - e. Powyższe zdarzenia są odnotowane przez ABI - Załącznik C - "Rejestr incydentów".

11. Kontrola systemu ochrony danych osobowych i przegląd zarządzania

1. Celem procedury jest uporządkowanie i przedstawienie czynności związanych z: kontrolą stanu bezpieczeństwa danych osobowych oraz okresową oceną Systemu Ochrony Danych Osobowych
2. Procedura obejmuje wszystkie procesy organizacji, gdzie przestrzeganie zasad ochrony danych osobowych jest wymagane.
3. Do kontroli stanu ochrony danych osobowych w Zespole Szkół Agrotechnicznych w Słupsku upoważnieni są:
 - a. Administrator Danych Osobowych;
 - b. Administrator Bezpieczeństwa Informacji.
4. Raz w roku kontroli (audytowi) podlegają wszystkie systemy informatyczne przetwarzające dane osobowe oraz zabezpieczenia fizyczne i bezpieczeństwo osobowe.
5. Administrator Bezpieczeństwa Informacji przygotowuje plan kontroli uwzględniając zakres oraz potrzebne zasoby fizyczne, czasowe i osobowe.
6. Kontroli podlega warstwa sprzętowa, systemy operacyjne, aplikacje, realizacja zabezpieczeń przez pracowników Zespołu Szkół Agrotechnicznych w Słupsku oraz przestrzeganie Polityki Bezpieczeństwa. Kontrola (audyt) przeprowadzana jest z użyciem dokumentu Załącznik D - "Zakres kontroli (audyt) ODO".
7. Po dokonanej kontroli Administrator Bezpieczeństwa Informacji przygotowuje raport pokontrolny. Na jego podstawie informuje Administratora Danych Osobowych o konieczności podjęcia właściwych działań korygujących i doskonalących.
8. Raz w roku po przeprowadzonej kontroli Administrator Bezpieczeństwa Informacji przygotowuje ocenę roczną stanu funkcjonowania systemu ochrony danych osobowych i przedstawia go Administratorowi Danych Osobowych. Potwierdzeniem przeprowadzenia przeglądu stanu ODO jest protokół - Wzór - Załącznik E - "Przegląd stanu bezpieczeństwa danych osobowych".

12. Lokalizacja sprzętu komputerowego

Szczegółowy opis systemu informatycznego w Zespole Szkół Agrotechnicznych w Słupsku przedstawia „Mapa sieci „ załącznik F do Polityki Bezpieczeństwa .

13. Plan ciągłości działania

1. Awaria systemów komputerowych:

W razie wystąpienia awarii systemów komputerowych należy powiadomić ASI:

Pan Michał Gargas tel. 661 968 000

2. Awaria Sieci:

W pierwszej kolejności kontakt do jak w pkt.1.

W innych przypadkach kontakt z operatorem sieci

a. Telekomunikacja Polska S.A. tel. 19330

b. Systemy DK tel. 795 541 394

Zdarzenia losowe (pożar, powódź etc.)

Wznowienie działania Zespołu Szkół Agrotechnicznych

Koordinator Pan Jacek Wolikowski tel. 517 465 998

Zgłoszenie szkody do firmy ubezpieczeniowej z którą Zespół Szkół Agrotechnicznych ma aktualną umowę ubezpieczeniową.

3. Instrukcja Bezpieczeństwa Pożarowego

14. Postanowienia końcowe

1. "Polityka Bezpieczeństwa" jest dokumentem wewnętrznym i nie może być udostępniana osobom postronnym w żadnej formie.
2. Każdy pracownik Zespołu Szkół Agrotechnicznych w Słupsku obowiązany jest zapoznać się z treścią polityki.
3. Pracownik zobowiązany jest złożyć oświadczenie o tym, iż został zaznajomiony z przepisami Ustawy o ochronie danych osobowych oraz wydanymi na jej podstawie aktami wykonawczymi oraz instrukcjami obowiązującymi u Administratora Danych, a także o zobowiązaniu się do ich przestrzegania.
4. Oświadczenie potwierdzające zaznajomienie użytkownika z przepisami Ustawy o ochronie danych osobowych oraz wydanymi na jej podstawie aktami wykonawczymi oraz instrukcjami obowiązującymi u Administratora Danych, a także o zobowiązaniu się do ich przestrzegania, przechowywane jest w aktach osobowych pracownika.
 - Przypadki, nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu potraktowane będą jako ciężkie naruszenie obowiązków pracowniczych. 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.

- Kara dyscyplinarna, orzeczona wobec osoby uchylającej się od powiadomienia nie wyklucza odpowiedzialności karnej tej osoby zgodnie z ustawą z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (tekst jednolity Dz. U. z 2002 z późniejszymi zmianami) oraz możliwości wniesienia wobec niej sprawy z powództwa cywilnego przez pracodawcę o zrekompensowanie poniesionych strat.
 - Wszystkie regulacje dotyczące systemów informatycznych określone w polityce dotyczą również przetwarzania danych osobowych w bazach prowadzonych w jakiegokolwiek innej formie.
5. Użytkownicy zobowiązani są do stosowania przy przetwarzaniu danych osobowych postanowień zawartych w niniejszej polityce.
 6. W sprawach nieuregulowanych w niniejszej polityce mają zastosowanie przepisy Ustawy z dnia 29 sierpnia 1997 r., o ochronie danych osobowych (tj. Dz. U. z 2002 r z późniejszymi zmianami) oraz wydane na jej podstawie akta wykonawcze.

15. Załączniki

1. Załącznik A- Wykaz zbiorów danych osobowych.
2. Załącznik B - Struktura baz danych osobowych w Zespole Szkół Agrotechnicznych w Słupsku.
3. Załącznik C - Rejestr incydentów.
4. Załącznik D - Zakres kontroli (audyt) ochrony danych osobowych.
5. Załącznik E- Wzór -Przegląd stanu bezpieczeństwa danych osobowych.
6. Załącznik F - Mapa sieci.
7. Załącznik G - Instrukcja zarządzania systemem informatycznym służącym do przetwarzania Danych Osobowych w Zespole Szkół Agrotechnicznych w Słupsku.
8. Załącznik nr.1 Oświadczenie – wzór.
9. Załącznik nr.2 Upoważnienie – wzór.
10. Załącznik nr. 3 Rejestr – wzór.
11. Załącznik nr. 4 Zlecenie nadania – wzór.