Zarządzenie Nr ZSZ-22/2017
Dyrektora Zespołu Szkół Zawodowych w Rawiczu
z dnia 28.08.2017r.

w sprawie wprowadzenia w Zespole Szkół Zawodowych im. Stefana Bobrowskiego w Rawiczu

Polityki Bezpieczeństwa Informacji
w Zespole Szkół Zawodowych im. Stefana Bobrowskiego w Rawiczu

§1

W celu ochrony danych osobowych w Zespole Szkół Zawodowych im. Stefana Bobrowskiego w Rawiczu oraz przetwarzania ich zgodnie z prawem, dyrektor wprowadza: ***Politykę Bezpieczeństwa Informacji w Zespole Szkole Zawodowych im. Stefana Bobrowskiego w Rawiczu*** w powiązaniu z:

1. ***Instrukcją zarządzania systemem informatycznym służącym do przetwarzania danych osobowych*** (załącznik nr 1),
2. ***Regulaminem korzystania z Systemu LIBRUS Synergia w Zespole Szkół Zawodowych im. S. Bobrowskiego w Rawiczu w zakresie ochrony danych osobowych*** (załącznik nr 2).

§2

Polityka i powiązane instrukcje wyznaczają zasady dostępu do danych osobowych oraz sposoby ich wykorzystania i zabezpieczenia przez pracowników Zespołu Szkół Zawodowych im. Stefana Bobrowskiego w Rawiczu.

§3

Zobowiązuje się wszystkich pracowników do zapoznania z treścią Polityki i powiązanych instrukcji.

§4

W skład polityki bezpieczeństwa wchodzą n/w dokumenty:

1. Wykaz zbiorów danych osobowych (załącznik nr 3).
2. Protokół przekazania danych osobowych – wzór (załącznik nr 4).
3. Ewidencja udostępniania danych osobowych – wzór (załącznik nr 5).
4. Oświadczenie o zachowaniu w tajemnicy danych osobowych oraz o zapoznaniu się z dokumentami (wymienione w oświadczeniu) – wzór (załącznik nr 6).
5. Upoważnienie do przetwarzania danych osobowych uczniów i rodziców (opiekunów prawnych) – wzór (załącznik nr 7).
6. Upoważnienie do przetwarzania danych osobowych pracowników – wzór (załącznik nr 8).
7. Upoważnienie do przetwarzania danych osobowych uczniów, rodziców (opiekunów prawnych) i pracowników – wzór (załącznik nr 9).
8. Rejestr upoważnień – wzór (załącznik nr 10).
9. Ewidencja osób upoważnionych do przetwarzania danych osobowych – wzór (załącznik nr 11).
10. Potwierdzenie otrzymania dostępu do kont rodzica/opiekuna i ucznia/uczennicy oraz zapoznania się z zasadami funkcjonowania dziennika elektronicznego (załącznik nr 12).
11. Deklaracja dochowania tajemnicy danych z dziennika elektronicznego, wynikającej z Ustawy o Ochronie Danych Osobowych przez osoby nie zatrudnione w szkole (załącznik nr 13).

§5

Wycofuje się zarządzenie poprzednie Nr ZSZ-0132-9/2017 z dnia 4.05.2017r.
Upoważnienia do przetwarzania danych osobowych wydane przed 31.08.2017 tracą moc.
Powołanie Administratora Bezpieczeństwa Informacji wydane przed 31.08.2017 traci moc.

Powołanie Administratora Systemu Informatycznego wydane przed 31.08.2017 traci moc.

§6

Zarządzenie niniejsze obowiązuje od dnia 31.08.2017r.

……..……

(podpis dyrektora)

Polityka Bezpieczeństwa Informacji

w Zespole Szkół Zawodowych im. Stefana Bobrowskiego w Rawiczu

Podstawa prawna:

1. Ustawa z dnia 29 sierpnia 1997r. o ochronie danych osobowych (Dz.U. z 2016r., poz. 922), art.36 ust.2.
2. Rozporządzenie 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. 2004 nr 100 poz. 1024), paragraf 4 i 5.
3. Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. z 2016r., poz. 113), §20 ust.1.
4. Rozporządzenie Ministra Administracji i Cyfryzacji z dnia 10 grudnia 2014r. w sprawie wzorów zgłoszeń powołania i odwołania administratora bezpieczeństwa informacji (Dz. U. z 2014r., poz. 1934).
5. Rozporządzenie 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 bezpieczeństwa informacji (Dz. U. z 2015r., poz. 745).
6. Rozporządzenie Ministra Administracji i Cyfryzacji z dnia 11 maja 2015r. w sprawie sposobu prowadzenia przez administratora bezpieczeństwa informacji rejestru zbiorów danych (Dz. U. z 2015r., poz. 719).

Rozdział I. Postanowienia ogólne.

§ 1

Niniejsza *Polityka Bezpieczeństwa Informacji w Zespole Szkół Zawodowych im. Stefana Bobrowskiego w Rawiczu* została opracowana zgodnie z wymogami 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. 2004 nr 100 poz. 1024). Stanowi ona zestaw praw i reguł regulujących sposób zarządzania, ochrony i dystrybucji danych osobowych w Zespole Szkół Zawodowych w Rawiczu.

§ 2

Określenia i skróty użyte w Polityce oznaczają:

1. Administrator Danych Osobowych – Dyrektor Szkoły, zwany dalej ADO.
2. Administrator Bezpieczeństwa Informacji, zwany dalej ABI – pracownik powołany przez ADO, odpowiedzialny za nadzorowanie i przestrzeganie zasad ochrony, określonych w niniejszych dokumentach oraz wymagań w zakresie wynikającym z powszechnie obowiązujących przepisów prawa. ABI mianowany został odrębnym zarządzeniem przez ADO.
3. Administrator Systemu Informatycznego, zwany dalej ASI – pracownik wyznaczony przez ADO, odpowiedzialny za wdrożenie i stosowanie zasad bezpieczeństwa danych osobowych w zakresie technicznych zabezpieczeń systemu informatycznego Zespołu Szkół Zawodowych. ASI mianowany został odrębnym zarządzeniem przez ADO.

4. Dane osobowe – wszelkie informacje umożliwiające zidentyfikowanie osoby uczącej i pracującej w Zespole Szkół Zawodowych w Rawiczu.
5. Osoba upoważniona lub użytkownik systemu, zwany dalej użytkownikiem – osoba posiadająca upoważnienie przez ADO i uprawniona do przetwarzania danych osobowych w zakresie wskazanym w upoważnieniu. Użytkownikiem systemu może być pracownik Zespołu Szkół Zawodowych w Rawiczu wykonujący pracę na podstawie umowy o pracę, umowy zlecenia lub innej umowy cywilno – prawnej.
6. Identyfikator – należy przez to rozumieć elektroniczne, indywidualne oznaczenie pracowników w systemie informatycznym, tzw. login.
7. Ustawę – należy przez to rozumieć ustawę o ochronie danych osobowych z dnia 29 sierpnia 1997r. (Dz.U. z 2016r., poz. 922).
8. System informatyczny, zwany dalej systemem, w rozumieniu art. 7 pkt 2a) Ustawy.
9. Zabezpieczenie danych w systemie, zwane dalej zabezpieczeniem – czynności wykonywane w rozumieniu art. 7 pkt 2b) Ustawy.
10. Zespół Szkół Zawodowych w Rawiczu im. Stefana Bobrowskiego, zwany dalej Szkołą.
11. System LIBRUS Synergia w Zespole Szkół Zawodowych w zakresie ochrony danych osobowych zwany dalej E - dziennikiem.

Rozdział II. Cele i zakres polityki bezpieczeństwa.

§ 3

Polityka zakłada pełne zaangażowanie Dyrekcji oraz pracowników Szkoły dla zapewnienia bezpieczeństwa danych osobowych przetwarzanych zarówno w sposób tradycyjny (w wersji papierowej), jak i za pomocą systemów informatycznych.

§ 4

1. Polityka określa podstawowe zasady bezpieczeństwa przetwarzanych w Szkole danych osobowych.
2. Polityka dotyczy wszystkich danych osobowych, przetwarzanych w Szkole, niezależnie od formy ich przetwarzania.

§ 5

Celem Polityki jest zapewnienie ochrony danych osobowych przetwarzanych przez Zespół Szkół Zawodowych w Rawiczu przed wszelkiego rodzaju zagrożeniami, tak wewnętrznymi jak i zewnętrznymi, świadomymi lub nieświadomymi**.**

§ 6

Cele Polityki realizowane są poprzez zapewnienie danym osobowym następujących cech:

a. poufności – właściwości zapewniającej, że dane nie są udostępniane nieupoważnionym podmiotom,
b. integralności – właściwości zapewniającej, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany,
c. rozliczalności – właściwości zapewniającej, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi,
d. zgodności z prawem – właściwości zapewniającej, że gromadzone są wyłącznie dane niezbędne do właściwego funkcjonowania szkoły i realizowania przez nią zadań określonych w odrębnych przepisach.

W zawiązku z tym Szkoła może przetwarzać tylko takie informacje o pracownikach, które mają bezpośredni i jednoznaczny związek ze stosunkiem pracy oraz tylko takie informacje o uczniach, które związane są z procesem dydaktycznym podczas nauki w Szkole.

§ 7

Dla skutecznej realizacji Polityki ADO zapewnia:

a. odpowiednie do zagrożeń i kategorii danych objętych ochroną, środki techniczne i rozwiązania organizacyjne,
b. szkolenia w zakresie przetwarzania danych osobowych i sposobów ich ochrony,
c. monitorowanie zastosowanych środków ochrony.

§ 8

ADO zapewnia zgodność niniejszej Polityki z przepisami określającymi zasady przetwarzania danych osobowych oraz z polskimi normami ustanawiającymi wytyczne w dziedzinie zarządzania bezpieczeństwem systemów teleinformatycznych, tj.:

1. Ustawą z dnia 29 sierpnia 1997r. o ochronie danych osobowych (Dz.U. z 2016r., poz. 922),
2. Rozporządzeniem 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. 2004 nr 100 poz. 1024),
3. Normą PN-I-13335-1 „Technika informatyczna. Wytyczne do zarządzania bezpieczeństwem systemów informatycznych",
4. Normą PN-ISO/IEC-17799 „Technika informatyczna. Praktyczne zasady zarządzania bezpieczeństwem informacji".

Rozdział III. Obowiązki i odpowiedzialność w zakresie zarządzania bezpieczeństwem.

§ 9

1. Zarządzanie bezpieczeństwem systemów jest procesem ciągłym, realizowanym przy współdziałaniu osób upoważnionych do przetwarzania danych z ADO, ABI i ASI.
2. Wszystkie osoby upoważnione do przetwarzania danych zobowiązane są do:
   a. przetwarzania danych osobowych zgodnie z obowiązującymi przepisami,
   b. postępowania zgodnie z ustaloną przez ADO Polityką.
3. W przypadku naruszenia przepisów lub zasad postępowania, osoba upoważniona do przetwarzania danych osobowych podlega odpowiedzialności służbowej i karnej.
4. Użytkownik systemu ponosi wszelką odpowiedzialność za wszystkie operacje wykonane przy użyciu jego identyfikatora i hasła dostępu.
5. Wszelkie przekroczenia lub jakiekolwiek próby przekroczenia przyznanych uprawnień, traktowane będą jako naruszenie podstawowych obowiązków pracowniczych.
6. Na pisemny i uzasadniony wniosek administratora systemu informatycznego ABI może odebrać uprawnienia pracownikowi z podaniem daty oraz przyczyny odebrania uprawnień. W uzasadnionej sytuacji ABI może odebrać uprawnienia w sposób natychmiastowy. Z takiego postępowania ma on sporządzić notatkę służbową do wiadomości użytkownika systemu, którego sprawa dotyczy.
7. Użytkownika systemu, który utracił login i hasło, należy niezwłocznie wyrejestrować z systemu informatycznego. Wyrejestrowania z systemu dokonuje ASI.
8. Użytkownik systemu zatrudniony przy przetwarzaniu danych osobowych zobowiązany jest do zachowania ich w poufności oraz dołożenia wszelkich starań, aby dane osobowe nie zostały przekazane osobom nieuprawnionym.

§ 10

Osoby upoważnione przez ADO do przetwarzania danych osobowych zobowiązane są do:

a. ścisłego przestrzegania zakresu udzielonego upoważnienia,
b. zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia,

c. zgłaszania ADO incydentów związanych z naruszeniem bezpieczeństwa danych oraz niewłaściwego funkcjonowania systemu, a także informowania o przypadkach naruszenia bezpieczeństwa danych.

Rozdział IV. Ogólne zasady przetwarzania danych osobowych.

§ 11

1. Każdy uczeń i pracownik Szkoły ma prawo do ochrony dotyczących go danych osobowych.
2. Dane osobowe są przetwarzane w Szkole w celu realizacji zadań określonych przepisami prawa.
3. Należy dochować szczególnej staranności w realizacji przedsięwzięć dotyczących ochrony interesów osób, których dane dotyczą oraz przestrzegania zasad bezpieczeństwa przetwarzania danych osobowych, uwzględniając:
    a. przepisy prawa,
    b. zasady udostępniania danych osobowych,
    c. dotrzymanie okresu przechowywania danych identyfikujących osobę,
    d. procedury ochrony danych osobowych.

§ 12

1. Naczelną zasadą przetwarzania danych osobowych w Szkole jest zachowanie w tajemnicy przez osoby mające dostęp do danych, wszelkich informacji dotyczących ich przetwarzania oraz sposobów zabezpieczania.
2. Możliwość wystąpienia zagrożeń danych przetwarzanych w systemach lub kartotekach, skorowidzach, księgach, wykazach i innych zbiorach ewidencyjnych nakłada na użytkowników i ich przełożonych obowiązek wykonywania czynności, związanych z zapewnieniem danym właściwej ochrony.
3. Przekazywanie danych osobowych w formie papierowej do organu prowadzącego i innych instytucji współpracujących ze Szkołą dokonywany jest wyłącznie przez osoby posiadające upoważnienia.
4. Kopiowanie danych osobowych oraz wykonywanie wydruków jest zabronione, chyba, że konieczność ich sporządzania wynika z nałożonych na użytkownika obowiązków i dozwolona jest przepisami prawa.
5. Kopie zawierające dane osobowe można przekazywać tylko osobom upoważnionym lub podmiotom do tego uprawnionym.
6. Kopie, o których mowa w ust. 5, mogą być wykorzystywane tylko w celach, do jakich zostały sporządzone. Niepotrzebne kopie należy niszczyć w sposób uniemożliwiający ich odtworzenie.

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

§ 13

1. Przetwarzanie danych osobowych odbywa się w Zespole Szkół Zawodowych im. Stefana Bobrowskiego w Rawiczu przy ulicy:
    - Gen. Hallera 6, 8, 10, 12,
    - Sienkiewicza 27
    - Grota Roweckiego 9

2. Za obszar przetwarzania danych należy rozumieć obszar, w którym wykonywana jest choćby jedna z czynności wymienionych w art. 7 pkt. 2 Ustawy Obszarami

do przetwarzania danych osobowych z użyciem sprzętu komputerowego oraz sposobem ręcznym są:

Budynek A, ul. Gen. Hallera 12
- gabinet Wicedyrektora obszar za biurkiem ze wszystkimi urządzeniami oraz szafy,
- biblioteka szkolna obszar za biurkiem nauczyciela bibliotekarza ze wszystkimi urządzeniami,
- pokój nauczycielski ze sprzętem komputerowym oraz szafy,
- we wszystkich salach lekcyjnych biurko nauczyciela ze sprzętem komputerowym.

Budynek B, ul. Gen Hallera 10
- gabinet Wicedyrektora obszar za biurkiem ze wszystkimi urządzeniami oraz szafy,
- we wszystkich salach lekcyjnych biurko nauczyciela ze sprzętem komputerowym,
- pokój nauczycielski ze sprzętem komputerowym oraz szafy.

Sala Gimnastyczna, ul. Gen Hallera 8
- wydzielona część sekretariatu Szkoły, obszar za ladą ze wszystkimi urządzeniami oraz szafy i szafy aktowe ze skarbczykiem,
- gabinet Dyrektora Głównego ze wszystkim urządzeniami oraz szafy,
- pokój nauczycielski nauczycieli wychowania fizycznego – sprzęt komputerowy oraz szafy,
- serwerownia ze wszystkimi urządzeniami.

Budynek C, ul. Gen Hallera 6
- gabinet Wicedyrektora obszar za biurkiem ze wszystkimi urządzeniami oraz szafy,
- gabinet Głównego Księgowego obszar za biurkiem ze wszystkimi urządzeniami oraz szafy,
- biuro księgowości – obszar za biurkami ze wszystkimi urządzeniami oraz szafy,
- gabinet kadrowej – obszar za biurkiem ze wszystkimi urządzeniami oraz szafy,
- pomieszczenie Archiwum z szafami,
- gabinet pedagoga szkolnego obszar za biurkiem ze sprzętem komputerowym oraz szafy,
- we wszystkich salach lekcyjnych biurko nauczyciela za sprzętem komputerowym,
- biuro projektu – obszar za biurkiem ze wszystkimi urządzeniami oraz szafy,
- MCI – biurka ze sprzętem komputerowym,
- pokój nauczycielski wraz ze sprzętem komputerowym oraz szafy.

Budynek G, ul. Grota Roweckiego 9
- we wszystkich salach lekcyjnych biurko nauczyciela za sprzętem komputerowym,
- pokój nauczycielski wraz ze sprzętem komputerowym oraz szafy.

Budynki Warsztatów Szkolnych, ul. Sienkiewicza 27
- we wszystkich salach lekcyjnych biurko nauczyciela,
- pokój nauczycielski wraz ze sprzętem komputerowym oraz szafy,
- pomieszczenie biuro – obszar ze wszystkimi urządzeniami oraz szafy.

3. Przebywanie osób nieuprawnionych wewnątrz obszaru, o którym mowa w pkt. 2, jest dopuszczalne tylko w obecności osób zatrudnionych przy przetwarzaniu tych danych lub za zgodą ADO.

4. Przetwarzanie danych osobowych to wykonywanie na nich operacji takich jak: zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie, usuwanie zarówno w systemie informatycznym, jak i ręcznym.

Rozdział VI. Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych.

§ 14

1. W Szkole dane osobowe mogą być przetwarzane w zbiorach danych, przy zastosowaniu systemów oraz zbiorów ewidencyjnych w postaci kartotek, skorowidzów, ksiąg i wykazów.
2. *Wykaz zbiorów danych osobowych* wymieniony jest w załączniku nr 3. Wykaz może być zmieniany decyzją ADO.
3. Osoby upoważnione do przetwarzania danych tworzą zbiory danych osobowych lub wnioskują o ich wycofanie, zgodnie z potrzebami realizacji zadań służbowych, za zgodą ADO.

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

§ 15

1. Tworzy się zbiory danych osobowych przez nadanie danym osobowym odpowiedniej struktury, dostępnej według określonych kryteriów, niezależnie od tego, czy zestaw danych jest rozproszony lub podzielony funkcjonalnie.
2. Przetwarzanie danych osobowych może odbywać się metodą:
   a. papierową, w której dane osobowe przetwarza się klasycznie w postaci dokumentów,
   b. informatyczną, w której dane osobowe przetwarza się w systemie informatycznym,
   c. dualną, w której dane osobowe przetwarza się klasycznie i jednocześnie w systemie informatycznym,
   d. zbiorów rozproszonych, w której dane osobowe przetwarzane są w kilku obszarach przetwarzania.
3. Zawartość pól informacyjnych, występujących w systemach zastosowanych w celu przetwarzania danych osobowych, musi być zgodna z przepisami prawa, które uprawniają lub zobowiązują ADO do przetwarzania danych osobowych.

Rozdział VIII. Sposób przepływu danych pomiędzy poszczególnymi systemami.

§ 16

1. Przepływ danych pomiędzy systemami zastosowanymi w celu przetwarzania danych osobowych może odbywać się w postaci przepływu jednokierunkowego lub przepływu dwukierunkowego.
2. Przepływ jednokierunkowy oznacza, że system informatyczny udostępnia dane ze zbioru (bazy) danych tylko w trybie „do odczytu".
3. Przepływ dwukierunkowy umożliwia upoważnionemu użytkownikowi korzystanie z danych w trybach „do odczytu" i „do zapisu", tj. umożliwia wprowadzanie nowych danych i modyfikację istniejących.
4. Przesyłanie danych pomiędzy systemami może odbywać się w sposób manualny, przy wykorzystaniu nośników zewnętrznych (np. dyskietka, CD, DVD, dysk zewnętrzny, PenDrive itp.) lub w sposób półautomatyczny, przy wykorzystaniu funkcji eksportu/ importu danych za pomocą teletransmisji (np. poprzez wewnętrzną sieć teleinformatyczną).

5. Przesyłanie danych może odbywać się zarówno w obrębie szkoły, jak i na zewnątrz (m.in. do organu prowadzącego Szkołę lub podmiotów współpracujących ze Szkołą w organizowaniu zadań związanych z procesem edukacyjnym, w szczególności organizujących egzamin maturalny, egzamin potwierdzający kwalifikacje w zawodzie, proces rekrutacyjny, e-dziennik).

Rozdział IX. Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych.

§ 17

ADO zapewnia zastosowanie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych.

§ 18

1. Środki ochrony zastosowane przez ADO dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych, obejmują:
    a. środki fizyczne,
    b. środki osobowe,
    c. środki techniczne.
2. Środki ochrony fizycznej obejmują:
    a. lokalizację miejsc przetwarzania danych osobowych w pomieszczeniach o ograniczonym i kontrolowanym dostępie,
    b. ustalenie zasad pobierania kluczy do pomieszczeń i szaf,
    c. składowanie zbiorów danych osobowych (w tym nośników wymiennych i nośników kopii zapasowych) w odpowiednio zabezpieczonych pomieszczeniach i szafach.
3. Środki ochrony osobowej obejmują:
    a. dopuszczenie do przetwarzania danych osobowych wyłącznie osób posiadających upoważnienie wydane przez ADO,
    b. zapoznanie tych osób z zasadami przetwarzania danych osobowych oraz obsługą systemu służącego do przetwarzania danych.
4. Środki ochrony technicznej obejmują:
    a. mechanizmy kontroli dostępu do systemów i zasobów,
    b. zastosowanie odpowiednich i regularnie aktualizowanych informatycznych narzędzi ochronnych,
    c. regularne tworzenie kopii zapasowych zbiorów danych przetwarzanych w systemach informatycznych.

Rozdział X. Aktualizacja regulacji wewnętrznych.

§ 19

Co najmniej raz w roku odbywa się udokumentowany przegląd Polityki Bezpieczeństwa Informacji i innych procedur dotyczących ochrony informacji. Przeglądu dokonuje Administrator Bezpieczeństwa Informacji. Po przeglądzie sporządzany jest Raport. Administrator Bezpieczeństwa Informacji przedstawia Raport Administratorowi Danych Osobowych w terminie 30 dni od dnia dokonania przeglądu.

Rozdział XI. Szkolenie z zakresu przetwarzania danych osobowych.

§ 20

1. Każda osoba przed rozpoczęciem przetwarzania danych osobowych ma obowiązek zapoznania się z przepisami dotyczącymi bezpieczeństwa przetwarzania i ochrony danych osobowych.

2. ADO zobowiązany jest umożliwić podwładnym zapoznanie się z przepisami, o których mowa w ust. 1.
3. W przypadku wprowadzania w Szkole nowych przepisów dotyczących wdrażania procedur przetwarzania i ochrony danych osobowych, ADO może zorganizować dodatkowe szkolenia dla określonych grup użytkowników.

Rozdział XII. Inwentaryzacja sprzętu i oprogramowania.

§ 21

ASI na bieżąco dokonuje inwentaryzacji sprzętu i oprogramowania. Nie rzadziej niż raz na pół roku sporządza raport. W ciągu 30 dni od sporządzenia raportu ASI przedstawia raport Administratorowi Danych Osobowych.

Rozdział XIII. Analiza utraty integralności, dostępności i poufności informacji.

§ 22

Nie rzadziej niż raz w roku Administrator Danych Osobowych przeprowadza analizę utraty integralności, dostępności i poufności informacji oraz podejmuje działania minimalizujące ryzyka z tych analiz wynikające.

Rozdział XIV. Obowiązki osób powołanych przez ADO.

§ 23

Do zadań ABI należy:
1. wykonywanie zadań z zakresu przetwarzania i ochrony danych zgodnie z przepisami Ustawy, organizując je, koordynując i nadzorując,
2. prowadzenie Rejestru zbiorów danych,
3. prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych. Ewidencja odzwierciedla aktualny stan w zakresie użytkowników i ich uprawnień.
4. dokonywanie przeglądów Polityki Bezpieczeństwa Informacji i innych procedur dotyczących ochrony informacji,
5. zapewnienie przestrzegania przepisów o ochronie danych osobowych zgodnie z Rozporządzeniem Ministra Administracji i Cyfryzacji z dnia 11 maja 2015 r., m.in. sporządzanie planu sprawdzeń i sprawozdań,
6. prowadzenie dokumentacji związanej z udostępnianiem danych osobowych,
7. reagowanie na zgłoszenia dotyczące naruszenia zasad ochrony informacji,
8. prowadzenie szkoleń dotyczących ochrony informacji, we współpracy z ADO, uczestniczenie w szkoleniach dla ABI.

ABI stosuje środki techniczne i przedsięwzięcia organizacyjne zapewniające skuteczną realizację zadań bezpieczeństwa zbiorów danych przetwarzanych w Szkole.

§ 24

Do zadań ASI należy:
1. administrowanie systemami, w których przetwarzane są dane osobowe,
2. nadawanie użytkownikom identyfikatorów i haseł pierwszego logowania,
3. instalowanie, aktualizowanie i konfigurowanie oprogramowania systemowego i aplikacyjnego oraz urządzeń, o ile czynności te nie są wykonywane przez upoważnionych przedstawicieli dostawcy systemu, na podstawie zawartej umowy,
4. instalowanie i kontrolowanie licencji oprogramowania antywirusowego na komputerach, na których przetwarzane są dane osobowe i aktualizowanie go w razie potrzeby,

5. reagowanie i rejestrowanie przypadków naruszenia bądź zagrożenia bezpieczeństwa danych osobowych przetwarzanych w systemie,
6. nadzorowanie tworzenia oraz przechowywania kopii zapasowych baz danych, zawierających dane osobowe,
7. przygotowywanie urządzeń, dysków i innych elektronicznych nośników informacji, zawierających dane osobowe, do likwidacji, przekazania innemu podmiotowi, konserwacji lub naprawy,
8. kompletowanie i nadzór nad przechowywaniem dokumentacji dotyczącej licencji oprogramowania,
9. powiadamianie ADO o miejscu przechowywania oraz metodzie i częstotliwości tworzenia kopii zapasowych zbiorów danych osobowych przetwarzanych w systemach,
10. wykonywanie bieżącej konserwacji i przeglądu systemu oraz uaktualnianie kont i uprawnień użytkowników,
11. dokonywanie bieżącej inwentaryzacji sprzętu i oprogramowania,
12. wykonywanie przeglądu systemów oraz nośników informacji służących do przetwarzania danych.

……..
Podpis Dyrektora

Załącznik nr 3
do Polityki Bezpieczeństwa Informacji
w ZSZ w Rawiczu

Wykaz zbiorów danych osobowych

Dane osobowe uczniów i rodziców (opiekunów prawnych):	
prowadzone w formie elektronicznej	**prowadzone w formie tradycyjnej (papierowej)**
SIO w formie papierowej wydruk	teczki uczniów
Nabór Optivum	dzienniki uczniów
e- dziennik Librus	księga uczniów
e-Sekretariat	ewidencja świadectw i legitymacji
Świadectwa Optivum	dziennik pedagoga
	arkusze ocen
	protokóły egzaminów
	ewidencja wydanych duplikatów świadectw (korespondencja rzeczowy wykaz akt B5)
	archiwum jednostki
	rejestr wypadków uczniów
	rejestr decyzji zwolnień lekarskich uczniów
	opinie i orzeczenia z Poradni Psychologiczno – Pedagogicznej i zaświadczenia lekarskie
	dane osobowe uczniów i ich rodzin w zakresie bezpieczeństwa i zdrowia oraz dydaktyczno- wychowawczo- opiekuńczej działalności szkoły
Dane osobowe pracowników:	
prowadzone w formie elektronicznej	**prowadzone w formie tradycyjnej (papierowej)**
SJO Bestia	archiwum jednostki
Płatnik	teczki osobowe pracowników
SIO w formie papierowej wydruk	rejestr wyjazdów służbowych (delegacje)
iPKO biznes	ewidencja zwolnień lekarskich pracowników
Kadry Optivum w formie papierowej wydruk	ewidencja wydanych upoważnień
Płace Optivum w formie papierowej wydruk	dane osobowe pracowników i ich rodzin związane z zatrudnieniem i płacami
Księgowość Optivum	dane osobowe pracowników i ich rodzin związane ze świadczeniami z ZFŚS
Inwentarz Optivum	dane osobowe emerytów związane ze świadczeniami z ZFŚS
Arkusz Organizacyjny Optivum w formie papierowej wydruk	praktykanci i stażyści
Plan lekcji Optivum	

Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych

Podstawa prawna:

1. Ustawa z dnia 29 sierpnia 1997r. o ochronie danych osobowych (Dz.U. z 2016r., poz. 922).
2. Rozporządzenie 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. 2004 nr 100 poz. 1024).

Rozdział I. Procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności.

1. Procedury nadawania w Szkole uprawnień do przetwarzania danych osobowych obejmują:
   a. podpisanie przez osobę, do której obowiązków należy przetwarzanie danych osobowych, oświadczenia o zachowaniu w tajemnicy danych osobowych oraz zasad ich przetwarzania, sposobów ich zabezpieczania, obejmującego także okres po ustaniu stosunku pracy, oraz o zapoznaniu się z:
      - Ustawą z dnia 29 sierpnia 1997r. o ochronie danych osobowych (Dz.U. z 2016r., poz. 922),
      - Rozporządzeniem 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. 2004 nr 100 poz. 1024),
      - *Polityką Bezpieczeństwa Informacji w Zespole Szkole Zawodowych im. Stefana Bobrowskiego w Rawiczu.*
   b. wydanie przez ADO upoważnienia do przetwarzania danych osobowych pracownikom administracji przetwarzającym dane oraz pracownikom pedagogicznym.
2. Kopie upoważnień, o których mowa w ust. 1 przechowuje się w aktach osobowych pracownika. Każde upoważnienie jest rejestrowane w rejestrze upoważnień (załącznik nr 10).
3. Upoważnienia, o których mowa w ust. 1, są imienne i udzielane w formie pisemnej na czas określony lub czas nieokreślony – do odwołania udzielonego upoważnienia.
4. Przyznanie uprawnień w zakresie dostępu do systemu informatycznego polega na wprowadzeniu do systemu przez ASI dla każdego użytkownika systemu unikalnego loginu i hasła pierwszego logowania.
5. Hasło pierwszego logowania w systemie ustanawia ASI. Każdy użytkownik systemu informatycznego ma obowiązek dokonać jego zmiany na indywidualne, co najmniej ośmioznakowe hasło, w skład którego muszą wchodzić duże i małe litery, cyfry oraz znaki specjalne.

6. Na terenie warsztatów szkolnych nauczyciel loguje się do e-dziennika za pomocą przeglądarki internetowej. Nie przetwarza się danych osobowych z użyciem sprzętu komputerowego w innej formie.

Rozdział II. Stosowane metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem.

1. Każdy z pracowników loguje się do systemu operacyjnego wykorzystując osobisty login i hasło. Login ma budowę: nazwisko.imię. Hasło składa się z co najmniej ośmiu znaków – liter małych i dużych, cyfr oraz znaków specjalnych. Każdy z pracowników ma obowiązek zmiany hasła nie rzadziej niż raz na 30 dni. Użytkownik, który zapomni hasło, zgłasza ten fakt administratorowi domeny, który resetuje hasło.

Rozdział III. Procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu.

1. Przy logowaniu do systemu przetwarzającego dane osobowe wprowadza się login oraz hasło dostępu.
2. Przy zakończeniu pracy związanej z przetwarzaniem danych pracownik wylogowuje się z systemu.

Rozdział IV. Procedury tworzenia kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania.

1. Kopie zapasowe tworzone są w następujący sposób:
    a. kopie baz danych tworzone są automatycznie, codziennie,
    b. kopie dokumentów użytkowników tworzone są automatycznie, raz w tygodniu,
    c. kopie systemów informatycznych tworzone są automatycznie, raz w tygodniu.

Rozdział V. Sposób, miejsce i okres przechowywania elektronicznych nośników informacji zawierających dane osobowe oraz kopii zapasowych.

1. Okres przechowywania kopii zapasowych wynosi nie mniej niż 3 lata.
2. Monitoring wizyjny nagrywany jest na dysk rejestratora. Dostęp do niego mają upoważnione przez ADO osoby.
3. Pracowników Zespołu Szkół Zawodowych w Rawiczu obowiązuje bezwzględny zakaz wynoszenia płyt lub innych nośników danych z danymi osobowymi poza teren siedziby jednostki, chyba że zgodę na taką czynność wyrazi dyrektor jednostki.
4. Nośniki danych oraz wydruki, które nie są przeznaczone do udostępnienia, przechowuje się w specjalnie zamykanych szafach, do których dostęp mają tylko osoby uprawnione.

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

1. Dopuszcza się możliwość przyłączenia sieci internetowej do systemu, w którym przetwarzane są dane osobowe pod następującymi warunkami:
    a. na każdym stanowisku komputerowym oraz serwerze musi być zainstalowane oprogramowanie antywirusowe,

b. każdy e-mail wpływający do jednostki musi być sprawdzony pod kątem występowania wirusów,
c. zabrania się używania nośników niewiadomego pochodzenia bez wcześniejszego sprawdzenia ich programem antywirusowym, którego dokonuje użytkownik zamierzający go użyć,
d. zabrania się pobierania z Internetu plików niewiadomego pochodzenia oraz odczytywania załączników poczty elektronicznej bez wcześniejszego sprawdzenia ich programem antywirusowym.

2. ASI kontroluje licencje programu antywirusowego na komputerach, na których przetwarzane są dane osobowe i aktualizuje go w razie potrzeby.
3. Na stanowiskach, na których przetwarzane są dane osobowe ekrany monitorów powinny być tak ustawione, aby osoby nieupoważnione nie miały dostępu do informacji na nich wyświetlanych.
4. Użytkownicy systemu są odpowiedzialni za nieudostępnianie stanowisk pracy osobom postronnym.
5. Kontroli podlega dostęp do pomieszczeń, w których znajduje się sprzęt komputerowy, w celu zabezpieczenia sprzętu oraz danych osobowych i oprogramowania przed ich wykorzystaniem lub zniszczeniem przez osoby trzecie. Pomieszczenia, w których znajduje się sprzęt komputerowy służący do przetwarzania danych osobowych wyposażone są w solidne zamki. Ostatni z pracowników, który opuszcza pomieszczenie ma obowiązek zamknąć drzwi na klucz.
6. Dopuszcza się, za zgodą dyrektora jednostki i wiedzą ABI, instalowanie programów do przetwarzania danych osobowych na komputerach przenośnych tzw. notebookach. Musi on jednak posiadać zainstalowane mechanizmy ochronne oraz kompleksowe oprogramowanie antywirusowe. Użytkownik takiego komputera musi dochować wszelkiej staranności, aby zapobiec kradzieży tego komputera przenośnego.
7. Urządzenia, dyski lub inne nośniki informacji przeznaczone do:
   a. likwidacji, pozbawia się danych poprzez formatowanie oraz fizyczne uszkodzenie uniemożliwiające ich odczytanie,
   b. przekazania, pozbawia się zapisu zawierającego dane osobowe,
   c. naprawy, pozbawia się zapisu danych osobowych lub naprawia pod nadzorem ASI.
8. Koperty z hasłami administratorów przechowywane są w gabinecie ABI, zamknięte w sejfie.
9. Brudnopisy oraz zbędne kopie dokumentów zawierających dane osobowe należy niszczyć niszczarką.

Rozdział VII. Procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych.

1. Nie rzadziej niż raz na pół roku ASI wykonuje przegląd systemów oraz nośników informacji służących do przetwarzania danych. Po przeglądzie ASI sporządza raport i przedstawia go ADO.
2. ASI wykonuje bieżące konserwacje systemów oraz nośników informacji służących do przetwarzania danych.
3. ASI uaktualnia konta i uprawnienia użytkowników.
4. ASI przygotowuje urządzenia, dyski i inne elektroniczne nośniki informacji, zawierające dane osobowe, do likwidacji, przekazania innemu podmiotowi, konserwacji lub naprawy.
5. Naprawa sprzętu komputerowego użytkowanego w systemie może odbywać się w szkole i dokonywać jej może jedynie ASI lub wyspecjalizowana firma informatyczna. Naprawa sprzętu komputerowego poza szkołą, o ile to możliwe powinna zostać poprzedzona wymontowaniem twardego dysku zawierającego dane osobowe.

Rozdział VIII. Zasady udostępniania danych.

1. Dane osobowe mogą być wydane jedynie na pisemny wniosek osoby, której dotyczą lub pisemny wniosek zainteresowanego i za zgodą ADO.
2. Z czynności przekazania danych sporządza się protokół przekazania danych osobowych (wzór stanowi załącznik nr 4).
3. ABI zobowiązany jest do prowadzenia ewidencji udostępniania danych osobowych (wzór stanowi załącznik nr 5).

Rozdział IX. Procedura postępowania w sytuacji naruszenia polityki bezpieczeństwa.

1. Każda osoba przetwarzająca dane osobowe, w przypadku podejrzenia naruszenia zabezpieczenia danych osobowych, zobowiązana jest niezwłocznie powiadomić o tym ADO, ABI lub ASI.
2. ABI w porozumieniu z ASI po otrzymaniu powiadomienia:
    a. sprawdza stan urządzeń wykorzystywanych do przetwarzania danych osobowych,
    b. sprawdza sposób działania programów (w tym obecność wirusów komputerowych),
    c. sprawdza zawartość zbioru danych osobowych,
    d. poddaje analizie metody pracy osób upoważnionych do przetwarzania danych osobowych.
3. W przypadku stwierdzenia naruszenia zabezpieczeń danych ABI w porozumieniu z ASI:
    a. podejmuje niezbędne działania mające na celu uniemożliwienie dalszego ich naruszenia (odłączenie wadliwych urządzeń, zablokowanie dostępu do sieci telekomunikacyjnej, programów oraz zbiorów danych itp.),
    b. w celu powstrzymania lub ograniczenia dostępu do danych osoby niepowołanej podejmuje odpowiednie kroki poprzez: fizyczne odłączenie urządzeń i segmentów sieci, które mogłyby umożliwić dostęp do bazy danych osoby nieupoważnionej, wylogowanie użytkownika podejrzewanego o naruszenie zabezpieczenia ochrony danych, zmianę hasła na konto administratora i użytkownika, poprzez które uzyskano nielegalny dostęp w celu uniknięcia ponownej próby włamania,
    c. zabezpiecza, utrwala wszelkie informacje i dokumenty mogące stanowić pomoc przy ustaleniu przyczyn naruszenia,
    d. niezwłocznie przywraca prawidłowy stan działania systemu,
    e. dokonuje analizy stanu zabezpieczeń wraz z oszacowaniem rozmiaru szkód powstałych na skutek naruszenia,
    f. sporządza szczegółowy raport zawierający w szczególności: datę i godzinę otrzymania informacji o naruszeniu, opis jego przebiegu, przyczyny oraz wnioski ze zdarzenia.
4. Raport, wraz z ewentualnymi załącznikami (kopie dowodów dokumentujących naruszenie) ABI przekazuje administratorowi danych osobowych.
5. ADO w porozumieniu z ABI oraz ASI podejmuje niezbędne działania w celu wyeliminowania naruszeń zabezpieczeń danych w przyszłości, a w szczególności:
    a. jeżeli przyczyną zdarzenia był stan techniczny urządzenia, sposób działania programu, uaktywnienie się wirusa komputerowego lub jakość komunikacji w sieci telekomunikacyjnej, niezwłocznie przeprowadza przeglądy oraz konserwacje urządzeń i programów, ustala źródło pochodzenia wirusa oraz wdraża skuteczniejsze zabezpieczenie antywirusowe, a w miarę potrzeby kontaktuje się z dostawcą usług telekomunikacyjnych,

b. jeżeli przyczyną zdarzenia były wadliwe metody pracy, błędy i zaniedbania osób zatrudnionych przy przetwarzaniu danych osobowych, przeprowadza dodatkowe kursy i szkolenia osób biorących udział przy przetwarzaniu danych, a wobec osób winnych zaniedbań wyciąga konsekwencje przewidziane prawem,
c. jeżeli przyczyną zdarzenia jest sprzeczny z prawem czyn lub zachodzi takie podejrzenie, zawiadamia organ ścigania.

Kto przetwarza dane osobowe lub umożliwia dostęp do nich osobom nieupoważnionym podlega przepisom karnym na podstawie art. 49 – art. 54 ustawy o ochronie danych osobowych.

Rawicz, dnia 31.08.2017r.

……
Podpis Dyrektora

Załącznik nr 4
do Polityki Bezpieczeństwa Informacji
w ZSZ w Rawiczu

Rawicz, dnia …….

PROTOKÓŁ
przekazania danych osobowych

Niniejszym potwierdzam odbiór danych osobowych

.....

.....

.....

.....

.....

.....

na podstawie wniosku złożonego dnia .....

....
(podpis ADO) (data i podpis odbierającego)

Załącznik nr 5
do Polityki Bezpieczeństwa Informacji
w ZSZ w Rawiczu

EWIDENCJA UDOSTĘPNIANIA DANYCH OSOBOWYCH

L.p.	Wnioskodawca	Data złożenia wniosku	Udostępnione dane	Data udostępnienia danych	Uwagi

Załącznik nr 6
do Polityki Bezpieczeństwa Informacji
w ZSZ w Rawiczu

..... Rawicz, dnia ……
(imię i nazwisko)

.....
(adres)

OŚWIADCZENIE

Oświadczam, że zapoznałem/łam się z następującymi dokumentami:

a. Ustawą z dnia 29 sierpnia 1997r. o ochronie danych osobowych (Dz.U. z 2016r., poz. 922),
b. Rozporządzeniem 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. 2004 nr 100 poz. 1024),
c. *Polityką Bezpieczeństwa Informacji w Zespole Szkole Zawodowych im. Stefana Bobrowskiego w Rawiczu* wraz z załącznikami.

Oświadczam, że zobowiązuję się do zachowania w tajemnicy danych osobowych, do których mam lub będę miał(a) dostęp, zasad ich przetwarzania i sposobów ich zabezpieczenia w związku z wykonywaniem przeze mnie pracy zarówno w trakcie trwania umowy jak i po jej wygaśnięciu lub rozwiązaniu.

.....
(data i podpis składającego oświadczenie)

Załącznik nr 7
do Polityki Bezpieczeństwa Informacji
w ZSZ w Rawiczu

Rawicz, dnia …….

Upoważnienie nr …….

Upoważniam Pana/Panią ……..... do przetwarzania danych osobowych w Zespole Szkół Zawodowych im. Stefana Bobrowskiego w Rawiczu obejmujących następujący zakres: **dane osobowe uczniów i rodziców (opiekunów prawnych), niezbędne do prowadzenia dokumentacji szkolnej oraz dla celów egzaminów.**

Informuję, że udostępnianie danych osobowych lub umożliwianie dostępu do nich osobie nieuprawnionej podlega karze grzywny, karze ograniczenia albo pozbawienia wolności do lat dwóch.
Podstawa prawna: art.51 ustawy z dnia z dnia 29 sierpnia 1997r. o ochronie danych osobowych (Dz.U. z 2016r., poz. 922).

Upoważnienie jest ważne od dnia ……. do dnia ……/ do odwołania

Identyfikator: .....

....
(data i podpis upoważnionego) (data i podpis ADO)

Załącznik nr 8
do Polityki Bezpieczeństwa Informacji
w ZSZ w Rawiczu

Rawicz, dnia …….

Upoważnienie nr …….

Upoważniam Pana/Panią ……..... do dostępu do **danych osobowych pracowników**, w zakresie dotyczącym przetwarzania danych zgodnie z zakresem Pana/Pani obowiązków i uprawnień.

Naruszenie obowiązków w zakresie ochrony danych osobowych może skutkować nałożeniem na pracownika kary porządkowej, a nawet rozwiązaniem umowy o pracę bez wypowiedzenia z powodu ciężkiego naruszenia obowiązków pracowniczych.

Podstawa prawna: art.51 ustawy z dnia z dnia 29 sierpnia 1997r. o ochronie danych osobowych (Dz.U. z 2016r., poz. 922).

Upoważnienie jest ważne od dnia ……. do dnia ……/ do odwołania

Identyfikator: .....

....
(data i podpis upoważnionego) (data i podpis ADO)

Załącznik nr 9
do Polityki Bezpieczeństwa Informacji
w ZSZ w Rawiczu

Rawicz, dnia …….

Upoważnienie nr …….

Upoważniam Pana/Panią ……..... do przetwarzania danych osobowych w Zespole Szkół Zawodowych im. Stefana Bobrowskiego w Rawiczu obejmujących następujący zakres: **dane osobowe uczniów i rodziców (opiekunów prawnych), niezbędne do prowadzenia dokumentacji szkolnej oraz dla celów egzaminów, dane osobowe pracowników**, w zakresie dotyczącym przetwarzania danych zgodnie z zakresem Pana/Pani obowiązków i uprawnień.

Naruszenie obowiązków w zakresie ochrony danych osobowych może skutkować nałożeniem na pracownika kary porządkowej, a nawet rozwiązaniem umowy o pracę bez wypowiedzenia z powodu ciężkiego naruszenia obowiązków pracowniczych.

Podstawa prawna: art.51 ustawy z dnia z dnia 29 sierpnia 1997r. o ochronie danych osobowych (Dz.U. z 2016r., poz. 922).

Upoważnienie jest ważne od dnia ……. do dnia ……/ do odwołania

Identyfikator: .....

....
(data i podpis upoważnionego) (data i podpis ADO)

Załącznik nr 10
do Polityki Bezpieczeństwa Informacji
w ZSZ w Rawiczu

REJESTR UPOWAŻNIEŃ

Numer upoważnienia	Imię i nazwisko osoby upoważnionej	Data nadania	Data ustania	Zakres upoważnienia	Podpis osoby upoważnionej

Załącznik nr 11
do Polityki Bezpieczeństwa Informacji
w ZSZ w Rawiczu

EWIDENCJA OSÓB UPOWAŻNIONYCH DO PRZETWARZANIA DANYCH OSOBOWYCH W ZESPOLE SZKÓŁ ZAWODOWYCH W RAWICZU

L.p.	Numer upoważnienia / pracownik dydaktyczny	Imię i nazwisko osoby upoważnionej	Identyfikator	Data nadania upoważnienia	Zakres upoważnienia

Załącznik nr 2
do Polityki Bezpieczeństwa Informacji
w ZSZ w Rawiczu

Regulamin
korzystania z Systemu LIBRUS Synergia
w ZSZ im. S. Bobrowskiego w Rawiczu w zakresie ochrony danych osobowych

ROZDZIAŁ I. Postanowienia ogólne

1) W szkole, za pośrednictwem strony https://synergia.librus.pl funkcjonuje elektroniczny dziennik. Usługi związane z dziennikiem dostarczane są przez firmę zewnętrzną, współpracującą ze szkołą. Podstawą działania dziennika elektronicznego jest umowa podpisana przez dyrektora szkoły i uprawnionego przedstawiciela firmy dostarczającej oraz obsługującej system dziennika elektronicznego.
2) Administratorem danych osobowych zamieszczonych w Systemie LIBRUS Synergia jest Zespół Szkół Zawodowych im. S. Bobrowskiego w Rawiczu.
3) Za niezawodność działania systemu, ochronę danych osobowych umieszczonych na serwerach oraz tworzenie kopii bezpieczeństwa odpowiada firma nadzorująca pracę Systemu LIBRUS Synergia, pracownicy szkoły, którzy mają bezpośredni dostęp do przeglądania i edycji danych oraz rodzice (prawni opiekunowie) i uczniowie w zakresie udostępnionych im danych. Szczegółową odpowiedzialność wszystkich stron reguluje zawarta pomiędzy stronami umowa oraz przepisy obowiązującego w Polsce prawa.

ROZDZIAŁ II. Konta w dzienniku elektronicznym

1) Każdy użytkownik Systemu LIBRUS Synergia (szkolny administrator dziennika elektronicznego, dyrektor szkoły, wychowawca klasy, nauczyciel, pedagog, pracownik biblioteki szkolnej, pracownik sekretariatu, rodzic, uczeń) posiada własne konto dostępowe do systemu dziennika elektronicznego, za które osobiście odpowiada. Konstrukcja systemu, ze względu na bezpieczeństwo danych w systemie, wymusza na użytkowniku okresową zmianę hasła konta. Hasło dostarczone przez administratora służy tylko do pierwszego zalogowania. Hasło wprowadzone przez użytkownika powinno się składać co najmniej z 8 znaków i być kombinacją liter (dużych i małych) i cyfr.
2) Każdy użytkownik jest zobowiązany stosować się do zasad bezpieczeństwa w posługiwaniu się loginem i hasłem do systemu, które poznał na szkoleniu (nauczyciele na Radzie Pedagogicznej lub indywidualnym szkoleniu, rodzice na zebraniu z rodzicami, uczniowie na zajęciach), w szczególności do utrzymywania w tajemnicy hasła umożliwiającego dostęp do zasobów Systemu LIBRUS Synergia, również po upływie jego ważności.
3) W przypadku utraty hasła lub podejrzenia, że zostało odczytane/wykradzione przez osobę nieuprawnioną, użytkownik zobowiązany jest do niezwłocznego, osobistego poinformowania o tym fakcie szkolnego administratora dziennika elektronicznego.
4) Użytkownik, po zalogowaniu na swoim koncie, zobowiązany jest do sprawdzenia wiarygodności informacji odnośnie:
   - ✓ ostatniego udanego logowania
   - ✓ ostatniego nieudanego logowania.

   W razie stwierdzenia nieścisłości powinien osobiście o tym fakcie powiadomić szkolnego administratora dziennika elektronicznego.

ROZDZIAŁ III. Przekazywanie informacji w dzienniku elektronicznym

1) Użytkownikowi systemu dziennika elektronicznego nie wolno umożliwiać korzystania z zasobów osobom trzecim.
2) Pracownikom szkoły nie wolno udzielać osobom trzecim żadnych informacji zawartych w systemie dziennika elektronicznego. Wszystkie dane osobowe uczniów i ich rodziców są poufne.
3) Pracownikom szkoły nie wolno przekazywać żadnych informacji odnośnie loginów i haseł dostępowych do konta rodzicom i uczniom drogą telefoniczną oraz z wykorzystaniem poczty elektronicznej.
4) Rodzicowi przysługuje prawo wglądu do informacji o swoim dziecku, ale tylko w szkole. Jeśli zaistnieje taki przypadek, to (w asyście dyrektora, wychowawcy, nauczyciela przedmiotowego lub pedagoga) rodzicowi udostępnia się za pomocą komputera wszystkie informacje dotyczące jego dziecka z zachowaniem poufności danych osobowych innych uczniów.
5) Szkoła, na życzenie rodzica (prawnego opiekuna), może (z zachowaniem poufności danych osobowych) udostępnić rodzicowi (prawnemu opiekunowi) papierowe wydruki, które są przewidziane dla konta rodzica (prawnego opiekuna) w systemie dziennika elektronicznego.

ROZDZIAŁ IV. Dyrektor szkoły

1) Dyrektor szkoły jest zobowiązany dochowywać tajemnicy odnośnie postanowień zawartych w umowie dotyczącej wprowadzenia w szkole Systemu LIBRUS Synergia, mogących narazić działanie systemu informatycznego na utratę bezpieczeństwa.
2) Dyrektor szkoły dokonuje podziału zadań i obowiązków związanych z organizacją ochrony danych osobowych, w szczególności wyznacza administratora szkolnego dziennika elektronicznego oraz drugą osobę, która może w zastępstwie pełnić rolę administratora.
3) Dyrektor szkoły zobowiązany jest do stosowania podpisu elektronicznego archiwów dziennika elektronicznego za cały poprzedni rok szkolny. Archiwa wyżej wymienionych dzienników przechowywane są w szkolnym sejfie.

ROZDZIAŁ V. Szkolny administrator dziennika elektronicznego

1) Informacje o nowo utworzonych kontach (login, hasło) szkolny administrator dziennika elektronicznego ma obowiązek przekazać bezpośrednio ich właścicielom lub (w przypadku rodziców/opiekunów i uczniów) wychowawcom klas. W razie nieznajomości danej osoby, szkolny administrator dziennika elektronicznego ma obowiązek sprawdzić legitymację szkolną lub dowód osobisty celem weryfikacji tożsamości osoby.
2) Na prośbę użytkownika dziennika elektronicznego szkolny administrator przypomina loginy, generuje nowe hasła i przekazuje je, z zachowaniem zasad poufności, bezpośrednio zainteresowanym osobom lub (w przypadku rodziców/opiekunów i uczniów) wychowawcom klas.
3) Nie rzadziej niż raz na 3 miesiące szkolny administrator dziennika elektronicznego generuje dzienniki wszystkich oddziałów szkolnych jako kopie bezpieczeństwa. Przechowuje je na płycie CD w szkolnym sejfie. Po zakończeniu roku szkolnego wyżej wymienione kopie bezpieczeństwa zostają bezpowrotnie usunięte przez administratora e-dziennika.
4) Jeżeli nastąpi zablokowanie konta nauczyciela, szkolny administrator dziennika elektronicznego powinien:
   - ✓ skontaktować się osobiście z nauczycielem i wyjaśnić powód blokady,

- ✓ w razie zaistnienia próby naruszenia bezpieczeństwa powiadomić firmę nadzorującą poprzez wysłanie informacji do Superadministratora,
- ✓ sprawdzić wraz z nauczycielem aktualną zawartość jego konta z tworzonymi kopiami bezpieczeństwa i jeśli jest taka potrzeba przywrócić je do prawidłowej zawartości,
- ✓ wygenerować i przekazać nowe jednorazowe hasło dla nauczyciela.

5) Szkolny administrator dziennika elektronicznego, w pierwszym tygodniu nowego roku szkolnego, generuje dzienniki poszczególnych klas za cały poprzedni rok szkolny i przekazuje je dyrektorowi szkoły.

ROZDZIAŁ VI. Wychowawca klasy

1) Na pierwszym zebraniu z rodzicami wychowawca klasy ma obowiązek osobiście rozdać rodzicom (prawnym opiekunom) loginy i hasła do ich kont oraz kont ich dzieci. Podczas godziny do dyspozycji wychowawcy, wychowawca przekazuje loginy i hasła do kont uczniowskich swoim wychowankom.
2) Wychowawca informuje rodziców (prawnych opiekunów) i uczniów o zasadach bezpiecznego korzystania z konta dziennika elektronicznego, ze szczególnym uwzględnieniem zasad ochrony danych osobowych użytkownika konta.
3) Fakt otrzymania loginów i haseł oraz zapoznania się z zasadami bezpiecznego korzystania z konta dziennika elektronicznego, rodzic (prawny opiekun) potwierdza podpisem na dokumencie (załącznik nr 15) w obecności wychowawcy klasy. Wymieniony dokument wychowawca przechowuje w teczce wychowawcy.
4) Na prośbę rodzica (prawnego opiekuna) lub ucznia administrator przypomina użytkownikowi jego login i generuje nowe hasło po czym przekazuje je wychowawcy klasy. Wychowawca przekazuje użytkownikowi wyżej wymienione dane do konta z zachowaniem następujących zasad:
   - ✓ rodzic otrzymuje login i hasło dla konta rodzica i ucznia
   - ✓ uczeń otrzymuje login i hasło dla konta ucznia

ROZDZIAŁ VII. Nauczyciel

1) Nauczyciel jest osobiście odpowiedzialny za swoje konto i zobowiązany do ochrony danych osobowych umieszczonych w systemie dziennika elektronicznego, a w szczególności:
   - ✓ chroni dane dostępowe do swojego konta (login, hasło) przed osobami trzecimi,
   - ✓ po zalogowaniu się do swojego konta sprawdza informację o ostatnim udanym i nieudanym logowaniu – w razie potrzeby niezwłocznie informuje o zagrożeniu administratora szkolnego dziennika elektronicznego,
   - ✓ nie udostępnia uczniom komputera, który służy w pracowni do korzystania z dziennika elektronicznego,
   - ✓ nie pozostawia bez nadzoru uczniów w pracowni z komputerem służącym do dostępu do dziennika elektronicznego,
   - ✓ jeżeli do dostępu do dziennika elektronicznego korzysta z laptopa, nie udostępnia go osobom trzecim,
   - ✓ dba o to, by poufne dane prezentowane na monitorze komputera nie były widoczne dla osób trzecich,
   - ✓ po zakończeniu pracy z dziennikiem elektronicznym wylogowuje się z konta,
2) Nauczyciel nie udostępnia osobom nieupoważnionym, zgromadzonych na zewnętrznych nośnikach lub wydrukach, wygenerowanych dzienników, plików świadectw szkolnych, plików generowanych w dzienniku elektronicznym statystyk itp.

ROZDZIAŁ VIII. Sekretariat

1) Za obsługę konta „sekretariat” odpowiedzialna jest wyznaczona przez dyrektora szkoły osoba, która na stałe pracuje w sekretariacie szkoły.
2) W przypadku zaistnienia takiej potrzeby, na polecenie dyrektora szkoły, szkolny administrator dziennika elektronicznego przydziela osobie pracującej w sekretariacie konto z uprawnieniami administratora.
3) Po skreśleniu ucznia z listy uczniów, pracownik sekretariatu szkoły drukuje jego kartotekę i umieszcza w arkuszu ocen.
4) Wszelkie informacje zaczerpnięte z dziennika elektronicznego, dotyczące ucznia, pracownik sekretariatu może przekazać zainteresowanemu lub jego rodzicowi wyłącznie po okazaniu przez niego legitymacji szkolnej lub dokumentu tożsamości.

ROZDZIAŁ IX. Rodzice (prawni opiekunowie)

1) Rodzice (prawni opiekunowie) mają w systemie dziennika elektronicznego swoje niezależne konto, zapewniające podgląd wyników w nauce i frekwencji ucznia na zajęciach szkolnych oraz dające możliwość komunikowania się z nauczycielami w sposób zapewniający ochronę danych osobowych innych uczniów.
2) Rodzic osobiście odpowiada za swoje konto w dzienniku elektronicznym szkoły i ma obowiązek nieudostępniania go swojemu dziecku ani innym nieupoważnionym osobom.

ROZDZIAŁ X. Uczeń

1) Uczeń ma w systemie dziennika elektronicznego swoje niezależne konto, umożliwiające podgląd swoich wyników w nauce i frekwencji, zapewniające ochronę danych osobowych innych uczniów.
2) Uczeń osobiście odpowiada za swoje konto w dzienniku elektronicznym szkoły i ma obowiązek nieudostępniania go innym, nieupoważnionym osobom.

ROZDZIAŁ XI. Postanowienia końcowe

1) Wszystkie poufne dokumenty i materiały utworzone na podstawie danych z dziennika elektronicznego, które nie będą potrzebne, należy zniszczyć.
2) Wszystkie zeskanowane i przesłane do bazy danych karty powinny być przechowywane w szkole do końca tygodnia, a następnie zniszczone z wykorzystaniem niszczarki.
3) Osoby z zewnątrz (serwisanci, osoby odbywające praktykę studencką, pracownicy urzędów państwowych dokonujących kontroli itp.), jeśli jest to wymagane treścią dokumentów i stanem urządzeń do których mają dostęp, zobowiązują się do poszanowania i zachowania tajemnicy wynikającej z ustawy o ochronie danych osobowych, potwierdzając to własnoręcznym podpisem na odpowiednim dokumencie (załącznik nr 13).
4) W razie kontroli z zewnątrz odpowiedniego organu uprawnionego do kontrolowania dokumentacji szkolnej, na polecenie dyrektora szkoły, na czas kontroli, szkolny administrator dziennika elektronicznego udostępnia wyznaczonej do tego celu osobie konto w dzienniku elektronicznym dające możliwość sprawdzenia prawidłowego prowadzenia przez nauczycieli dokumentacji bez możliwości dokonywania w dzienniku elektronicznym jakichkolwiek zmian.

……
Podpis Dyrektora

Załącznik nr 12
do Polityki Bezpieczeństwa Informacji
w ZSZ w Rawiczu

Potwierdzenie otrzymania dostępu do kont rodzica/opiekuna i ucznia/uczennicy oraz zapoznania się z zasadami funkcjonowania dziennika elektronicznego.

Potwierdzam otrzymanie dostępu (loginów i haseł) do swoich kont (rodzica/prawnego opiekuna oraz ucznia/uczennicy) oraz zapoznanie mnie z zasadami funkcjonowania dziennika elektronicznego w Zespole Szkół Zawodowych im. S. Bobrowskiego w Rawiczu .

Klasa: ……..…….
Rok szkolny: ……...…..

Rodzic musi podpisać się czytelnie, pełnym imieniem i nazwiskiem, gdyż podpis ten będzie traktowany jako wzór podpisu rodzica/opiekuna dziecka.

Lp.	Imię i nazwisko ucznia/uczennicy	Imię i nazwisko rodzica/opiekuna	Czytelny podpis rodzica lub prawnego opiekuna
1.			
2.			
3.			
4.			
5.			
6.			
7.			
8.			
9.			
10.			
11.			

Załącznik nr 13
do Polityki Bezpieczeństwa Informacji
w ZSZ w Rawiczu

Deklaracja dochowania tajemnicy danych z dziennika elektronicznego, wynikającej z Ustawy o Ochronie Danych Osobowych przez osoby nie zatrudnione w szkole.

Art. 23 p.1 ust. 2 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych.

Lista osób nie zatrudnionych w szkole, które zadeklarowały przestrzeganie tajemnicy danych z dziennika elektronicznego w Zespole Szkół Zawodowych im. S. Bobrowskiego w Rawiczu**.**

LP.	IMIĘ I NAZWISKO (komu udzielany jest dostęp do danych)	CZYTELNY PODPIS (komu udzielany jest dostęp do danych)	DATA	TERMIN DOSTĘPU DO DANYCH	PODPIS DYREKTORA SZKOY
1.					
2.					
3.					
4.					
5.					
6.					
7.					
8.					