Zarządzenie nr 206/2015/2016
Dyrektora Szkoły Podstawowej z Oddziałami Integracyjnymi nr 1 im. Janusza Korczaka w Rybniku
z dnia 17 marca 2016 roku

w sprawie ustanowienia, wdrożenia, eksploatacji, monitorowania, przeglądu, utrzymania i doskonalenia systemu zarządzania bezpieczeństwem informacji oraz wprowadzenia „Polityki bezpieczeństwa" i „Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych"

Działając na podstawie:

- art. 36 ust. 2 ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych,
- § 4 i § 5 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 roku w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych,
- § 20 ust. 1 rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 roku w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych

zarządzam, co następuje:

§ 1.

1. Ustanawia się system zarządzania bezpieczeństwem informacji w Szkole Podstawowej z Oddziałami Integracyjnymi nr 1 im. Janusza Korczaka w Rybniku, zwaną dalej „Szkołą".
2. Informacje to aktywa, które podobnie jak inne ważne aktywa są niezbędne dla prawidłowego funkcjonowania Szkoły i z tego powodu podlegają ochronie.
3. Informacja przybiera różne formy – może być wydrukowana lub zapisana na papierze, przechowywana elektronicznie, przesyłana pocztą i za pomocą nośników elektronicznych lub wypowiadana w rozmowie.
4. Bezpieczeństwo informacji oznacza ochronę informacji przed zagrożeniami w celu zapewnienia ciągłości działania, efektywnego wykorzystania informacji i minimalizacji ryzyka.

§ 2.

Zarządzanie bezpieczeństwem informacji jest realizowane przez zapewnienie przez Dyrektora warunków umożliwiających wykonanie i egzekwowanie następujących działań:

1) zapewnienia aktualizacji regulacji wewnętrznych w zakresie dotyczącym zmieniającego się otoczenia,

2) utrzymywania aktualności inwentaryzacji środków przetwarzania informacji obejmującej ich rodzaj i konfigurację,
3) przeprowadzania okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji oraz podejmowania działań minimalizujących to ryzyko, stosownie do wyników przeprowadzonej analizy,
4) podejmowania działań zapewniających, że osoby zaangażowane w proces przetwarzania informacji posiadają stosowne uprawnienia i uczestniczą w tym procesie w stopniu adekwatnym do realizowanych przez nie zadań oraz obowiązków mających na celu zapewnienie bezpieczeństwa informacji, a w razie konieczności bezzwłocznej zmiany tych uprawnień,
5) zapewnienia szkolenia osób zaangażowanych w proces przetwarzania informacji ze szczególnym uwzględnieniem takich zagadnień, jak:
   a) zagrożenia bezpieczeństwa informacji,
   b) skutki naruszenia zasad bezpieczeństwa informacji, w tym odpowiedzialność prawna,
   c) stosowanie środków zapewniających bezpieczeństwo informacji, w tym minimalizujących ryzyko błędów ludzkich,
6) zapewnienia ochrony przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami, przez:
   a) monitorowanie dostępu do informacji,
   b) czynności zmierzające do wykrycia nieautoryzowanych działań związanych z przetwarzaniem informacji,
   c) zapewnienie środków uniemożliwiających nieautoryzowany dostęp na poziomie systemów operacyjnych, usług sieciowych i aplikacji,
7) ustanowienia podstawowych zasad gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość,
8) zabezpieczenia informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikację, usunięcie lub zniszczenie,
9) zawierania w umowach serwisowych podpisanych z wykonawcami zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji,
10) ustalenia zasad postępowania z informacjami, zapewniających minimalizację wystąpienia ryzyka kradzieży informacji i środków przetwarzania informacji, w tym urządzeń mobilnych,
11) zapewnienia odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych, polegającego w szczególności na:
   a) dbałości o aktualizację oprogramowania,
   b) minimalizowaniu ryzyka utraty informacji w wyniku awarii,
   c) ochronie przed błędami, utratą, nieuprawnioną modyfikacją,
   d) stosowaniu mechanizmów kryptograficznych w sposób adekwatny do zagrożeń lub wymogów przepisów prawa,
   e) zapewnieniu bezpieczeństwa plików systemowych,

f) redukcji ryzyk wynikających z wykorzystania opublikowanych podatności technicznych systemów teleinformatycznych,
g) niezwłocznym podejmowaniu działań po dostrzeżeniu nieujawnionych podatności systemów teleinformatycznych na możliwość naruszenia bezpieczeństwa,
h) kontroli zgodności systemów teleinformatycznych z odpowiednimi normami i politykami bezpieczeństwa,

12) bezzwłocznego zgłaszania incydentów związanych z bezpieczeństwem informacji w określony i z góry ustalony sposób, umożliwiający szybkie podjęcie działań korygujących,
13) zapewnienia okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji, nie rzadziej niż raz w roku.

§ 3.

1. Celem systemu zarządzania bezpieczeństwem informacji jest zapewnienie poufności, dostępności i integralności informacji.
2. Zapewnienie poufności oznacza zabezpieczenie informacji przed dostępem nieuprawnionych osób, podmiotów lub procesów.
3. Zapewnienie dostępności oznacza możliwość wykorzystania informacji w dowolnym momencie przez uprawnioną osobę.
4. Zapewnienie integralności oznacza zabezpieczenie informacji przed nieuprawnioną modyfikacją.

§ 4.

1. Zarządzanie bezpieczeństwem informacji wiąże się z zapewnieniem niezaprzeczalności odbioru i nadania informacji oraz rozliczalności działań.
2. Niezaprzeczalność odbioru oznacza zdolność systemu teleinformatycznego do udowodnienia, że adresat informacji otrzymał ją w określonym miejscu i czasie.
3. Niezaprzeczalność nadania oznacza zdolność systemu teleinformatycznego do udowodnienia, że nadawca informacji faktycznie ją nadał lub wprowadził do systemu teleinformatycznego w określonym miejscu i czasie.
4. Rozliczalność działań oznacza zapewnienie, że wszystkie działania istotne dla przetwarzania informacji zostały zarejestrowane w systemie teleinformatycznym i możliwym jest zidentyfikowanie użytkownika, który działania wykonał.

§ 5.

1. System zarządzania bezpieczeństwem informacji został zaprojektowany tak, aby zapewnić adekwatne i proporcjonalne zabezpieczenia, które odpowiednio chronią informacje, oraz uzyskać zaufanie zainteresowanych stron.

2. [redacted]	*dane niepodlegające udostępnianiu – art. 5 ustawy z dnia 6*	[redacted]

września 2001 roku
o dostępie do informacji
publicznej

§ 6.

1. System zarządzania bezpieczeństwem informacji swoim zakresem obejmuje całość funkcjonowania Szkoły i wszystkich pracowników Szkoły.
2. Minimalnym wymaganiem dotyczącym zarządzania bezpieczeństwem informacji jest udział w nim wszystkich pracowników Szkoły.

§ 7.

System zarządzania bezpieczeństwem informacji wdraża się poprzez procedury i zabezpieczenia wspomagające w zakresie:

1) organizacji bezpieczeństwa informacji,
2) zarządzania aktywami,
3) bezpieczeństwa zasobów ludzkich,
4) bezpieczeństwa fizycznego i środowiskowego,
5) zarządzania systemami i sieciami,
6) kontroli dostępu,
7) pozyskiwania, rozwoju i utrzymania systemów teleinformatycznych,
8) zarządzania incydentami związanymi z bezpieczeństwem informacji,
9) zarządzania ciągłością działania,
10) zapewnienia zgodności.

§ 8.

Wdrażanie bezpieczeństwa informacji w Szkole inicjuje, koordynuje i kontroluje Dyrektor.

§ 9.

1. W Szkole wyodrębnia się trzy grupy informacji:
   1) dane osobowe,
   2) arkusze egzaminacyjne Okręgowej Komisji Egzaminacyjnej,
   3) informacje niebędące danymi osobowymi lub arkuszami egzaminacyjnymi Okręgowej Komisji Egzaminacyjnej.
2. Poziom ochrony informacji szacuje się poprzez analizę poufności, integralności i dostępności dla rozważanej grupy informacji i przyjmuje się, że:
   1) dane osobowe i arkusze egzaminacyjne Okręgowej Komisji Egzaminacyjnej są informacjami poufnymi, chronionymi przed dostępem nieuprawnionych osób, dostępnymi w sposób nieprzerwany, chronionymi przed nieuprawnioną modyfikacją,
   2) informacje niebędące danymi osobowymi lub arkuszami egzaminacyjnymi Okręgowej Komisji Egzaminacyjnej są informacjami ogólnodostępnymi lub dostępnymi na wniosek, w sposób nieprzerwany, chronionymi przed nieuprawnioną modyfikacją.

§ 10.

Dla informacji przetwarzanych w Szkole nie stosuje się etykiet klasyfikacyjnych ani elektronicznych środków znakowania.

§ 11.

1. Informacje przed upublicznieniem w formie Biuletynu Informacji Publicznej podlegają akceptacji Dyrektora.
2. Informacje już upublicznione podlegają sprawdzeniu pod kątem ich nieuprawnionej modyfikacji. Sprawdzenia dokonuje Dyrektor lub wskazany przez Dyrektora pracownik.
3. W Szkole nie wykorzystuje się systemów publikujących dane w postaci elektronicznej, które umożliwiają sprzężenie zwrotne i bezpośrednie wprowadzanie danych.

§ 12.

1. W celu zapewnienia ochrony przed nieautoryzowanym dostępem fizycznym, uszkodzeniami lub zakłóceniami w Szkole oraz w odniesieniu do informacji wyznacza się obszar bezpieczny.

2.	*dane niepodlegające udostępnianiu – art. 5 ustawy z dnia 6 września 2001 roku o dostępie do informacji publicznej*	
3.	*dane niepodlegające udostępnianiu – art. 5 ustawy z dnia 6 września 2001 roku o dostępie do informacji publicznej*	

§ 13.

1.	*dane niepodlegające udostępnianiu – art. 5 ustawy z dnia 6 września 2001 roku o dostępie do informacji publicznej*	
2.	*dane niepodlegające udostępnianiu – art. 5 ustawy z dnia 6 września 2001 roku o dostępie do informacji*	

	publicznej	
3.	*dane niepodlegające udostępnianiu – art. 5 ustawy z dnia 6 września 2001 roku o dostępie do informacji publicznej*	
4.	*dane niepodlegające udostępnianiu – art. 5 ustawy z dnia 6 września 2001 roku o dostępie do informacji publicznej*	

5. Drzwi i okna pozostawione bez dozoru są zamykane.
6. Korzystanie w obszarze bezpiecznym z urządzeń fotograficznych, wideo, audio lub innych urządzeń nagrywających, w tym kamer w urządzeniach przenośnych bez zgody Dyrektora jest zabronione.
7. Wykonywanie w obszarze bezpiecznym przez wykonawcę lub użytkownika reprezentującego stronę trzecią pracy bez nadzoru jest zabronione.

§ 14.

1. W Szkole utrzymywana jest aktualność inwentaryzacji środków przetwarzania informacji w formie spisu środków przetwarzania informacji, którego wzór stanowi załącznik nr 1 do zarządzenia.
2. Przez środki przetwarzania informacji rozumie się komputery stacjonarne i przenośne, drukarki, kopiarki, skanery, serwery, faksy, oprogramowanie oraz inne urządzenia służące do przetwarzania informacji, z wyłączeniem pomocy dydaktycznych.
3. Aktualność inwentaryzacji środków przetwarzania informacji zapewnia informatyk.
4. Przez informatyka należy rozumieć pracownika Szkoły, wykonawcę lub użytkownika reprezentującego stronę trzecią, który czuwa nad sprawnym i ciągłym działaniem systemów teleinformatycznych.

§ 15.

Korzystanie z prywatnych środków przetwarzania informacji do przetwarzania informacji w Szkole jest zabronione.

§ 16.

Nowe środki przetwarzania informacji, które mają być użytkowane w Szkole podlegają autoryzacji na zasadach określonych w „Procedurze autoryzacji nowych środków przetwarzania informacji”, która stanowi załącznik nr 2 do zarządzenia.

§ 17.

Oprogramowanie należy pozyskiwać w sposób zapewniający, że prawa autorskie nie są naruszane.

§ 18.

1. Poszczególne środki przetwarzania informacji mogą zostać powierzone z obowiązkiem zwrotu lub do wyliczenia się.
2. Powierzenie środka przetwarzania informacji z obowiązkiem zwrotu lub do wyliczenia się następuje w drodze odrębnego powierzenia mienia i jest ujmowane w ewidencji powierzonego mienia do zwrotu lub do wyliczenia się. Wzór powierzenia mienia stanowi załącznik nr 3 do zarządzenia, a wzór ewidencji powierzonego mienia do zwrotu lub do wyliczenia się stanowi załącznik nr 4 do zarządzenia.
3. Każdy pracownik ponosi odpowiedzialność za zniszczone środki przetwarzania informacji powstałe wskutek niewykonania lub nienależytego wykonania obowiązków na zasadach określonych w ustawie z dnia 26 czerwca 1974 roku Kodeks pracy.

§ 19.

[redacted]	*dane niepodlegające udostępnianiu – art. 5 ustawy z dnia 6 września 2001 roku o dostępie do informacji publicznej*	[redacted]

§ 20.

Dokumenty, które określają lokalizacje środków przetwarzania danych osobowych nie są publicznie dostępne.

§ 21.

[redacted]	*dane niepodlegające udostępnianiu – art. 5 ustawy z dnia 6 września 2001 roku o dostępie do informacji publicznej*	[redacted]

§ 22.

1. W Szkole obowiązuje zakaz wynoszenia komputerów i nośników służących do przetwarzania informacji bez wcześniejszej zgody Dyrektora. Zgoda może być wydana ustnie, ale nie może być domniemana lub dorozumiana – musi być wyrażona wprost.

2. Dyrektor może określić i sprawdzić czas zwrotu wynoszonych komputerów i nośników służących do przetwarzania informacji. Niezależnie od tego, Dyrektor lub wyznaczony przez Dyrektora pracownik może przeprowadzić kontrolę w celu wykrycia komputerów i nośników służących do przetwarzania informacji wynoszonych bez zezwolenia.

§ 23.

W przypadku przekazania komputerów służących do przetwarzania informacji do ponownego użycia, kasowane są z nich informacje, do których przyszły użytkownik nie ma dostępu, a w przypadku zbycia lub zniszczenia – kasowane są wszystkie informacje.

§ 24.

Dostęp do informacji i środków przetwarzania informacji jest kontrolowany.

§ 25.

1. Dostęp do informacji posiada każdy pracownik Szkoły w myśl zasady wiedzy koniecznej.
2. Dostęp do informacji wynika z zakresu czynności lub dokumentu równoważnego.

§ 26.

Dostęp wykonawcy lub użytkownika reprezentującego stronę trzecią do środków przetwarzania informacji należących do Szkoły i do przetwarzania informacji jest kontrolowany.

§ 27.

1. Przed przyznaniem wykonawcy lub użytkownikowi reprezentującemu stronę trzecią dostępu do środków przetwarzania informacji lub do informacji szacuje się ryzyko.

2. [redacted]	*dane niepodlegające udostępnianiu – art. 5 ustawy z dnia 6 września 2001 roku o dostępie do informacji publicznej*	[redacted]

§ 28.

Dostęp do środków przetwarzania informacji wymaga pisemnej zgody Dyrektora, której wzór stanowi załącznik nr 5 do zarządzenia.

§ 29.

Przetwarzanie danych osobowych wymaga pisemnego upoważnienia Dyrektora.

§ 30.

Zasady przyznawania praw dostępu do przetwarzania danych osobowych, do pracy w wykorzystaniem środków przetwarzania informacji oraz stosowane metody i środki uwierzytelniania dostępu zostały określone w „Procedurze kontroli dostępu", która stanowi załącznik nr 6 do zarządzenia.

§ 31.

Należy dążyć do standaryzacji profili praw dostępu dla użytkowników na typowych stanowiskach.

§ 32.

Wymagania dotyczące ochrony fizycznej, kontroli dostępu, wykonywania kopii zapasowych i ochrony przed działaniem złośliwego oprogramowania przy przetwarzaniu mobilnym informacji poza siedzibą Szkoły określa „Procedura przetwarzania mobilnego", która stanowi załącznik nr 7 do zarządzenia.

§ 33.

1. Użytkownik ponosi odpowiedzialność za utrzymanie skutecznej kontroli dostępu, szczególnie w odniesieniu do haseł dostępu i zabezpieczenia użytkowanych przez siebie środków przetwarzania informacji.
2. Nieużywane w danym momencie komputery należy zabezpieczyć przed nieupoważnionym dostępem poprzez blokadę klawiatury lub w inny równoważny sposób.

§ 34.

1. W celu redukowania ryzyka nieautoryzowanego dostępu lub uszkodzenia dokumentów papierowych i środków przetwarzania informacji wprowadza się politykę czystego biurka i politykę czystego ekranu.
2. Polityka czystego biurka polega na:
   1) przechowywaniu pod zamknięciem nieużywanych informacji umieszczonych na nośnikach elektronicznych lub w postaci papierowej, szczególnie jeśli pomieszczenie biurowe jest opuszczane,
   2) ochronie punktów przyjmowania i wysyłania korespondencji oraz nienadzorowanych faksów,
   3) zakazie korzystania z kopiarek i technik kopiowania (skanerów, aparatów cyfrowych) bez zgody na pracę z wykorzystaniem środków przetwarzania informacji, o której mowa w § 28 zarządzenia.
3. Polityka czystego ekranu polega na:
   1) ustawieniu ekranu monitora komputera w sposób uniemożliwiający osobie nieuprawnionej dostęp do informacji wyświetlanych na ekranie monitora,

2) zamykaniu aktywnych sesji po zakończeniu pracy, chyba, że są one zabezpieczane przez odpowiedni mechanizm blokujący – wygaszacz ekranu chroniony hasłem dostępu,
3) zablokowaniu komputera lub wylogowaniu się przy każdorazowym opuszczaniu stanowiska komputerowego w trakcie pracy.

§ 35.

Z drukarek i kopiarek należy niezwłocznie usuwać dokumenty zawierające dane osobowe.

§ 36.

	dane niepodlegające udostępnianiu – art. 5 ustawy z dnia 6 września 2001 roku o dostępie do informacji publicznej	

§ 37.

Praca z wykorzystaniem komputera służącego do przetwarzania informacji odbywa się w oparciu o:

1) „Procedurę rozpoczęcia, zawieszenia i zakończenia pracy na komputerze", która stanowi załącznik nr 8 do zarządzenia,
2) „Procedurę wykonywania przeglądów, konserwacji i napraw komputerów, nośników i oprogramowania służących do przetwarzania informacji", która stanowi załącznik nr 9 do zarządzenia,
3) „Procedurę tworzenia kopii zapasowych", która stanowi załącznik nr 10 do zarządzenia,
4) „Procedurę korzystania z sieci Internet", która stanowi załącznik nr 11 do zarządzenia,
5) „Procedurę ochrony przed złośliwym oprogramowaniem", która stanowi załącznik nr 12 do zarządzenia.

§ 38.

Informacje zawarte w wiadomościach elektronicznych oraz przekazywane telefonicznie i faksem podlegają ochronie przed nieuprawnionym dostępem i modyfikacją, w szczególności poprzez zapewnienie poprawnej adresacji, na zasadach określonych w „Procedurze korzystania ze środków wymiany informacji", która stanowi załącznik nr 13 do zarządzenia.

§ 39.

Praca z wykorzystaniem nośnika elektronicznego odbywa się na zasadach określonych w „Procedurze zarządzania nośnikami elektronicznymi", która stanowi załącznik nr 14 do zarządzenia.

§ 40.

Prowadzenie rozmów na tematy służbowe w miejscach publicznych jest zabronione.

§ 41.

[redacted]	*dane niepodlegające udostępnianiu – art. 5 ustawy z dnia 6 września 2001 roku o dostępie do informacji publicznej*	[redacted]

§ 42.

[redacted]	*dane niepodlegające udostępnianiu – art. 5 ustawy z dnia 6 września 2001 roku o dostępie do informacji publicznej*	[redacted]

§ 43.

Informatyk monitoruje i reguluje wykorzystanie zasobów, ze szczególnym uwzględnieniem zasobów o długim okresie oczekiwania na dostawę lub wysokich kosztach, oraz przewiduje przyszłą pojemność systemów teleinformatycznych, aby zapewnić ich właściwą wydajność.

§ 44.

[redacted]	*dane niepodlegające udostępnianiu – art. 5 ustawy z dnia 6 września 2001 roku o dostępie do informacji publicznej*	[redacted]

§ 45.

1. Zegary stosowanych środków przetwarzania informacji należy zsynchronizować. Znacznik czasu powinien odpowiadać prawdziwej dacie i czasowi.
2. Przynajmniej raz w roku należy sprawdzać i korygować każde istotne odchylenie zegarów ze względu na ich upływność. Sprawdzenia i korekty dokonuje informatyk.

§ 46.

1. [redacted]	*dane niepodlegające udostępnianiu*	[redacted]

	– art. 5 ustawy z dnia 6 września 2001 roku o dostępie do informacji publicznej	
2.	*dane niepodlegające udostępnianiu – art. 5 ustawy z dnia 6 września 2001 roku o dostępie do informacji publicznej*	
3.	*dane niepodlegające udostępnianiu – art. 5 ustawy z dnia 6 września 2001 roku o dostępie do informacji publicznej*	
4.	*dane niepodlegające udostępnianiu – art. 5 ustawy z dnia 6 września 2001 roku o dostępie do informacji publicznej*	

5. Rejestry zdarzeń podlegają archiwizacji przez okres dwóch lat.

§ 47.

1. Użytkownik okresowo weryfikuje poprawności działania aplikacji poprzez sprawdzenie użycia funkcji dodawania, modyfikacji i usuwania, które umożliwiają dokonywanie zmian w danych.

2.	*dane niepodlegające udostępnianiu – art. 5 ustawy z dnia 6 września 2001 roku o dostępie do informacji publicznej*	

§ 48.

	dane niepodlegające udostępnianiu – art. 5 ustawy z dnia 6 września 2001 roku o dostępie do informacji	

§ 49.

1. W trakcie przeprowadzania weryfikacji kandydatów do pracy oraz, gdy jest to wskazane, wykonawców i użytkowników reprezentujących stronę trzecią należy, w oparciu o odpowiednie dokumenty:
   1) sprawdzić kompletność i dokładność przedstawionego życiorysu,
   2) potwierdzić deklarowane wykształcenie i kwalifikacje zawodowe,
   3) potwierdzić tożsamość.
2. Za przeprowadzenie weryfikacji kandydatów do pracy odpowiada komisja rekrutacyjna, a w przypadku jej niepowołania – Dyrektor.
3. Za przeprowadzenie weryfikacji wykonawców i użytkowników reprezentujących stronę trzecią odpowiada komisja przetargowa lub pracownik dokonujący rozeznania rynku, a w przypadku niepowołania komisji przetargowej albo niewyznaczenia pracownika dokonującego rozeznania rynku – Dyrektor.

§ 50.

1. Należy uzyskać zapewnienie, że pracownicy, wykonawcy i użytkownicy reprezentujący stronę trzecią akceptują oraz będą stosować zasady i warunki związane z bezpieczeństwem informacji, odpowiednie do rodzaju i zakresu przyznanego im dostępu.
2. W przypadku pracowników zapewnienie uzyskuje się poprzez podpisanie przez pracownika zakresu czynności lub dokumentu równoważnego.
3. W przypadku wykonawców i użytkowników reprezentujących stronę trzecią zapewnienie uzyskuje się poprzez zastosowanie w umowie odpowiedniej klauzuli.

§ 51.

W zakresach czynności lub w dokumentach równoważnych zawiera się wymagania odnoszące się do:

1) ochrony aktywów przed nieuprawnionym dostępem, ujawnieniem, modyfikacją, zniszczeniem lub zniekształceniem,
2) wykonywania konkretnych działań i procesów bezpieczeństwa,
3) zapewnienia odpowiedzialności pracownika za jego działania.

§ 52.

Dyrektor wyposaża pracowników w środki wspomagające system zarządzania bezpieczeństwem informacji podczas ich normalnej pracy oraz minimalizujące ryzyko błędów ludzkich.

§ 53.

Dyrektor wprowadza pracowników oraz, gdy jest to wskazane, wykonawców i użytkowników reprezentujących stronę trzecią w obowiązki i zakres odpowiedzialności związane z bezpieczeństwem informacji przed przyznaniem dostępu do informacji lub środków przetwarzania informacji.

§ 54.

Pracownicy oraz, gdy jest to wskazane, wykonawcy i użytkownicy reprezentujący stronę trzecią powinni być świadomi zagrożeń i innych aspektów bezpieczeństwa informacji oraz swoich obowiązków i odpowiedzialności prawnej.

§ 55.

1. Pracownicy oraz, gdy jest to wskazane, wykonawcy i użytkownicy reprezentujący stronę trzecią podlegają szkoleniu w zakresie bezpieczeństwa informacji.
2. Szkolenie obejmuje w szczególności:
   1) zagrożenia bezpieczeństwa informacji,
   2) skutki naruszenia zasad bezpieczeństwa informacji, w tym odpowiedzialność prawna,
   3) stosowanie środków zapewniających bezpieczeństwo informacji, w tym minimalizujących ryzyko błędów ludzkich.
3. Szkolenie przeprowadza się przed przyznaniem dostępu do informacji.
4. Szkolenie przeprowadza Dyrektor lub wyznaczony przez Dyrektora pracownik.

§ 56.

Szkolenie, o którym mowa w § 55, nie zwalnia z obowiązku informowania przez Dyrektora pracowników oraz, tam gdzie jest to wskazane, wykonawców i użytkowników reprezentujących stronę trzecią o uaktualnieniach dokumentacji systemu zarządzania bezpieczeństwem informacji, które są związane z wykonywaną przez nich pracą oraz utrzymywania w sposób ciągły przez pracowników oraz, tam gdzie jest to wskazane, wykonawców i użytkowników reprezentujących stronę trzecią odpowiednich umiejętności i kwalifikacji.

§ 57.

Zasadę rozdzielania obowiązków i zakresów odpowiedzialności należy stosować tak dalece, jak to możliwe i praktyczne, w szczególności audyt wewnętrzny w zakresie bezpieczeństwa informacji powinien pozostać niezależny.

§ 58.

1. Wszystkie posiadane przez pracowników oraz wykonawców i użytkowników reprezentujących stronę trzecią środki przetwarzania informacji podlegają zwrotowi w momencie zakończenia stosunku pracy lub umowy.

2. W przypadku, gdy pracownicy, wykonawcy lub użytkownicy reprezentujący stronę trzecią dysponują wiedzą ważną dla funkcjonowania Szkoły, wiedza ta podlega udokumentowaniu i przekazaniu.

§ 59.

1. Dostęp do plików systemowych jest kontrolowany.

2.	*dane niepodlegające udostępnianiu – art. 5 ustawy z dnia 6 września 2001 roku o dostępie do informacji publicznej*	
3.	*dane niepodlegające udostępnianiu – art. 5 ustawy z dnia 6 września 2001 roku o dostępie do informacji publicznej*	

§ 60.

1. Każdy incydent związany z bezpieczeństwem informacji należy niezwłocznie zgłaszać tak, aby umożliwić szybkie podjęcie działań korygujących, na zasadach określonych w „Procedurze zarządzania incydentami związanymi z bezpieczeństwem informacji", która stanowi załącznik nr 15 do zarządzenia.
2. Przez incydent związany z bezpieczeństwem informacji rozumie się pojedyncze zdarzenie lub serię niepożądanych lub niespodziewanych zdarzeń związanych z bezpieczeństwem informacji, które stwarzają znaczne prawdopodobieństwo zakłócenia funkcjonowania Szkoły i zagrażają bezpieczeństwu informacji.
3. W szczególności jako incydent związany z bezpieczeństwem informacji należy zakwalifikować każdą awarię lub inne nienormalne zachowanie systemu teleinformatycznego, a także:
   1) utratę usługi, urządzenia lub funkcjonalności,
   2) przeciążenie lub niepoprawne działanie systemu teleinformatycznego,
   3) błędy ludzkie,
   4) niezgodność z dokumentacją systemu zarządzania bezpieczeństwem informacji lub zaleceniami,
   5) naruszenie ustaleń związanych z bezpieczeństwem fizycznym,
   6) niekontrolowane zmiany systemu teleinformatycznego,
   7) niepoprawne działanie środków przetwarzania informacji,
   8) naruszenie dostępu.

§ 61.

W celu przeciwdziałania przerwom w funkcjonowaniu Szkoły wprowadza się „Plany ciągłości działania”, które stanowią załącznik nr 16 do zarządzenia.

§ 62.

W zakresie kopiowania całości lub części książek, artykułów, raportów lub innych dokumentów oraz powielania, przekształcania do innego formatu lub wyodrębniania z nagrań komercyjnych (filmów, nagrań dźwiękowych) należy przestrzegać prawa autorskiego.

§ 63.

Należy przestrzegać zasad i warunków dotyczących oprogramowania i informacji otrzymanych z Internetu.

§ 64.

1.	*dane niepodlegające udostępnianiu – art. 5 ustawy z dnia 6 września 2001 roku o dostępie do informacji publicznej*	

2. W przypadku przechowywania danych na nośnikach elektronicznych należy zapewnić możliwość czytania danego nośnika i formatu przez cały okres przechowywania tak, aby zabezpieczyć się przed utratą danych spowodowaną zmianą technologii w przyszłości.

§ 65.

Zasady i okres przechowywania dowodów własności licencji określają przepisy kancelaryjne.

§ 66.

1. Przynajmniej raz w roku przeprowadza się audyt wewnętrzny w zakresie bezpieczeństwa informacji.
2. W trakcie przeprowadzania audytu dostęp do oprogramowania i danych powinien być możliwy jedynie w trybie odczytu. Zezwolenie na dostęp inny niż tylko w trybie odczytu powinno być możliwy jedynie w przypadku odizolowanych kopii. Kopie te podlegają skasowaniu po przeprowadzeniu audytu lub odpowiedniej ochronie, jeśli istnieje konieczność przechowywania związana z wymaganiami dokumentowania audytu.
3. W przypadku przeprowadzania audytu przez stronę trzecią uzgadnia się zakres sprawdzenia i sposób udostępnienia zasobów informacyjnych niezbędnych do przeprowadzenia audytu tak, aby nie zakłócać funkcjonowania Szkoły.

4. W przypadku przeprowadzania audytu ze wsparciem odpowiedniego oprogramowania, oprogramowanie to podlega ochronie dostępu na zasadach określonych w „Procedurze kontroli dostępu”.

§ 67.

1. Wprowadza się „Politykę bezpieczeństwa”, która stanowi załącznik nr 17 do zarządzenia. Dotychczas obowiązująca „Polityka bezpieczeństwa danych osobowych” traci moc.
2. Wprowadza się „Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych”, która stanowi załącznik nr 18 do zarządzenia. Dotychczas obowiązująca „Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych” traci moc.

§ 68.

1. Przynajmniej raz w roku zespół ds. zarządzania ryzykiem przeprowadza szacowanie ryzyka w bezpieczeństwie informacji na zasadach określonych w „Procedurze zarządzania ryzykiem” mając na uwadze utratę integralności, poufności i dostępności informacji.
2. Przykłady typowych zagrożeń, które mogą być pomocne w procesie szacowania ryzyka stanowią załącznik nr 19 do zarządzenia.
3. Przykłady podatności, które mogą być pomocne w procesie szacowania ryzyka stanowią załącznik nr 20 do zarządzenia.

§ 69.

1. Upoważnienia do przetwarzania danych osobowych nadane przed wejściem w życie niniejszego zarządzenia pozostają w mocy do momentu nadania nowych upoważnień do przetwarzania danych osobowych na zasadach określonych w „Procedurze kontroli dostępu”.
2. Z chwilą nadania lub odbioru upoważnień do przetwarzania danych osobowych przez upoważnione osoby, jeśli data odbioru jest inna niż data nadania upoważnień do przetwarzania danych osobowych, nadane przed wejściem w życie niniejszego zarządzenia upoważnienia do przetwarzania danych osobowych automatycznie tracą ważność – nie mają tu zastosowania zasady odwołania upoważnień do przetwarzania danych osobowych określone w „Procedurze kontroli dostępu”.
3. „Procedurę kontroli dostępu” stosuje się dla upoważnień do przetwarzania danych osobowych nadawanych od momentu wejścia w życie niniejszego zarządzenia.

§ 70.

Wymagania w zakresie bezpieczeństwa informacji nie mogą zostać zmniejszone przy wprowadzaniu nowych produktów lub usług.

§ 71.

Osoby, którym przypisano odpowiedzialność za zapewnienie bezpieczeństwa informacji, a przekazują te zadania innym osobom, pozostają odpowiedzialne za ich realizację i weryfikują, czy wszystkie delegowane zadania wykonywane są poprawnie.

§ 72.

Wszelkie wymagania bezpieczeństwa oraz zabezpieczenia lokalne wynikające ze współpracy z wykonawcą lub użytkownikiem reprezentującym stronę trzecią należy odzwierciedlać w umowie.

§ 73.

1. Zasady zabezpieczania hasła administratora określa „Procedura postępowania z hasłami administratora", która stanowi załącznik nr 21 do zarządzenia.
2. Hasło administratora jest to hasło, które umożliwia dostęp do konta użytkownika (administratora) o bardzo wysokich uprawnieniach i pozwala na wykonanie każdego działania w systemie teleinformatycznym, w tym nadawania i zabierania uprawnień innym użytkownikom systemu teleinformatycznego.

§ 74.

1. Przynajmniej raz w roku Dyrektor lub wyznaczony przez Dyrektora pracownik przeprowadza przegląd stosowanych zabezpieczeń oraz dokumentacji systemu zarządzania bezpieczeństwem informacji tak, aby uzyskać zapewnienie o ich ciągłej przydatności, adekwatności i skuteczności, z zastrzeżeniem ust. 2 i 3.
2. Przynajmniej raz w roku Dyrektor lub wyznaczony przez Dyrektora pracownik dokonuje przeglądu stosowanego oprogramowania pod kątem ich zgodności z prawem autorskim.
3. Przynajmniej raz w roku informatyk dokonuje przeglądu środków przetwarzania informacji pod kątem ich zgodności ze standardami wdrażania bezpieczeństwa informacji. Jeśli stosowane są testy penetracyjne to należy przedsięwziąć środki ostrożności.

§ 75.

Nie dopuszcza się wykonywania innych czynności mających związek z systemem zarządzania bezpieczeństwem informacji niż te, które przewiduje niniejsza zarządzenie oraz nie dopuszcza się wykonywania czynności przewidzianych niniejszym zarządzeniem w sposób odmienny niż to przewidziano. Postanowienia niniejszego paragrafu nie oznaczają uchylenia w obszarze systemu zarządzania bezpieczeństwem informacji ani pierwszeństwa niniejszego zarządzenia przed innymi przepisami prawa i regulacjami dotyczącymi zasad postępowania w Szkole wynikających ze świadczenia pracy.

§ 76.

Obowiązki wynikające z § 28, 53, 55 i 72 dotyczą nowozatrudnionych pracowników, wykonawców lub użytkowników reprezentujących stronę trzecią.

§ 77.

Nadzór nad realizacją zarządzenia sprawuje Dyrektor.

§ 78.

Zarządzenie wchodzi w życie z dniem 1 kwietnia 2016 roku, za wyjątkiem § 14, który wchodzi w życie z dniem 1 lipca 2016 roku.

Załącznik nr 1 do zarządzenia nr 206/2015/2016 – wzór spisu środków przetwarzania informacji

SPIS ŚRODKÓW PRZETWARZANIA INFORMACJI

Rodzaj urządzenia	**Nazwa urządzenia**	**Numer seryjny**	**Numer inwentarzowy**	**Numer IP**	**Zainstalowane oprogramowanie**	**Numer licencji zainstalowanego oprogramowania**	**Uwagi**
				jeśli dotyczy	*jeśli dotyczy*	*jeśli dotyczy*	*np. informacja o wykreśleniu ze spisu*

Załącznik nr 2 do zarządzenia nr 206/2015/2016 – „Procedura autoryzacji nowych środków przetwarzania informacji”

PROCEDURA AUTORYZACJI NOWYCH ŚRODKÓW PRZETWARZANIA INFORMACJI

§ 1.

1. „Procedura autoryzacji nowych środków przetwarzania informacji”, zwana w dalszej części „Procedurą”, określa zasady dopuszczania do użytkowania nowych środków przetwarzania informacji oraz uaktualniania już zainstalowanego oprogramowania służącego do przetwarzania informacji w Szkole Podstawowej z Oddziałami Integracyjnymi nr 1 im. Janusza Korczaka w Rybniku.
2. Ilekroć w „Procedurze” mowa o:
   1) Dyrektorze – należy przez to rozumieć Dyrektora Szkoły Podstawowej z Oddziałami Integracyjnymi nr 1 im. Janusza Korczaka w Rybniku lub osobę zastępującą,
   2) informatyku – należy przez to rozumieć pracownika Szkoły Podstawowej z Oddziałami Integracyjnymi nr 1 im. Janusza Korczaka w Rybniku, wykonawcę lub użytkownika reprezentującego stronę trzecią, który czuwa nad sprawnym i ciągłym działaniem systemu teleinformatycznego,
   3) Szkole – należy przez to rozumieć Szkołę Podstawową z Oddziałami Integracyjnymi nr 1 im. Janusza Korczaka w Rybniku,
   4) środkach przetwarzania informacji – należy przez to rozumieć komputery stacjonarne i przenośne, drukarki, kopiarki, skanery, serwery, faksy, oprogramowanie oraz inne urządzenia służące do przetwarzania informacji.

§ 2.

1. Dla każdych nowych środków przetwarzania informacji, przed ich pozyskaniem lub wdrożeniem do użytkowania, należy zidentyfikować i uzgodnić wymagania bezpieczeństwa informacji.
2. Wymagania bezpieczeństwa informacji powinny być uzasadnione.

§ 3.

Autoryzacji podlegają wszystkie nowe środki przetwarzania informacji mające być użytkowane w Szkole.

§ 4.

[redacted] *dane niepodlegające udostępnianiu – art. 5 ustawy z dnia 6 września 2001 roku o dostępie do informacji* [redacted]

	publicznej	

§ 5.

	dane niepodlegające udostępnianiu – art. 5 ustawy z dnia 6 września 2001 roku o dostępie do informacji publicznej	

§ 6.

1.	*dane niepodlegające udostępnianiu – art. 5 ustawy z dnia 6 września 2001 roku o dostępie do informacji publicznej*	
2.	*dane niepodlegające udostępnianiu – art. 5 ustawy z dnia 6 września 2001 roku o dostępie do informacji publicznej*	
3.	*dane niepodlegające udostępnianiu – art. 5 ustawy z dnia 6 września 2001 roku o dostępie do informacji publicznej*	

§ 7.

4.	*dane niepodlegające udostępnianiu – art. 5 ustawy z dnia 6 września 2001 roku o dostępie do informacji publicznej*	

§ 8.

1. Wprowadzenie do eksploatacji nowego lub kolejnych wersji już zainstalowanego oprogramowania służącego do przewarzania informacji powinno odbywać się wyłącznie za zgodą Dyrektora.

2.	*dane niepodlegające udostępnianiu – art. 5 ustawy z dnia 6 września 2001 roku o dostępie do informacji publicznej*	

§ 9.

1. Po wprowadzeniu do eksploatacji nowego środka przetwarzania informacji informatyk dokonuje przeglądu zabezpieczeń, aby mieć pewność, że nie zostały one naruszone na skutek wprowadzonych zmian.
2. W razie konieczności procedury eksploatacyjne i plany ciągłości działania należy dostosować do wprowadzonych zmian, a pracowników Szkoły odpowiednio przeszkolić.

§ 10.

Wprowadzenie do eksploatacji nowego środka przetwarzania informacji nie powinno zakłócać funkcjonowania Szkoły.

§ 11.

Nadzór nad realizacją „Procedury” sprawuje Dyrektor.

Załącznik nr 3 do zarządzenia nr 206/2015/2016 – wzór powierzenia mienia

Rybnik, dnia … roku

POWIERZENIE MIENIA NR …

Na podstawie przepisów art. 124 § 1 pkt 2 i art. 124 § 2 ustawy z dnia 26 czerwca 1974 roku Kodeks pracy powierzam w celu wykonywania obowiązków służbowych Pani/Panu* … *(imię i nazwisko)* … *(nazwa powierzonego mienia)* z obowiązkiem zwrotu.

Jest Pani zobowiązana/Pan zobowiązany* do dbania o powierzone mienie i ponosi odpowiedzialność materialną za zniszczenie lub zgubienie powierzonego mienia. Za powierzone mienie odpowiada Pani/Pan* w pełnej wysokości.

Powierzenie mienia ważne jest do momentu zwrotu powierzonego mienia.

Dyrektor

……
(podpis i pieczątka)

Przyjmuję powierzenie mienia.

Pracownik

……
(data i podpis)

**niepotrzebne skreślić lub skasować*

Załącznik nr 4 do zarządzenia nr 206/2015/2016 – wzór ewidencji powierzonego mienia z obowiązkiem zwrotu lub do wyliczenia się

EWIDENCJA POWIERZONEGO MIENIA Z OBOWIĄZKIEM ZWROTU LUB DO WYLICZENIA SIĘ

Numer powierzenia mienia	Nazwa powierzonego mienia	Numer inwentarzowy powierzonego mienia	Data odebrania, przez pracownika, powierzonego mienia	Podpis pracownika, któremu powierzono mienie	Data zwrotu powierzonego mienia	Podpis pracownika zwracającego powierzone mienie	Podpis pracownika przyjmującego zwracane mienie	Uwagi

Załącznik nr 5 do zarządzenia nr 206/2015/2016 – wzór zgody na pracę z wykorzystaniem środków przetwarzania informacji

Rybnik, dnia … roku

ZGODA NA PRACĘ Z WYKORZYSTANIEM ŚRODKÓW PRZETWARZANIA INFORMACJI

Udzielam Pani/Panu* … *(imię i nazwisko)* zgody na pracę z wykorzystaniem środków przetwarzania informacji w ramach wykonywania czynności służbowych.

Dyrektor

……
(pieczątka i podpis)

Oświadczam, że jestem świadoma/świadomy* swojej odpowiedzialności za utrzymanie skutecznej kontroli dostępu, w szczególności w odniesieniu do haseł i zabezpieczenia użytkowanych przez siebie środków przetwarzania informacji.

Pracownik, któremu udzielono zgody

……
(podpis)

** niepotrzebne skreślić lub skasować*

Załącznik nr 6 do zarządzenia nr 206/2015/2016 – „Procedura kontroli dostępu”

PROCEDURA KONTROLI DOSTĘPU

§ 1.

1. „Procedura kontroli dostępu”, zwana w dalszej części „Procedurą”, określa zasady przyznawania praw dostępu do przetwarzania danych osobowych, do pracy na komputerze i z wykorzystaniem oprogramowania służącego do przetwarzania informacji oraz stosowane metody i środki uwierzytelniania dostępu w Szkole Podstawowej z Oddziałami Integracyjnymi nr 1 im. Janusza Korczaka w Rybniku.
2. Ilekroć w „Procedurze” jest mowa o:
   1) administratorze danych – należy przez to rozumieć Szkołę Podstawową z Oddziałami Integracyjnymi nr 1 im. Janusza Korczaka w Rybniku reprezentowaną przez Dyrektora Szkoły Podstawowej z Oddziałami Integracyjnymi nr 1 im. Janusza Korczaka w Rybniku,
   2) Dyrektorze – należy przez to rozumieć Dyrektora Szkoły Podstawowej z Oddziałami Integracyjnymi nr 1 im. Janusza Korczaka w Rybniku lub osobę zastępującą,
   3) informatyku – należy przez to rozumieć pracownika Szkoły Podstawowej z Oddziałami Integracyjnymi nr 1 im. Janusza Korczaka w Rybniku, wykonawcę lub użytkownika reprezentującego stronę trzecią, który czuwa nad sprawnym i ciągłym działaniem systemu teleinformatycznego,
   4) Szkole – należy przez to rozumieć Szkołę Podstawową z Oddziałami Integracyjnymi nr 1 im. Janusza Korczaka w Rybniku,
   5) użytkowniku – należy przez to rozumieć pracownika Szkoły Podstawowej z Oddziałami Integracyjnymi nr 1 im. Janusza Korczaka w Rybniku, wykonawcę lub użytkownika reprezentującego stronę trzecią, któremu przyznano prawo dostępu do pracy na komputerze i z wykorzystaniem oprogramowania służącego do przetwarzania informacji będących własnością Szkoły Podstawowej z Oddziałami Integracyjnymi nr 1 im. Janusza Korczaka w Rybniku.

§ 2.

1. Prawo dostępu przyznawane jest zgodnie z zasadą wiedzy koniecznej oraz poziomami bezpieczeństwa i klasyfikacji informacji.
2. Dostęp jest niemożliwy, dopóki procedura nadawania uprawnień nie zostanie zakończona.

§ 3.

	dane niepodlegające udostępnianiu – art. 5 ustawy z dnia 6	

	września 2001 roku o dostępie do informacji publicznej	

§ 4.

1.	*dane niepodlegające udostępnianiu – art. 5 ustawy z dnia 6 września 2001 roku o dostępie do informacji publicznej*	
2.	*dane niepodlegające udostępnianiu – art. 5 ustawy z dnia 6 września 2001 roku o dostępie do informacji publicznej*	
3.	*dane niepodlegające udostępnianiu – art. 5 ustawy z dnia 6 września 2001 roku o dostępie do informacji publicznej*	
4.	*dane niepodlegające udostępnianiu – art. 5 ustawy z dnia 6 września 2001 roku o dostępie do informacji publicznej*	
5.	*dane niepodlegające udostępnianiu – art. 5 ustawy z dnia 6 września 2001 roku o dostępie do informacji publicznej*	

§ 5.

6.	*dane niepodlegające udostępnianiu – art. 5 ustawy z dnia 6 września 2001 roku*	

	o dostępie do informacji publicznej	

§ 6.

1.	*dane niepodlegające udostępnianiu – art. 5 ustawy z dnia 6 września 2001 roku o dostępie do informacji publicznej*	
2.	*dane niepodlegające udostępnianiu – art. 5 ustawy z dnia 6 września 2001 roku o dostępie do informacji publicznej*	
3.	*dane niepodlegające udostępnianiu – art. 5 ustawy z dnia 6 września 2001 roku o dostępie do informacji publicznej*	
4.	*dane niepodlegające udostępnianiu – art. 5 ustawy z dnia 6 września 2001 roku o dostępie do informacji publicznej*	
5.	*dane niepodlegające udostępnianiu – art. 5 ustawy z dnia 6 września 2001 roku o dostępie do informacji publicznej*	
6.	*dane niepodlegające udostępnianiu – art. 5 ustawy z dnia 6 września 2001 roku o dostępie do informacji publicznej*	
7.	*dane niepodlegające*	

	udostępnianiu – art. 5 ustawy z dnia 6 września 2001 roku o dostępie do informacji publicznej	
8.	*dane niepodlegające udostępnianiu – art. 5 ustawy z dnia 6 września 2001 roku o dostępie do informacji publicznej*	
9.	*dane niepodlegające udostępnianiu – art. 5 ustawy z dnia 6 września 2001 roku o dostępie do informacji publicznej*	
10.	*dane niepodlegające udostępnianiu – art. 5 ustawy z dnia 6 września 2001 roku o dostępie do informacji publicznej*	

§ 7.

1.	*dane niepodlegające udostępnianiu – art. 5 ustawy z dnia 6 września 2001 roku o dostępie do informacji publicznej*	
2.	*dane niepodlegające udostępnianiu – art. 5 ustawy z dnia 6 września 2001 roku o dostępie do informacji publicznej*	
3.	*dane niepodlegające udostępnianiu – art. 5 ustawy z dnia 6 września 2001 roku*	

	o dostępie do informacji publicznej	
4.	*dane niepodlegające udostępnianiu – art. 5 ustawy z dnia 6 września 2001 roku o dostępie do informacji publicznej*	
5.	*dane niepodlegające udostępnianiu – art. 5 ustawy z dnia 6 września 2001 roku o dostępie do informacji publicznej*	

§ 8.

	dane niepodlegające udostępnianiu – art. 5 ustawy z dnia 6 września 2001 roku o dostępie do informacji publicznej	

§ 9.

1. Do przetwarzania danych osobowych mogą być dopuszczone wyłącznie osoby posiadające upoważnienie.
2. Upoważnienie do przetwarzania danych osobowych nadaje i odwołuje Dyrektor, który pełni funkcję administratora danych.
3. Upoważnienie do przetwarzania danych osobowych i jego odwołanie sporządzane są na piśmie, w dwóch jednobrzmiących egzemplarzach – jeden przeznaczony jest dla osoby, której nadano lub odebrano upoważnienie do przetwarzania danych osobowych, drugi – dla Dyrektora. Wzór upoważnienia do przetwarzania danych osobowych stanowi załącznik nr 1 do „Procedury". Wzór odwołania upoważnienia stanowi załącznik nr 2 do „Procedury".
4. Upoważnienia do przetwarzania danych osobowych nie sporządza się dla Dyrektora.
5. Upoważnienia do przetwarzania danych osobowych ujmowane są w ewidencji osób upoważnionych do przetwarzania danych osobowych, której wzór stanowi załącznik nr 3 do „Procedury". Ewidencję osób upoważnionych do przetwarzania danych osobowych prowadzi Dyrektor.

§ 10.

Dyrektor dokonuje przeglądu praw dostępu użytkowników przynajmniej raz w roku oraz po wprowadzeniu wszelkich zmian, takich jak awans, degradacja lub zakończenie stosunku pracy.

§ 11.

	dane niepodlegające udostępnianiu – art. 5 ustawy z dnia 6 września 2001 roku o dostępie do informacji publicznej	

§ 12.

Użytkownikowi, który zmienił stanowisko lub opuścił Szkołę niezwłocznie odbierane i blokowane są prawa dostępu.

§ 13.

Nadzór nad realizacją „Procedury” sprawuje Dyrektor.

Załącznik nr 1 do „Procedury kontroli dostępu” – wzór upoważnienia do przetwarzania danych osobowych

Rybnik, dnia … roku

UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH

Na podstawie art. 37 ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych upoważniam Panią/Pana* … *(imię i nazwisko)* do przetwarzania danych osobowych w następującym zbiorze danych osobowych/następujących zbiorach danych osobowych*: ... *(nazwa zbioru lub nazwy zbiorów danych osobowych)*.

Zgodnie z art. 39 ust. 2 ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych jest Pani zobowiązana/Pan zobowiązany* zachować w tajemnicy przetwarzane dane osobowe oraz sposoby ich zabezpieczenia.

Administrator danych

……
(pieczątka i podpis)

Upoważniona osoba*

……
(podpis)

** niepotrzebne skreślić lub skasować*

Załącznik nr 2 do „Procedury kontroli dostępu” – wzór odwołania upoważnienia do przetwarzania danych osobowych

Rybnik, dnia … roku

ODWOŁANIE UPOWAŻNIENIA DO PRZETWARZANIA DANYCH OSOBOWYCH

Na podstawie art. 37 ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych odwołuję z dniem … *(data)* upoważnienie do przetwarzania danych osobowych wystawione dla Pani/Pana* … *(imię i nazwisko).*

Administrator danych

……
(pieczątka i podpis)

** niepotrzebne skreślić lub skasować*

Załącznik nr 3 do „Procedury kontroli dostępu” – wzór ewidencji osób upoważnionych do przetwarzania danych osobowych

EWIDENCJA OSÓB UPOWAŻNIONYCH DO PRZETWARZANIA DANYCH OSOBOWYCH

Imię i nazwisko	Data nadania upoważnienia	Data odebrania upoważnienia	Zakres upoważnienia	Identyfikator użytkownika w systemie

Załącznik nr 7 do zarządzenia nr 206/2015/2016 – „Procedura przetwarzania mobilnego”

PROCEDURA PRZETWARZANIA MOBILNEGO

§ 1.

1. „Procedura przetwarzania mobilnego”, zwana w dalszej części „Procedurą”, określa wymagania dotyczące ochrony fizycznej, kontroli dostępu, wykonywania kopii zapasowych i ochrony przed działaniem złośliwego oprogramowania przy przetwarzaniu mobilnym informacji poza siedzibą Szkoły Podstawowej z Oddziałami Integracyjnymi nr 1 im. Janusza Korczaka w Rybniku.
2. Ilekroć w „Procedurze” jest mowa o:
   1) Dyrektorze – należy przez to rozumieć Dyrektora Szkoły Podstawowej z Oddziałami Integracyjnymi nr 1 im. Janusza Korczaka w Rybniku lub osobę zastępującą,
   2) informatyku – należy przez to rozumieć pracownika Szkoły Podstawowej z Oddziałami Integracyjnymi nr 1 im. Janusza Korczaka w Rybniku, wykonawcę lub użytkownika reprezentującego stronę trzecią, który czuwa nad sprawnym i ciągłym działaniem systemu teleinformatycznego,
   3) Szkole – należy przez to rozumieć Szkołę Podstawową z Oddziałami Integracyjnymi nr 1 im. Janusza Korczaka w Rybniku,
   4) urządzeniach przenośnych – należy przez to rozumieć notebooki, palmtopy, laptopy, tablety, karty elektroniczne, telefony komórkowe i inne urządzenia przenośne będące własnością Szkoły Podstawowej z Oddziałami Integracyjnymi nr 1 im. Janusza Korczaka w Rybniku.

§ 2.

1. [redacted]	*dane niepodlegające udostępnianiu – art. 5 ustawy z dnia 6 września 2001 roku o dostępie do informacji publicznej*	[redacted]

2. Dyrektor może określić i sprawdzić czas zwrotu urządzenia przenośnego. Niezależnie od tego, Dyrektor lub wyznaczona przez Dyrektora osoba może przeprowadzić kontrolę w celu wykrycia urządzeń przenośnych wynoszonych bez zgody Dyrektora.

§ 3.

[redacted]	*dane niepodlegające udostępnianiu – art. 5 ustawy z dnia 6 września 2001 roku*	[redacted]

	o dostępie do informacji publicznej	

§ 4.

1. Używając urządzeń przenośnych należy zwracać szczególną uwagę na to, aby nie naruszyć bezpieczeństwa informacji, w szczególności w niechronionym środowisku.
2. Używając urządzeń przenośnych należy stosować środki uwierzytelniania określone w „Procedurze kontroli dostępu”.
3. Używając urządzeń przenośnych należy przestrzegać zaleceń producenta dotyczących ochrony, w tym ochrony przed wystawieniem na silne pola elektromagnetyczne.

§ 5.

	dane niepodlegające udostępnianiu – art. 5 ustawy z dnia 6 września 2001 roku o dostępie do informacji publicznej	

§ 6.

Urządzenia przenośne należy zabezpieczyć przed działaniem złośliwego oprogramowania przy pomocy oprogramowania antywirusowego na zasadach określonych w „Procedurze ochrony przed złośliwym oprogramowaniem”.

§ 7.

1. Urządzenia przenośne podlegają prewencji programowej i technicznej.
2. O przeprowadzeniu prewencji programowej i technicznej decyduje informatyk.

§ 8.

1. Kopie zapasowe informacji i oprogramowania służącego do przetwarzania informacji znajdujących się na urządzeniach przenośnych należy wykonywać regularnie i na zasadach określonych w „Procedurze tworzenia kopii zapasowych”.

2.	*dane niepodlegające udostępnianiu – art. 5 ustawy z dnia 6 września 2001 roku o dostępie do informacji publicznej*	

§ 9.

1. Osoby korzystające z przetwarzania mobilnego informacji podlegają szkoleniu w zakresie bezpiecznego korzystania z urządzeń przenośnych, aby zwiększyć świadomość występowania dodatkowego ryzyka związanego z tym sposobem pracy oraz zabezpieczeń, które trzeba wprowadzić.
2. Szkolenie przeprowadza się przed udzieleniem zgodny na przetwarzanie mobilne informacji.
3. Szkolenie przeprowadza Dyrektor.

§ 10.

Zgubienie lub kradzież urządzenia przenośnego traktowane jest jako incydent związany z bezpieczeństwem informacji i należy wtedy postępować zgodnie z „Procedurą zarządzania incydentami związanymi z bezpieczeństwem informacji".

§ 11.

Wszelkie czynności związane z instalacją oprogramowania i konfiguracją urządzeń przenośnych wykonuje informatyk.

§ 12.

Nadzór nad realizacją „Procedury" sprawuje Dyrektor.

Załącznik nr 8 do zarządzenia nr 206/2015/2016 – „Procedura rozpoczęcia, zawieszenia i zakończenia pracy na komputerze”

PROCEDURA ROZPOCZĘCIA, ZAWIESZENIA I ZAKOŃCZENIA PRACY NA KOMPUTERZE

§ 1.

1. „Procedura rozpoczęcia, zawieszenia i zakończenia pracy na komputerze”, zwana w dalszej części „Procedurą”, określa czynności, które użytkownik powinien podjąć w celu rozpoczęcia, zawieszenia i zakończenia pracy na komputerze, a także zasady, których użytkownik powinien przestrzegać w trakcie pracy na komputerze w Szkole Podstawowej z Oddziałami Integracyjnymi nr 1 im. Janusza Korczaka w Rybniku.
2. Ilekroć w „Procedurze” jest mowa o:
   1) Dyrektorze – należy przez to rozumieć Dyrektora Szkoły Podstawowej z Oddziałami Integracyjnymi nr 1 im. Janusza Korczaka w Rybniku lub osobę zastępującą,
   2) użytkowniku – należy przez to rozumieć pracownika Szkoły Podstawowej z Oddziałami Integracyjnymi nr 1 im. Janusza Korczaka w Rybniku, wykonawcę lub użytkownika reprezentującego stronę trzecią, któremu przyznano prawo dostępu do pracy na komputerze i z wykorzystaniem oprogramowania służącego do przetwarzania informacji będących własnością Szkole Podstawowej z Oddziałami Integracyjnymi nr 1 im. Janusza Korczaka w Rybniku.

§ 2.

Do pracy na komputerze dopuszczeni są jedynie użytkownicy posiadający zgodę Dyrektora na pracę z wykorzystaniem środków przetwarzania informacji.

§ 3.

1. Przed rozpoczęciem pracy na komputerze użytkownik sprawdza, czy nie ma oznak fizycznego naruszenia zabezpieczeń.

2.	*dane niepodlegające udostępnianiu – art. 5 ustawy z dnia 6 września 2001 roku o dostępie do informacji publicznej*	
3.	*dane niepodlegające udostępnianiu – art. 5 ustawy z dnia 6 września 2001 roku o dostępie do informacji publicznej*	

4.	*dane niepodlegające udostępnianiu – art. 5 ustawy z dnia 6 września 2001 roku o dostępie do informacji publicznej*	
5.	*dane niepodlegające udostępnianiu – art. 5 ustawy z dnia 6 września 2001 roku o dostępie do informacji publicznej*	
6.	*dane niepodlegające udostępnianiu – art. 5 ustawy z dnia 6 września 2001 roku o dostępie do informacji publicznej*	

7. Po poprawnym zalogowaniu się, użytkownik rozpoczyna pracę na komputerze.

§ 4.

W trakcie uruchamiania komputera użytkownik nie powinien odchodzić od komputera.

§ 5.

W trakcie pracy ekran monitora komputera powinien być ustawiony w sposób uniemożliwiający osobie nieuprawnionej wgląd lub spisanie informacji wyświetlanych na ekranie monitora.

§ 6.

1. Przy każdorazowym opuszczeniu stanowiska komputerowego w trakcie pracy, użytkownik powinien zablokować komputer lub wylogować się.
2. Blokada komputera następuje po naciśnięciu skrótu klawiszowego Windows + I lub klawiszy Ctrl + Alt + Delete i potwierdzenie klawiszem Enter podświetlonej opcji „Zablokuj komputer”.
3. Po zablokowaniu komputera lub wylogowaniu się użytkownik, aby ponownie przystąpić do pracy, powinien się zalogować.

§ 7.

Zmianę użytkownika komputera każdorazowo powinno poprzedzać wylogowanie się poprzedniego użytkownika.

§ 8.

1. Przed zakończeniem pracy na komputerze użytkownik powinien zapisać wszystkie zmiany, a następnie zamknąć lub wylogować się z uruchomionego oprogramowania.
2. Zakończenie pracy na komputerze polega na wylogowaniu się, zamknięciu komputera i, jeśli jest to możliwe, wyłączeniu monitora.
3. Użytkownik powinien pozostać przy komputerze do chwili jego wyłączenia.

§ 9.

Nadzór nad realizacją „Procedury” sprawuje Dyrektor.

Załącznik nr 9 do zarządzenia nr 206/2015/2016 – „Procedura wykonywania przeglądów, konserwacji i napraw komputerów, nośników i oprogramowania służących do przetwarzania informacji”

PROCEDURA WYKONYWANIA PRZEGLĄDÓW, KONSERWCJI I NAPRAW KOMPUTERÓW, NOŚNIKÓW I OPROGRAMOWANIA SŁUŻĄCYCH DO PRZETWARZANIA INFORMACJI

§ 1.

1. „Procedura wykonywania przeglądów, konserwacji i napraw komputerów, nośników i oprogramowania służących do przetwarzania informacji”, zwana w dalszej części „Procedurą”, określa zasady i sposób wykonywania przeglądów, konserwacji i napraw komputerów, nośników i oprogramowania służących do przetwarzania informacji oraz osoby odpowiedzialne za ich wykonywanie w Szkole Podstawowej z Oddziałami Integracyjnymi nr 1 im. Janusza Korczaka w Rybniku.
2. Ilekroć w „Procedurze” jest mowa o:
   1) Dyrektorze – należy przez to rozumieć Dyrektora Szkoły Podstawowej z Oddziałami Integracyjnymi nr 1 im. Janusza Korczaka w Rybniku lub osobę zastępującą,
   2) informatyku – należy przez to rozumieć pracownika Szkoły Podstawowej z Oddziałami Integracyjnymi nr 1 im. Janusza Korczaka w Rybniku, wykonawcę lub użytkownika reprezentującego stronę trzecią, który czuwa nad sprawnym i ciągłym działaniem systemu teleinformatycznego,
   3) Szkole – należy przez to rozumieć Szkołę Podstawową z Oddziałami Integracyjnymi nr 1 im. Janusza Korczaka w Rybniku.

§ 2.

Przeglądy, konserwacje i naprawa komputerów, nośników i oprogramowania służących do przetwarzania informacji wykonywane są w pomieszczeniach stanowiących obszar bezpieczny, o którym mowa w § 12 zarządzenia nr 206/2015/2016.

§ 3.

Konserwacja komputera służącego do przetwarzania informacji polega na wyczyszczeniu podzespołów komputera z wykorzystaniem specjalistycznych preparatów.

§ 4.

Przegląd oprogramowania służącego do przetwarzania informacji polega na sprawdzeniu konfiguracji oraz rejestrów zdarzeń (logów).

§ 5.

Przeglądy, konserwacje i naprawy komputerów, nośników i oprogramowania służących do przetwarzania informacji przeprowadza informatyk.

§ 6.

1.	*dane niepodlegające udostępnianiu – art. 5 ustawy z dnia 6 września 2001 roku o dostępie do informacji publicznej*	
2.	*dane niepodlegające udostępnianiu – art. 5 ustawy z dnia 6 września 2001 roku o dostępie do informacji publicznej*	
3.	*dane niepodlegające udostępnianiu – art. 5 ustawy z dnia 6 września 2001 roku o dostępie do informacji publicznej*	

4. Po wykonaniu prac przez serwisanta, informatyk sprawdza stan komputerów lub nośników służących do przetwarzania informacji oraz zmienia hasła administratora w przypadku konieczności ich wcześniejszego ujawnienia serwisantowi. Zasady postępowania z hasłami administratora określa „Procedura postępowania z hasłami administratora".
5. Wykonane przez serwisanta prace należy udokumentować.

§ 7.

1. Komputery, nośniki i oprogramowanie służące do przetwarzania informacji należy przeglądać i konserwować zgodnie z zaleceniami dostawcy lub producenta co do częstotliwości i zakresu.
2. Komputery, nośniki i oprogramowanie służące do przetwarzania informacji należy naprawiać niezwłocznie.

§ 8.

Zabronione jest wykonywanie przeglądów, konserwacji i napraw komputerów, nośników i oprogramowania służących do przetwarzania informacji samodzielnie przez pracownika Szkoły, chyba, że jest nim informatyk.

§ 9.

1. W przypadku stwierdzenia w wyniku wykonywania napraw, przeglądów i konserwacji komputerów, nośników i oprogramowania służących do przetwarzania informacji

istotnych błędów, należy je odnotować w rejestrze błędów, którego wzór stanowi załącznik do „Procedury”.

2. Jeśli błąd stanowi incydent związany z bezpieczeństwem informacji, należy postępować zgodnie z „Procedurą zarządzania incydentami związanymi z bezpieczeństwem informacji”.

§ 10.

Nadzór nad realizacją „Procedury” sprawuje Dyrektor.

Załącznik do „Procedury wykonywania przeglądów, konserwacji i napraw komputerów, nośników i oprogramowania służących do przetwarzania informacji” – wzór rejestru błędów

REJESTR BŁĘDÓW

Data stwierdzenia błędu	Opis błędu	Podpis

Załącznik nr 10 do zarządzenia nr 206/2015/2016 – „Procedura tworzenia kopii zapasowych”

PROCEDURA TWORZENIA KOPII ZAPASOWYCH

§ 1.

1. „Procedura tworzenia kopii zapasowych”, zwana w dalszej części „Procedurą”, określa zasady tworzenia i przechowywania kopii zapasowych informacji i oprogramowania służącego do przetwarzania informacji oraz osoby odpowiedzialne za ich tworzenie w Szkole Podstawowej z Oddziałami Integracyjnymi nr 1 im. Janusza Korczaka w Rybniku.
2. Ilekroć w „Procedurze” jest mowa o:
   1) Dyrektorze – należy przez to rozumieć Dyrektora Szkoły Podstawowej z Oddziałami Integracyjnymi nr 1 im. Janusza Korczaka w Rybniku lub osobę zastępującą,
   2) informatyku – należy przez to rozumieć pracownika Szkoły Podstawowej z Oddziałami Integracyjnymi nr 1 im. Janusza Korczaka w Rybniku, wykonawcę lub użytkownika reprezentującego stronę trzecią, który czuwa nad sprawnym i ciągłym działaniem systemu teleinformatycznego,
   3) użytkowniku – należy przez to rozumieć pracownika Szkoły Podstawowej z Oddziałami Integracyjnymi nr 1 im. Janusza Korczaka w Rybniku, wykonawcę lub użytkownika reprezentującego stronę trzecią, któremu przyznano prawo dostępu do pracy na komputerze i z wykorzystaniem oprogramowania służącego do przetwarzania informacji będących własnością Szkole Podstawowej z Oddziałami Integracyjnymi nr 1 im. Janusza Korczaka w Rybniku.

§ 2.

1. Informacje i oprogramowanie służące do przetwarzania informacji należy zabezpieczać poprzez wykonywanie kopii zapasowych.
2. Kopie zapasowe należy tworzyć niezależnie dla każdego oprogramowania służącego do przetwarzania informacji.

§ 3.

[redacted] *dane niepodlegające udostępnianiu – art. 5 ustawy z dnia 6 września 2001 roku o dostępie do informacji publicznej* [redacted]

§ 4.

1. Kopie zapasowe tworzone są według potrzeb tak, aby zapewnić ciągłość działania.
2. [redacted] *dane niepodlegające* [redacted]

	udostępnianiu – art. 5 ustawy z dnia 6 września 2001 roku o dostępie do informacji publicznej	

§ 5.

Nośniki zawierające kopię zapasową należy wyjmować z komputera w trakcie bieżącej pracy komputera.

§ 6.

Kopie zapasowe podlegają ochronie na zasadach określonych w „Procedurze kontroli dostępu”.

§ 7.

Nośniki zawierające kopie zapasowe należy przechowywać w sposób uniemożliwiający ich utratę, uszkodzenie lub dostęp osób nieuprawnionych. Zasady przechowywania nośników określa „Procedura zarządzania nośnikami”.

§ 8.

1. Nie należy przechowywać zbędnych kopii zapasowych.
2. Po upływie okresu użyteczności lub przechowywania, kopie zapasowe należy skasować lub zniszczyć tak, aby nie było możliwe ich odczytanie.

3.	*dane niepodlegające udostępnianiu – art. 5 ustawy z dnia 6 września 2001 roku o dostępie do informacji publicznej*	

§ 9.

1.	*dane niepodlegające udostępnianiu – art. 5 ustawy z dnia 6 września 2001 roku o dostępie do informacji publicznej*	
2.	*dane niepodlegające udostępnianiu – art. 5 ustawy z dnia 6 września 2001 roku*	

§ 10.

Nadzór nad realizacją „Procedury” sprawuje Dyrektor.

Załącznik nr 11 do zarządzenia nr 206/2015/2016 – „Procedura korzystania z sieci Internet”

PROCEDURA KORZYSTANIA Z SIECI INTERNET

§ 1.

1. „Procedura korzystania z sieci Internet”, zwana w dalszej części „Procedurą”, określa zasady korzystania z sieci Internet w Szkole Podstawowej z Oddziałami Integracyjnymi nr 1 im. Janusza Korczaka w Rybniku.
2. Ilekroć w „Procedurze” jest mowa o:
   1) Dyrektorze – należy przez to rozumieć Dyrektora Szkoły Podstawowej z Oddziałami Integracyjnymi nr 1 im. Janusza Korczaka w Rybniku lub osobę zastępującą,
   2) informatyku – należy przez to rozumieć pracownika Szkoły Podstawowej z Oddziałami Integracyjnymi nr 1 im. Janusza Korczaka w Rybniku, wykonawcę lub użytkownika reprezentującego stronę trzecią, który czuwa nad sprawnym i ciągłym działaniem systemu teleinformatycznego,
   3) Szkole – należy przez to rozumieć Szkołę Podstawową z Oddziałami Integracyjnymi nr 1 im. Janusza Korczaka w Rybniku,
   4) użytkowniku – należy przez to rozumieć pracownika Szkoły Podstawowej z Oddziałami Integracyjnymi nr 1 im. Janusza Korczaka w Rybniku, wykonawcę lub użytkownika reprezentującego stronę trzecią, któremu przyznano prawo dostępu do pracy na komputerze i z wykorzystaniem oprogramowania służącego do przetwarzania informacji będących własnością Szkoły Podstawowej z Oddziałami Integracyjnymi nr 1 im. Janusza Korczaka w Rybniku.

§ 2.

Do sieci Internet powinien być podłączony tylko komputer lub urządzenie mobilne będące własnością Szkoły.

§ 3.

Zabrania się:

1) prowadzenia ataków, włamań i innych działań związanych z ingerencją w dane komputerów innych użytkowników lub osób trzecich oraz komputerów lub urządzeń mobilnych w sieci Internet, a także świadomego lub nieświadomego prowadzenia innych działań destrukcyjnych,
2) utrudniania lub uniemożliwiania innym użytkownikom korzystania z sieci Internet poprzez uruchamianie oprogramowania nadmiernie obciążającego transfer,
3) wprowadzania wszelkich nieuzgodnionych z informatykiem zmian we właściwościach połączeń sieciowych komputera, w szczególności adresu IP, MAC oraz rozpowszechniania tych ustawień konfiguracyjnych osobom trzecim,

4) przeglądania stron WWW potencjalnie niebezpiecznych w szczególności zawierających hazard lub cracki,
5) wykorzystywania sieci Internet do prowadzenia działalności niezgodnej z przepisami prawa, w szczególności do rozsyłania niechcianej poczty elektronicznej (spam) oraz wymiany plików w sieciach typu P2P,
6) uruchamiania przez użytkownika oprogramowania umożliwiającego przejmowanie zdalnej kontroli nad komputerem lub urządzeniem mobilnym będącym własnością Szkoły.

§ 4.

Informatyk bada przepływy ruchu sieciowego oraz skanuje porty komunikacyjne w celach diagnostycznych oraz w celu zapewnienia należytego bezpieczeństwa infrastruktury informatycznej.

§ 5.

Nadzór nad realizacją „Procedury” sprawuje Dyrektor.

Załącznik nr 12 do zarządzenia nr 206/2015/2016 – „Procedura ochrony przed złośliwym oprogramowaniem”

PROCEDURA OCHRONY PRZED ZŁOŚLIWYM OPROGRAMOWANIEM

§ 1.

1. „Procedura ochrony przed złośliwym oprogramowaniem”, zwana w dalszej części „Procedurą”, określa rodzaje i działanie złośliwego oprogramowania, działania profilaktyczne i ochronne przed złośliwym oprogramowaniem oraz osoby odpowiedzialne za ich stosowanie w Szkole Podstawowej z Oddziałami Integracyjnymi nr 1 im. Janusza Korczaka w Rybniku.
2. Ilekroć w „Procedurze” mowa o:
   1) Dyrektorze – należy przez to rozumieć Dyrektora Szkoły Podstawowej z Oddziałami Integracyjnymi nr 1 im. Janusza Korczaka w Rybniku lub osobę zastępującą,
   2) informatyku – należy przez to rozumieć pracownika Szkoły Podstawowej z Oddziałami Integracyjnymi nr 1 im. Janusza Korczaka w Rybniku, wykonawcę lub użytkownika reprezentującego stronę trzecią, który czuwa nad sprawnym i ciągłym działaniem systemu teleinformatycznego,
   3) Szkole – należy przez to rozumieć Szkołę Podstawową z Oddziałami Integracyjnymi nr 1 im. Janusza Korczaka w Rybniku.

§ 2.

Do złośliwego oprogramowania zalicza się w szczególności:

1) wirus – program lub fragment wrogiego wykonalnego kodu, który dołącza się, nadpisuje lub zamienia inny program w celu reprodukcji samego siebie bez zgody użytkownika,
2) robak – złośliwe oprogramowanie rozmnażające się tylko przez sieć Internet, zwłaszcza przez pocztę elektroniczną, nie potrzebuje programu „żywiciela”,
3) wabbit – program rezydentny nie powielający się przez sieć Internet, wynikiem jego działania jest jedna określona operacja, np. powielanie tego samego pliku aż do wyczerpania zasobów pamięci komputera,
4) trojan – ukrywa się pod nazwą lub w części pliku, który użytkownikowi wydaje się pomocny. Oprócz właściwego działania pliku, zgodnego z jego nazwą, trojan wykonuje operacje w tle szkodliwe dla użytkownika, np. otwiera port komputera, przez który może być dokonany atak włamywacza (hakera),
5) backdoor – przejmuje kontrolę nad zainfekowanym komputerem, umożliwiając wykonanie na nim czynności administracyjnych, łącznie z usuwaniem i zapisem danych. Podszywa się pod pliki i programy, z których często korzysta użytkownik. Umożliwia włamywaczowi administrowaniem systemem operacyjnym przez sieć Internet i wykonywanie zadań wbrew wiedzy i woli użytkownika,

6) program szpiegujący – oprogramowanie zbierające informacje o użytkowniku bez jego zgody, np. informacje o odwiedzanych witrynach, hasła dostępu. Występuje często jako dodatkowy i ukryty komponent większego programu, odporny na usuwanie i ingerencję użytkownika. Może wykonywać działania bez wiedzy użytkownika, np. zmieniać wpisy do rejestru systemu operacyjnego i ustawienia użytkownika. Może pobierać i uruchamiać pliki z sieci Internet,
7) rootkit – maskuje obecności pewnych uruchomionych programów lub procesów systemowych, które z reguły służą włamywaczowi (hakerowi) do administrowania zaatakowanym systemem. Rootkit zostaje wkompilowany lub wstrzyknięty w istotne procedury systemowe, jest trudny do wykrycia z racji tego, że nie występuje jako osobna aplikacja. Zainstalowanie rootkita jest najczęściej ostatnim krokiem po włamaniu do systemu, w którym prowadzona będzie ukryta kradzież danych lub infiltracja,
8) keylogger – odczytuje i zapisuje wszystkie naciśnięcia klawiszy przez użytkownika. Dzięki temu adresy, kody, cenne informacje mogą odstać się w niepowołane ręce.

§ 3.

1. Profilaktyka i ochrona przed złośliwym oprogramowaniem obejmuje w szczególności:
   1) instalację, stosowanie i regularne uaktualnienia oprogramowania antywirusowego (wykrywającego i naprawczego),
   2) uświadamianie pracowników w zakresie bezpieczeństwa informacji oraz właściwych mechanizmach kontroli dostępu oraz zarządzania zmianami,
   3) stałe monitorowanie komunikatów pochodzących z zainstalowanego oprogramowania antywirusowego,
   4) zakaz korzystania z nieautoryzowanego oprogramowania,
   5) zakaz korzystania z sieci Internet bez aktywnej ochrony oprogramowaniem antywirusowym,
   6) sprawdzanie (skanowanie) oprogramowaniem antywirusowym komputerów i nośników służących do przetwarzania informacji, w tym tych otrzymywanych spoza Szkoły oraz wiadomości elektronicznych,
   7) korzystanie z list dyskusyjnych i sprawdzanie stron internetowych zamieszczających informacje o złośliwym oprogramowaniu,
   8) tworzenie kopii zapasowych.
2. Za stosowanie elementów profilaktyki i ochrony przed złośliwym oprogramowaniem, o których mowa w ust. 1 pkt 1, 6, 7 i 8 odpowiada informatyk, za stosowanie elementu, o którym mowa w ust. 1 pkt 2 odpowiada Dyrektor, a za stosowanie elementu, o którym mowa w ust. 1 pkt 3, 4 i 5 odpowiadają wszyscy pracownicy Szkoły.

§ 4.

W przypadku, gdy ochrona przed złośliwym oprogramowaniem, o której mowa w § 3 ust. 1 jest niewystarczająca, użytkownik zawiadamia o tym fakcie informatyka.

§ 5.

Szczególną uwagę należy zwracać na ochronę przed wprowadzeniem złośliwego oprogramowania w trakcie konserwacji lub wykonywania procedur awaryjnych, kiedy możliwe jest obejście normalnych mechanizmów ochrony przed złośliwym oprogramowaniem.

§ 6.

Nadzór nad realizacją „Procedury” sprawuje Dyrektor.

Załącznik nr 13 do zarządzenia nr 206/2015/2016 – „Procedura korzystania ze środków wymiany informacji”

PROCEDURA KORZYSTANIA ZE ŚRODKÓW WYMIANY INFORMACJI

§ 1.

1. „Procedura korzystania ze środków wymiany informacji”, zwana w dalszej części „Procedurą”, określa zabezpieczenia, które należy stosować w przypadku korzystania ze środków wymiany informacji w Szkole Podstawowej z Oddziałami Integracyjnymi nr 1 im. Janusza Korczaka w Rybniku.
2. Ilekroć w „Procedurze” mowa o:
   1) Dyrektorze – należy przez to rozumieć Dyrektora Szkoły Podstawowej z Oddziałami Integracyjnymi nr 1 im. Janusza Korczaka w Rybniku lub osobę zastępującą,
   2) informatyku – należy przez to rozumieć pracownika Szkoły Podstawowej z Oddziałami Integracyjnymi nr 1 im. Janusza Korczaka w Rybniku, wykonawcę lub użytkownika reprezentującego stronę trzecią, który czuwa nad sprawnym i ciągłym działaniem systemu teleinformatycznego,
   3) Szkole – należy przez to rozumieć Szkołę Podstawową z Oddziałami Integracyjnymi nr 1 im. Janusza Korczaka w Rybniku.

§ 2.

Środki wymiany informacji to poczta elektroniczna, telefon, faks.

§ 3.

Zabezpieczenia stosowane w przypadku wymiany informacji przy użyciu środków komunikacji elektronicznej obejmują w szczególności:

1) ochronę wymienianej informacji przed przechwyceniem, kopiowaniem, modyfikacją, błędnym rutingiem i zniszczeniem,
2) wykrywanie i ochronę przed złośliwym oprogramowaniem, które może być przesłane za pomocą środków komunikacji elektronicznej,
3) zobowiązanie pracowników oraz wykonawców i użytkowników reprezentujących stronę trzecią do niedziałania na szkodę Szkoły z wykorzystaniem środków komunikacji elektronicznej,
4) korzystanie z technik kryptograficznych.

§ 4.

1. Pracownik Szkoły, który korzysta z poczty elektronicznej powinien przestrzegać następujących zasad:
   1) zwracać szczególną uwagę na poprawność adresu poczty elektronicznej adresata,

2) przesyłać informacje zgodnie z uprawnieniami adresatów do korzystania z określonego typu informacji,
3) nie uruchamiać wykonywalnych załączników dołączonych do wiadomości przesyłanych pocztą elektroniczną. W takim przypadku uzgodnić postępowanie z informatykiem,
4) nie rozsyłać informacji stanowiących zagrożenie dla systemu teleinformatycznego oraz tzw. łańcuszków szczęścia,
5) okresowo przeglądać zawartość poczty elektronicznej i kasować niepotrzebne wiadomości.

2. Jeżeli istotne jest potwierdzenie otrzymania przez adresata przesyłki, pracownik Szkoły powinien skorzystać, o ile jest to technicznie możliwe, z opcji systemu poczty elektronicznej informującej o dostarczeniu i otwarciu dokumentu lub powinien zawrzeć w treści wiadomości prośbę o potwierdzenie otrzymania i zapoznania się z informacją.
3. W przypadku przesyłania pocztą elektroniczną danych osobowych powinny zostać zastosowane środki ochrony kryptograficznej.

§ 5.

Pracownik Szkoły, który korzysta z faksu powinien zwracać uwagę w szczególności na problemy związane z:

– nieautoryzowanym dostępem do wbudowanych pamięci w celu odzyskania wiadomości,
– rozmyślnym lub przypadkowym programowaniem faksów w taki sposób, aby wysyłały wiadomości pod określone numery,
– wysyłaniem dokumentów lub wiadomości pod zły numer w wyniku pomyłki w wybieraniu numeru lub użycia niewłaściwego numeru z pamięci urządzenia.

§ 6.

1. Pracownik Szkoły, który prowadzi rozmowę telefoniczną powinien zwracać uwagę na możliwość podsłuchania lub przechwycenia rozmowy telefonicznej przez:
   1) osoby znajdujące się w bezpośrednim sąsiedztwie, gdy są używane telefony komórkowe,
   2) zastosowanie różnych form podsłuchu,
   3) osoby znajdujące się po stronie odbiorcy.
2. Pozostawianie w automatycznych sekretarkach wiadomości zawierających dane osobowe jest zabronione, ponieważ mogą zostać odsłuchane przez nieuprawnione osoby, zapisane w publicznych systemach lub zapisane niewłaściwie w wyniku pomyłki w wybieraniu numeru.

§ 7.

Pozostawianie w oprogramowaniu służącym do przetwarzania informacji osobistych informacji, które mogłyby być gromadzone w celu nieautoryzowanego użycia jest zabronione.

§ 8.

Pracownik Szkoły, który korzysta z faksu, drukarki, kopiarki powinien być świadomym, że urządzenia te wyposażone są w podręczną pamięć, w której przechowują strony na wypadek błędów transmisji lub braku papieru, a drukują je zaraz po usunięciu błędu.

§ 9.

Nadzór nad realizacją „Procedury" sprawuje Dyrektor.

Załącznik nr 14 do zarządzenia nr 206/2015/2016 – „Procedura zarządzania nośnikami”

PROCEDURA ZARZĄDZANIA NOŚNIKAMI

§ 1.

1. „Procedura zarządzania nośnikami”, zwana w dalszej części „Procedurą”, określa zasady użytkowania, przechowywania, przekazywania i niszczenia nośników służących do przetwarzania informacji w Szkole Podstawowej z Oddziałami Integracyjnymi nr 1 im. Janusza Korczaka w Rybniku.
2. Ilekroć w „Procedurze” mowa o:
   1) Dyrektorze – należy przez to rozumieć Dyrektora Szkoły Podstawowej z Oddziałami Integracyjnymi nr 1 im. Janusza Korczaka w Rybniku lub osobę zastępującą,
   2) informatyku – należy przez to rozumieć pracownika Szkoły Podstawowej z Oddziałami Integracyjnymi nr 1 im. Janusza Korczaka w Rybniku, wykonawcę lub użytkownika reprezentującego stronę trzecią, który czuwa nad sprawnym i ciągłym działaniem systemu teleinformatycznego,
   3) nośnikach – należy przez to rozumieć taśmę, dysk, pamięć typu flash, wyjmowany dysk twardy oraz płytę CD lub DVD służące do przetwarzania informacji.
   4) Szkole – należy przez to rozumieć Szkołę Podstawową z Oddziałami Integracyjnymi nr 1 im. Janusza Korczaka w Rybniku.

§ 2.

1. Użytkowanie nośników wymaga pisemnej zgody, o której mowa w § 28 zarządzenia nr 206/2015/2016.
2. Użytkowanie nośników do innych celów niż cele służbowe jest zabronione.

§ 3.

1.	*dane niepodlegające udostępnianiu – art. 5 ustawy z dnia 6 września 2001 roku o dostępie do informacji publicznej*	
2.	*dane niepodlegające udostępnianiu – art. 5 ustawy z dnia 6 września 2001 roku o dostępie do informacji publicznej*	

3. Nośniki użyte do przetwarzania danych osobowych mogą być wykorzystywane do innych celów wyłącznie po skasowaniu danych osobowych lub nadpisaniu za pomocą technik uniemożliwiających ich odtworzenie. Nie dopuszcza się standardowego formatowania.

§ 4.

[redacted]	*dane niepodlegające udostępnianiu – art. 5 ustawy z dnia 6 września 2001 roku o dostępie do informacji publicznej*	[redacted]

§ 5.

Nośniki należy zabezpieczać przed dostępem osób nieuprawnionych, nieautoryzowaną modyfikacją i zniszczeniem.

§ 6.

1. [redacted]	*dane niepodlegające udostępnianiu – art. 5 ustawy z dnia 6 września 2001 roku o dostępie do informacji publicznej*	[redacted]

2. Nośniki należy przechowywać zgodnie z zaleceniami producenta.

§ 7.

1. W trakcie transportu nośników należy chronić zawartość przed fizycznym uszkodzeniem, wpływem temperatury, wilgotności czy pola elektromagnetycznego, które mogą pogorszyć skuteczność odtworzenia informacji z nośników, poprzez opakowanie zgodne z zaleceniami producenta.

2. [redacted]	*dane niepodlegające udostępnianiu – art. 5 ustawy z dnia 6 września 2001 roku o dostępie do informacji publicznej*	[redacted]

§ 8.

W przypadku użytkowania nośników poza budynkami Szkoły należy postępować zgodnie z „Procedurą przetwarzania mobilnego”.

§ 9.

W przypadku przekazania nośników do ponownego użycia, należy skasować zapisane na nośnikach informacje i licencjonowane oprogramowanie służące do przetwarzania informacji, do których przyszły użytkownik nie ma dostępu, a w przypadku zbycia lub zniszczenia – wszystkie informacje i licencjonowane oprogramowanie służące do przetwarzania informacji podlegają kasowaniu lub nadpisaniu za pomocą technik uniemożliwiających ich odtworzenie. Nie dopuszcza się standardowego formatowania.

§ 10.

1. Nośniki należy likwidować poprzez spopielenie, pocięcie lub uszkodzenie w taki sposób, aby nie było możliwe ponowne wykorzystanie nośników.
2. W trakcie gromadzenia nośników do niszczenia należy wziąć pod uwagę efekt agregacji, który może spowodować, że duża ilość niewrażliwych informacji stanie się wrażliwa.

§ 11.

W przypadku brakowania dokumentów tradycyjnych lub przekazania ich do Archiwum Państwowego należy odpowiadające im zapisy na nośnikach usunąć lub zabezpieczyć przed ich odczytaniem.

§ 12.

Nadzór nad realizacją „Procedury” sprawuje Dyrektor.

Załącznik nr 15 do zarządzenia nr 206/2015/2016 – „Procedura zarządzania incydentami związanymi z bezpieczeństwem informacji”

PROCEDURA ZARZĄDZANIA INCYDENTAMI ZWIĄZANYMI Z BEZPIECZEŃSTWEM INFORMACJI

§ 1.

1. „Procedura zarządzania incydentami związanymi z bezpieczeństwem informacji”, zwana w dalszej części „Procedurą”, określa zasady zgłaszania incydentów związanych z bezpieczeństwem informacji i słabości w systemie teleinformatycznym lub usłudze oraz zarządzania incydentami związanymi z bezpieczeństwem informacji i udoskonaleniami w Szkole Podstawowej z Oddziałami Integracyjnymi nr 1 im. Janusza Korczaka w Rybniku.
2. Ilekroć w „Procedurze” jest mowa o:
   1) Dyrektorze – należy przez to rozumieć Dyrektora Szkoły Podstawowej z Oddziałami Integracyjnymi nr 1 im. Janusza Korczaka w Rybniku lub osobę zastępującą,
   2) informatyku – należy przez to rozumieć pracownika Szkoły Podstawowej z Oddziałami Integracyjnymi nr 1 im. Janusza Korczaka w Rybniku, wykonawcę lub użytkownika reprezentującego stronę trzecią, który czuwa nad sprawnym i ciągłym działaniem systemu teleinformatycznego,
   3) Szkole – należy przez to rozumieć Szkołę Podstawową z Oddziałami Integracyjnymi nr 1 im. Janusza Korczaka w Rybniku.

§ 2.

1.	*dane niepodlegające udostępnianiu – art. 5 ustawy z dnia 6 września 2001 roku o dostępie do informacji publicznej*	
2.	*dane niepodlegające udostępnianiu – art. 5 ustawy z dnia 6 września 2001 roku o dostępie do informacji publicznej*	

§ 3.

1.	*dane niepodlegające udostępnianiu*	

	– art. 5 ustawy z dnia 6 września 2001 roku o dostępie do informacji publicznej	
2.	*dane niepodlegające udostępnianiu – art. 5 ustawy z dnia 6 września 2001 roku o dostępie do informacji publicznej*	
3.	*dane niepodlegające udostępnianiu – art. 5 ustawy z dnia 6 września 2001 roku o dostępie do informacji publicznej*	
4.	*dane niepodlegające udostępnianiu – art. 5 ustawy z dnia 6 września 2001 roku o dostępie do informacji publicznej*	

§ 4.

1.	*dane niepodlegające udostępnianiu – art. 5 ustawy z dnia 6 września 2001 roku o dostępie do informacji publicznej*	
2.	*dane niepodlegające udostępnianiu – art. 5 ustawy z dnia 6 września 2001 roku o dostępie do informacji publicznej*	

§ 5.

1.	*dane niepodlegające udostępnianiu – art. 5 ustawy z dnia 6*	

	września 2001 roku o dostępie do informacji publicznej	
2.	*dane niepodlegające udostępnianiu – art. 5 ustawy z dnia 6 września 2001 roku o dostępie do informacji publicznej*	
3.	*dane niepodlegające udostępnianiu – art. 5 ustawy z dnia 6 września 2001 roku o dostępie do informacji publicznej*	

§ 6.

1.	*dane niepodlegające udostępnianiu – art. 5 ustawy z dnia 6 września 2001 roku o dostępie do informacji publicznej*	
2.	*dane niepodlegające udostępnianiu – art. 5 ustawy z dnia 6 września 2001 roku o dostępie do informacji publicznej*	

§ 7.

	dane niepodlegające udostępnianiu – art. 5 ustawy z dnia 6 września 2001 roku o dostępie do informacji publicznej	

§ 8.

	dane niepodlegające udostępnianiu	

	– art. 5 ustawy z dnia 6 września 2001 roku o dostępie do informacji publicznej	

§ 9.

1.	*dane niepodlegające udostępnianiu – art. 5 ustawy z dnia 6 września 2001 roku o dostępie do informacji publicznej*	
2.	*dane niepodlegające udostępnianiu – art. 5 ustawy z dnia 6 września 2001 roku o dostępie do informacji publicznej*	
3.	*dane niepodlegające udostępnianiu – art. 5 ustawy z dnia 6 września 2001 roku o dostępie do informacji publicznej*	

§ 10.

1.	*dane niepodlegające udostępnianiu – art. 5 ustawy z dnia 6 września 2001 roku o dostępie do informacji publicznej*	
2.	*dane niepodlegające udostępnianiu – art. 5 ustawy z dnia 6 września 2001 roku o dostępie do informacji publicznej*	
3.	*dane niepodlegające udostępnianiu – art. 5 ustawy z dnia 6*	

	września 2001 roku o dostępie do informacji publicznej	

§ 11.

1.	*dane niepodlegające udostępnianiu – art. 5 ustawy z dnia 6 września 2001 roku o dostępie do informacji publicznej*	
2.	*dane niepodlegające udostępnianiu – art. 5 ustawy z dnia 6 września 2001 roku o dostępie do informacji publicznej*	

§ 12.

	dane niepodlegające udostępnianiu – art. 5 ustawy z dnia 6 września 2001 roku o dostępie do informacji publicznej	

§ 13.

1.	*dane niepodlegające udostępnianiu – art. 5 ustawy z dnia 6 września 2001 roku o dostępie do informacji publicznej*	
2.	*dane niepodlegające udostępnianiu – art. 5 ustawy z dnia 6 września 2001 roku o dostępie do informacji publicznej*	

§ 14.

1.	*dane niepodlegające udostępnianiu – art. 5 ustawy z dnia 6 września 2001 roku o dostępie do informacji publicznej*	
2.	*dane niepodlegające udostępnianiu – art. 5 ustawy z dnia 6 września 2001 roku o dostępie do informacji publicznej*	

§ 15.

	dane niepodlegające udostępnianiu – art. 5 ustawy z dnia 6 września 2001 roku o dostępie do informacji publicznej	

§ 16.

1.	*dane niepodlegające udostępnianiu – art. 5 ustawy z dnia 6 września 2001 roku o dostępie do informacji publicznej*	
2.	*dane niepodlegające udostępnianiu – art. 5 ustawy z dnia 6 września 2001 roku o dostępie do informacji publicznej*	

§ 17.

1.	*dane niepodlegające udostępnianiu – art. 5 ustawy z dnia 6 września 2001 roku*	

	o dostępie do informacji publicznej	
2.	*dane niepodlegające udostępnianiu – art. 5 ustawy z dnia 6 września 2001 roku o dostępie do informacji publicznej*	
3.	*dane niepodlegające udostępnianiu – art. 5 ustawy z dnia 6 września 2001 roku o dostępie do informacji publicznej*	

§ 18.

1.	*dane niepodlegające udostępnianiu – art. 5 ustawy z dnia 6 września 2001 roku o dostępie do informacji publicznej*	
2.	*dane niepodlegające udostępnianiu – art. 5 ustawy z dnia 6 września 2001 roku o dostępie do informacji publicznej*	

§ 19.

	dane niepodlegające udostępnianiu – art. 5 ustawy z dnia 6 września 2001 roku o dostępie do informacji publicznej	

§ 20.

	dane niepodlegające udostępnianiu – art. 5 ustawy z dnia 6	

września 2001 roku
o dostępie do informacji
publicznej

§ 21.

Nadzór nad realizacją „Procedury” sprawuje Dyrektor.

Załącznik nr 16 do zarządzenia nr 206/2015/2016 – „Plany ciągłości działania”

PLANY CIĄGŁOŚCI DZIAŁANIA

§ 1.

1. „Plany ciągłości działania” określają sposoby przeciwdziałania przerwom w funkcjonowaniu Szkole Podstawowej z Oddziałami Integracyjnymi nr 1 im. Janusza Korczaka w Rybniku.
2. Ilekroć w „Planach” jest mowa o:
   1) Dyrektorze – należy przez to rozumieć Dyrektora Szkoły Podstawowej z Oddziałami Integracyjnymi nr 1 im. Janusza Korczaka w Rybniku lub osobę zastępującą,
   2) informatyku – należy przez to rozumieć pracownika Szkoły Podstawowej z Oddziałami Integracyjnymi nr 1 im. Janusza Korczaka w Rybniku, wykonawcę lub użytkownika reprezentującego stronę trzecią, który czuwa nad sprawnym i ciągłym działaniem systemu teleinformatycznego,
   3) Szkole – należy przez to rozumieć Szkołę Podstawową z Oddziałami Integracyjnymi nr 1 im. Janusza Korczaka w Rybniku.

§ 2.

[redacted]	*dane niepodlegające udostępnianiu – art. 5 ustawy z dnia 6 września 2001 roku o dostępie do informacji publicznej*	[redacted]

§ 3.

[redacted]	*dane niepodlegające udostępnianiu – art. 5 ustawy z dnia 6 września 2001 roku o dostępie do informacji publicznej*	[redacted]

§ 4.

[redacted]	*dane niepodlegające udostępnianiu – art. 5 ustawy z dnia 6 września 2001 roku o dostępie do informacji*	[redacted]

	publicznej	

§ 5.

	dane niepodlegające udostępnianiu – art. 5 ustawy z dnia 6 września 2001 roku o dostępie do informacji publicznej	

§ 6.

1.	*dane niepodlegające udostępnianiu – art. 5 ustawy z dnia 6 września 2001 roku o dostępie do informacji publicznej*	
2.	*dane niepodlegające udostępnianiu – art. 5 ustawy z dnia 6 września 2001 roku o dostępie do informacji publicznej*	
3.	*dane niepodlegające udostępnianiu – art. 5 ustawy z dnia 6 września 2001 roku o dostępie do informacji publicznej*	

§ 7.

	dane niepodlegające udostępnianiu – art. 5 ustawy z dnia 6 września 2001 roku o dostępie do informacji publicznej	

§ 8.

	dane niepodlegające udostępnianiu – art. 5 ustawy z dnia 6 września 2001 roku o dostępie do informacji publicznej	

§ 9.

	dane niepodlegające udostępnianiu – art. 5 ustawy z dnia 6 września 2001 roku o dostępie do informacji publicznej	

§ 10.

	dane niepodlegające udostępnianiu – art. 5 ustawy z dnia 6 września 2001 roku o dostępie do informacji publicznej	

§ 11.

1.	*dane niepodlegające udostępnianiu – art. 5 ustawy z dnia 6 września 2001 roku o dostępie do informacji publicznej*	
2.	*dane niepodlegające udostępnianiu – art. 5 ustawy z dnia 6 września 2001 roku o dostępie do informacji publicznej*	

§ 12.

	dane niepodlegające udostępnianiu	

	– art. 5 ustawy z dnia 6 września 2001 roku o dostępie do informacji publicznej	

§ 13.

	dane niepodlegające udostępnianiu – art. 5 ustawy z dnia 6 września 2001 roku o dostępie do informacji publicznej	

§ 14.

Nadzór nad realizacją „Planów ciągłości działania” sprawuje Dyrektor.

Załącznik nr 17 do zarządzenia nr 206/2015/2016 – „Polityka bezpieczeństwa”

POLITYKA BEZPIECZEŃSTWA

§ 1.

„Polityka bezpieczeństwa” określa wykaz budynków, pomieszczeń lub części pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe, wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych, opis struktury zbiorów danych osobowych wskazujących zawartość poszczególnych pól informacyjnych i powiązania między nimi, sposób przepływu danych pomiędzy poszczególnymi systemami oraz środki techniczne i organizacyjne niezbędne do zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych w Szkole Podstawowej z Oddziałami Integracyjnymi nr 1 im. Janusza Korczaka w Rybniku.

§ 2.

Wykaz budynków, pomieszczeń lub części pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe stanowi załącznik nr 1 do „Polityki bezpieczeństwa”.

§ 3.

Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych stanowi załącznik nr 2 do „Polityki bezpieczeństwa”.

§ 4.

Opis struktury zbiorów danych osobowych wskazujących zawartość poszczególnych pól informacyjnych i powiązania między nimi stanowi załącznik nr 3 do „Polityki bezpieczeństwa”.

§ 5.

Sposób przepływu danych pomiędzy poszczególnymi systemami stanowi załącznik nr 4 do „Polityki bezpieczeństwa”.

§ 6.

Środki techniczne i organizacyjne niezbędne do zapewnienia poufności przetwarzanych danych osobowych określają:

1) „Procedura kontroli dostępu”,
2) „Procedura rozpoczęcia, zawieszenia i zakończenia pracy na komputerze”,
3) „Procedura ochrony przed złośliwym oprogramowaniem”.

§ 7.

Środki techniczne i organizacyjne niezbędne do zapewnienia integralności przetwarzanych danych osobowych określają:

1) „Procedura kontroli dostępu”,
2) „Procedura wykonywania przeglądów, konserwacji i napraw komputerów, nośników i oprogramowania służącego do przetwarzania informacji”,
3) „Procedura ochrony przed złośliwym oprogramowaniem”,
4) „Procedura korzystania ze środków wymiany informacji”.

§ 8.

Środki techniczne i organizacyjne niezbędne do zapewnienia rozliczalności przetwarzanych danych osobowych określa „Procedura kontroli dostępu”.

§ 9.

Nadzór nad realizacją „Polityki bezpieczeństwa” sprawuje Dyrektor Szkoły Podstawowej z Oddziałami Integracyjnymi nr 1 im. Janusza Korczaka w Rybniku.

Załącznik nr 1 do „Polityki bezpieczeństwa” – wykaz budynków, pomieszczeń lub części pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe

WYKAZ BUDYNKÓW, POMIESZCZEŃ LUB CZĘŚCI POMIESZCZEŃ TWORZĄCYCH OBSZAR, W KTÓRYM PRZETWARZANE SĄ DANE OSOBOWE

Budynek tworzący obszar, w którym przetwarzane są dane osobowe: budynki Szkoły Podstawowej z Oddziałami Integracyjnymi nr 1 im. Janusza Korczaka w Rybniku przy ul. Bolesława Chrobrego 29.

[redacted]	*dane niepodlegające udostępnianiu – art. 5 ustawy z dnia 6 września 2001 roku o dostępie do informacji publicznej*	[redacted]

Załącznik nr 2 do „Polityki bezpieczeństwa” – wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych

WYKAZ ZBIORÓW DANYCH OSOBOWYCH WRAZ ZE WSKAZANIEM PROGRAMÓW ZASTOSOWANYCH DO PRZETWARZANIA TYCH DANYCH

Wykaz zbiorów danych osobowych przetwarzanych w systemach informatycznych i wykaz programów zastosowanych do ich przetwarzania:

Zbiór danych osobowych	Program zastosowany do ich przetwarzania
Księga ewidencji dzieci	
Zgłoszenie do obwodowej szkoły podstawowej	Nabór Optivum
Wniosek o przyjęcie kandydata do szkoły podstawowej	Nabór Optivum
Księga uczniów	
Dziennik lekcyjny	
Dziennik innych zajęć	
Dziennik zajęć w świetlicy	
Dziennik zajęć rewalidacyjno-wychowawczych	
Arkusz ocen ucznia	
Świadectwo szkolne	
Świadectwo ukończenia szkoły	
Ewidencja wydanych świadectw ukończenia szkoły	
Wynik sprawdzianu	Hermes
Zaświadczenie o szczegółowych wynikach sprawdzianu	
Ewidencja wydanych zaświadczeń o szczegółowych wynikach sprawdzianu	
Legitymacja szkolna	
Ewidencja wydanych legitymacji szkolnych	
Karta rowerowa	
Ewidencja wydanych kart rowerowych	
Protokolarz Rady Pedagogicznej	Edytor tekstu
Pomoc psychologiczno-pedagogiczna	Edytor tekstu
Dziennik (pedagoga)	
Wniosek o przyznanie wyprawki szkolnej	
Deklaracja rodziców	Edytor tekstu, PEFS 2007
Wniosek o przyjęcie do świetlicy szkolnej	
Decyzja w sprawie zwolnienia z zajęć lekcyjnych	
Karta biblioteczna	MOL Optivum
Lista obecności pracowników	Edytor tekstu

Ewidencja wyjść pracowników	Edytor tekstu
Kandydaci do pracy	
Akta osobowe	
Kadry	Kadry Optivum, PEFS 2007
Lista płac	
Wniosek o przyznanie świadczenia z zakładowego funduszu świadczeń socjalnych	Edytor tekstu
Protokół z przebiegu prac komisji kwalifikacyjnej	Edytor tekstu
Zaświadczenie o uzyskaniu akceptacji komisji kwalifikacyjnej	Edytor tekstu
Akt nadania stopnia awansu zawodowego nauczyciela	Edytor tekstu
Protokół powypadkowy ucznia	Edytor tekstu
Rejestr wypadków uczniów	Edytor tekstu
Protokół ustalenia okoliczności i przyczyn wypadku przy pracy	Edytor tekstu
Rejestr wypadków pracowników	Edytor tekstu
System informacji oświatowej	SIO
Arkusz organizacji pracy szkoły	Arkusz Optivum
Dziennik korespondencji	Edytor tekstu
Rejestr skarg i wniosków	Edytor tekstu
Rejestr wniosków o udostępnienie informacji publicznej	Edytor tekstu
Karta wycieczki (imprezy)	Edytor tekstu
Orzeczenie lekarskie	

Załącznik nr 3 do „Polityki bezpieczeństwa” – opis struktury zbiorów danych osobowych wskazujących zawartość poszczególnych pól informacyjnych i powiązania między nimi

OPIS STRUKTURY ZBIORÓW DANYCH OSOBOWYCH WSKAZUJACYCH ZAWARTOŚĆ POSZCZEGÓLNYCH PÓL INFORMACYJNYCH I POWIĄZANIA MIĘDZY NIMI

Zbiór danych „księga ewidencji dzieci” zawiera następujące pola:

- imię (imiona) dziecka,
- nazwisko dziecka,
- data urodzenia dziecka,
- miejsce urodzenia dziecka,
- numer PESEL dziecka lub seria i numer paszportu lub innego dokumentu potwierdzającego tożsamość,
- adres zamieszkania dziecka,
- imiona rodziców dziecka,
- nazwiska rodziców dziecka,
- adresy zamieszkania rodziców dziecka, jeżeli są inne niż adres zamieszkania dziecka,
- informacja o przedszkolu lub innej formie wychowania przedszkolnego, w którym dziecko spełnia obowiązek rocznego przygotowania przedszkolnego,
- informacja o spełnianiu przez dziecko obowiązku szkolnego,
- informacja o odroczeniu rozpoczęcia spełniania przez dziecko obowiązku szkolnego.

Zbiór danych „zgłoszenie do obwodowej szkoły podstawowej” zawiera następujące pola:

- nazwa szkoły obwodowej kandydata,
- adres szkoły obwodowej kandydata,
- imię kandydata,
- nazwisko kandydata,
- data urodzenia kandydata,
- numer ewidencyjny PESEL kandydata lub rodzaj, seria i numer innego dokumentu tożsamości,
- adres zamieszkania kandydata,
- informacje na temat orzeczenia o potrzebie kształcenia specjalnego kandydata,
- imiona rodziców (opiekunów prawnych) kandydata,
- nazwiska rodziców (opiekunów prawnych) kandydata,
- adresy zamieszkania rodziców (opiekunów prawnych) kandydata,
- numery telefonów rodziców (opiekunów prawnych) kandydata,
- informacje dodatkowe o kandydacie przekazywane dobrowolnie przez rodziców (opiekunów prawnych) kandydata.

Zbiór danych „wniosek o przyjęcie kandydata do szkoły podstawowej” zawiera następujące pola:

- imię kandydata,
- nazwisko kandydata,
- data urodzenia kandydata,
- numer ewidencyjny PESEL kandydata lub rodzaj, seria i numer innego dokumentu tożsamości,
- informacja na temat wybranych jednostek i oddziałów według kolejności preferencji,
- nazwa szkoły obwodowej kandydata,
- adres szkoły obwodowej kandydata,
- adres zamieszkania kandydata,
- informacja na temat orzeczenia o potrzebie kształcenia specjalnego kandydata,
- numer PESEL rodzeństwa kandydata, jeżeli kandydują do tej samej szkoły,
- imiona rodziców (opiekunów prawnych) kandydata,
- nazwiska rodziców (opiekunów prawnych) kandydata,
- telefony kontaktowe rodziców (opiekunów prawnych) kandydata,
- adres poczty elektronicznej rodziców (opiekunów prawnych) kandydata,
- informacja, czy kandydat uczęszcza do przedszkola znajdującego się w obwodzie szkoły podstawowej prowadzącej oddział wskazany na pierwszym miejscu listy preferencji,
- informacja, czy rodzeństwo kandydata kandyduje do tej samej szkoły podstawowej,
- informacja, czy rodzeństwo kandydata jest uczniem szkoły podstawowej prowadzącej oddział wskazany na pierwszym miejscu listy preferencji,
- informacja na temat wielodzietności rodziny kandydata,
- informacja na temat niepełnosprawności kandydata,
- informacja na temat niepełnosprawności jednego rodzica (opiekuna prawnego) kandydata,
- informacja na temat niepełnosprawności obojga rodziców (opiekunów prawnych) kandydata,
- informacja na temat niepełnosprawności rodzeństwa kandydata,
- informacja na temat samotnego wychowywania kandydata w rodzinie,
- informacja na temat objęcia kandydata piecza zastępczą,
- informacje dodatkowe o kandydacie przekazywane dobrowolnie przez rodziców (opiekunów prawnych) kandydata.

Zbiór danych „księga uczniów” zawiera następujące pola:

- imię (imiona) ucznia,
- nazwisko ucznia,
- data urodzenia ucznia,
- miejsce urodzenia ucznia,
- numer ewidencyjny PESEL ucznia lub seria i numer paszportu lub innego dokumentu

potwierdzającego tożsamość,
- adres zamieszkania ucznia,
- imiona rodziców ucznia,
- nazwiska rodziców ucznia,
- adresy zamieszkania rodziców (prawnych opiekunów) ucznia, jeżeli są różne od adresu zamieszkania ucznia,
- data rozpoczęcia przez ucznia nauki w danej szkole,
- oddział, do którego przyjęto ucznia,
- data ukończenia szkoły przez ucznia,
- data i przyczyna opuszczenia szkoły przez ucznia.

Zbiór danych „dziennik lekcyjny” zawiera następujące pola:
- imię ucznia,
- nazwisko ucznia,
- data urodzenia ucznia,
- miejsce urodzenia ucznia,
- adres zamieszkania ucznia,
- imiona rodziców ucznia,
- nazwiska rodziców ucznia,
- adresy zamieszkania rodziców ucznia, jeżeli są różne niż adres zamieszkania ucznia,
- adresy poczty elektronicznej rodziców dziecka, jeżeli posiadają,
- numery telefonów rodziców dziecka, jeżeli posiadają,
- tygodniowy plan zajęć edukacyjnych,
- imiona nauczycieli prowadzących poszczególne zajęcia edukacyjne,
- nazwiska nauczycieli prowadzących poszczególne zajęcia edukacyjne,
- obecność ucznia na poszczególnych zajęciach edukacyjnych,
- tematy zajęć edukacyjnych,
- oceny uzyskane przez ucznia z poszczególnych zajęć edukacyjnych.

Zbiór danych „dziennik innych zajęć” zawiera następujące pola:
- imię ucznia,
- nazwisko ucznia,
- oddział, do którego uczęszcza uczeń,
- adresy poczty elektronicznej rodziców dziecka, jeżeli posiadają,
- numery telefonów rodziców dziecka, jeżeli posiadają,
- indywidualny program pracy z uczniem lub program pracy grupy,
- tygodniowy plan zajęć,
- data, czas trwania i tematy przeprowadzonych zajęć,
- ocena postępów,
- wnioski dotyczące dalszej pracy,

– obecność ucznia na zajęciach.

Zbiór danych „dziennik zajęć w świetlicy” zawiera następujące pola:
– plan pracy świetlicy na dany rok szkolny,
– imię ucznia korzystającego ze świetlicy,
– nazwisko ucznia korzystającego ze świetlicy,
– oddział, do której uczęszcza uczeń korzystający ze świetlicy,
– tematy przeprowadzonych zajęć,
– obecność ucznia korzystającego ze świetlicy na poszczególnych godzinach zajęć.

Zbiór danych „dziennik zajęć rewalidacyjno-wychowawczych” zawiera następujące pola:
– imię ucznia,
– nazwisko ucznia,
– data urodzenia ucznia,
– miejsce urodzenia ucznia,
– adres zamieszkania ucznia,
– imiona rodziców ucznia,
– nazwiska rodziców ucznia,
– adresy zamieszkania rodziców ucznia, jeżeli są różne niż adres zamieszkania ucznia,
– adresy poczty elektronicznej rodziców dziecka, jeżeli posiadają,
– numery telefonów rodziców dziecka, jeżeli posiadają,
– obecność ucznia na zajęciach,
– indywidualny program zajęć,
– opis przebiegu zajęć z każdym uczniem.

Zbiór danych „arkusz ocen ucznia” zawiera następujące pola:
– imię (imiona) ucznia,
– nazwisko ucznia,
– data urodzenia ucznia,
– miejsce urodzenia ucznia,
– numer ewidencyjny PESEL ucznia,
– adres zamieszkania ucznia,
– imiona i nazwiska rodziców (prawnych opiekunów),
– data przyjęcia do szkoły,
– data i przyczyna opuszczenia szkoły,
– informacja o wynikach nauczania i zachowania uzyskanych przez ucznia,
– informacja o wydaniu świadectwa ukończenia szkoły,
– informacja o wydaniu duplikatu świadectwa,
– informacja o udzieleniu zezwolenia na indywidualny program lub tok nauki,
– informacja o wydłużeniu etapu edukacyjnego,

– numer, pod którym uczeń wpisany jest do księgi uczniów.

Zbiór danych „świadectwo szkolne” zawiera następujące pola:
– imię (imiona) ucznia,
– nazwisko ucznia,
– data urodzenia ucznia,
– miejsce urodzenia ucznia,
– numer ewidencyjny PESEL ucznia,
– rok szkolny,
– klasa, do której uczęszczał uczeń,
– nazwa szkoły, do której uczęszczał uczeń,
– numer szkoły, do której uczęszczał uczeń,
– imię szkoły, do której uczęszczał uczeń,
– miejscowość położenia szkoły, do której uczęszczał uczeń,
– województwo położenia szkoły, do której uczęszczał uczeń,
– informacja na temat promocji ucznia do następnej klasy,
– miejsce wydania świadectwa szkolnego,
– data wydania świadectwa szkolnego,
– numer świadectwa szkolnego,
– wyniki klasyfikacji rocznej.

Zbiór danych „świadectwo ukończenia szkoły” zawiera następujące pola:
– imię (imiona) ucznia,
– nazwisko ucznia,
– data urodzenia ucznia,
– miejsce urodzenia ucznia,
– numer ewidencyjny PESEL ucznia,
– rok szkolny, w którym uczeń ukończył szkołę,
– nazwa szkoły, którą ukończył uczeń,
– numer szkoły, którą ukończył uczeń,
– imię szkoły, którą ukończył uczeń,
– miejscowość położenia szkoły, którą ukończył uczeń,
– województwo położenia szkoły, którą ukończył uczeń,
– miejsce wydania świadectwa ukończenia szkoły,
– data wydania świadectwa ukończenia szkoły,
– numer świadectwa ukończenia szkoły,
– wyniki klasyfikacji końcowej.

Zbiór danych „ewidencja wydanych świadectw ukończenia szkoły” zawiera następujące pola:
– imię (imiona) ucznia,

– nazwisko ucznia,
– numer ewidencyjny PESEL ucznia,
– numer wydanego świadectwa ukończenia szkoły,
– data odbioru świadectwa ukończenia szkoły.

Zbiór danych „wynik sprawdzianu” zawiera następujące pola:
– imię (imiona) ucznia,
– nazwisko ucznia,
– data urodzenia ucznia,
– numer ewidencyjny PESEL ucznia,
– miejsce urodzenia ucznia,
– nazwisko rodowe ucznia,
– płeć ucznia,
– dysfunkcja ucznia,
– dysleksja ucznia.

Zbiór danych „zaświadczenie o szczegółowych wynikach sprawdzianu” zawiera następujące pola:
– imię (imiona) ucznia,
– nazwisko ucznia,
– data urodzenia ucznia,
– miejsce urodzenia ucznia,
– numer ewidencyjny PESEL ucznia,
– wyniki uzyskane ze sprawdzianu przez ucznia,
– miejsce wydania zaświadczenia o szczegółowych wynikach sprawdzianu,
– data wydania zaświadczenia o szczegółowych wynikach sprawdzianu,
– kod zaświadczenia o szczegółowych wynikach sprawdzianu.

Zbiór danych „ewidencja wydanych zaświadczeń o szczegółowych wynikach sprawdzianu” zawiera następujące pola:
– imię (imiona) ucznia,
– nazwisko ucznia,
– numer ewidencyjny PESEL ucznia,
– numer wydanego zaświadczenia o szczegółowych wynikach sprawdzianu,
– data odbioru zaświadczenia o szczegółowych wynikach sprawdzianu.

Zbiór danych „legitymacja szkolna” zawiera następujące pola:
– imię (imiona) ucznia,
– nazwisko ucznia,
– numer ewidencyjny PESEL ucznia,

- adres zamieszkania ucznia,
- zdjęcie ucznia,
- data wydania legitymacji szkolnej,
- termin ważności legitymacji szkolnej.

Zbiór danych „ewidencja wydanych legitymacji szkolnych” zawiera następujące pola:
- imię (imiona) ucznia,
- nazwisko ucznia,
- numer ewidencyjny PESEL ucznia,
- numer wydanej legitymacji szkolnej,
- data odbioru legitymacji szkolnej.

Zbiór danych „karta rowerowa” zawiera następujące pola:
- imię (imiona) ucznia,
- nazwisko ucznia,
- data urodzenia ucznia,
- adres zamieszkania ucznia,
- zdjęcie ucznia,
- data wydania karty rowerowej,
- informacje na temat zmiany adresu zamieszkania ucznia,
- nazwa podmiotu wydającego kartę rowerową.

Zbiór danych „ewidencja wydanych kart rowerowych” zawiera następujące pola:
- imię (imiona) ucznia,
- nazwisko ucznia,
- numer wydanej karty rowerowej,
- data odbioru karty rowerowej.

Zbiór danych „protokolarz Rady Pedagogicznej” zawiera następujące pola:
- imię ucznia,
- nazwisko ucznia,
- klasa, do której uczęszcza uczeń,
- imię nauczyciela,
- nazwisko nauczyciela.

Zbiór danych „pomoc psychologiczno-pedagogiczna” zawiera następujące pola:
- imię ucznia,
- nazwisko ucznia,
- dysfunkcja ucznia,
- informacja o stanie zdrowia ucznia,

- data urodzenia ucznia,
- adres zamieszkania ucznia,
- klasa, do której uczęszcza uczeń,
- imiona rodziców (prawnych opiekunów) ucznia,
- nazwiska rodziców (prawnych opiekunów) ucznia,
- adresy zamieszkania rodziców (prawnych opiekunów) ucznia, jeżeli są różne niż adres zamieszkania ucznia,
- adresy poczty elektronicznej rodziców (prawnych opiekunów) dziecka, jeżeli posiadają,
- numery telefonów rodziców (prawnych opiekunów) dziecka, jeżeli posiadają,
- imię nauczyciela,
- nazwisko nauczyciela.

Zbiór danych „dziennik (pedagoga)" zawiera następujące pola:
- tygodniowy plan zajęć pedagoga,
- zajęcia i czynności przeprowadzone w poszczególnych dniach, w tym informacje o kontaktach z osobami i instytucjami, z którymi pedagog współdziała przy wykonywaniu swoich zadań,
- imię ucznia objętego różnymi formami pomocy,
- nazwisko ucznia objętego różnymi formami pomocy.

Zbiór danych „wniosek o przyznanie wyprawki szkolnej" zawiera następujące pola:
- imię ucznia,
- nazwisko ucznia,
- adres zamieszkania ucznia,
- imiona rodziców (prawnych opiekunów) ucznia,
- nazwiska rodziców (prawnych opiekunów) ucznia,
- wiek rodzeństwa,
- informacja o dochodach (w tym zaświadczenie lub oświadczenie o zarobkach, zaświadczenie o zasiłkach),
- informacja o potrzebie kształcenia specjalnego.

Zbiór danych „deklaracja rodziców" zawiera następujące pola:
- imię ucznia,
- nazwisko ucznia,
- numer ewidencyjny PESEL ucznia,
- adres zamieszkania ucznia,
- data urodzenia ucznia,
- miejsce urodzenia ucznia,
- klasa, do której uczęszcza ucznia,
- szkoła, do której uczęszcza ucznia,

- numery telefonów rodziców (prawnych opiekunów) ucznia,
- informacje na temat zgody rodziców (prawnych opiekunów) na uczestnictwo ucznia w projektach edukacyjnych itp.

Zbiór danych „wniosek o przyjęcie do świetlicy szkolnej” zawiera następujące pola:
- imię dziecka,
- nazwisko dziecka,
- klasa, do której uczęszcza dziecko,
- data urodzenia dziecka,
- adres zamieszkania dziecka,
- numery telefonów rodziców (opiekunów prawnych) dziecka,
- numery telefonów do pracy rodziców (opiekunów prawnych) dziecka,
- informacja, czy rodzice (opiekunowie prawni) są zatrudnieni czy nie,
- informacja na temat godzin pracy rodziców (opiekunów prawnych) dziecka w poszczególne dni tygodnia,
- ważne dla wychowawcy informacje dotyczące zdrowia i zachowania dziecka,
- informacja na temat godzin przebywania dziecka w świetlicy w poszczególne dni tygodnia,
- informacja, czy dziecko będzie wracać do domu samodzielnie czy nie,
- informacja na temat osób, które odbierają dziecko ze świetlicy.

Zbiór danych „decyzja w sprawie zwolnienia z zajęć lekcyjnych” zawiera następujące pola:
- imię ucznia,
- nazwisko ucznia,
- numer ewidencyjny PESEL ucznia,
- adres zamieszkania ucznia.

Zbiór danych „karta biblioteczna” zawiera następujące pola:
- imię wypożyczającego,
- nazwisko wypożyczającego.

Zbiór danych „lista obecności pracowników” zawiera następujące pola:
- imię pracownika,
- nazwisko pracownika,
- data,
- godzina przyjścia,
- godzina wyjścia,
- przyczyna nieobecności.

Zbiór danych „ewidencja wyjść pracowników” zawiera następujące pola:
- imię pracownika,
- nazwisko pracownika,
- data wyjścia,
- godzina wyjścia,
- godzina przyjścia,
- cel wyjścia.

Zbiór danych „kandydaci do pracy” zawiera następujące pola:
- imię kandydata,
- nazwisko kandydata,
- adres zamieszkania kandydata,
- informacje o wykształceniu kandydata,
- informacje o przebiegu zatrudnienia kandydata.

Zbiór danych „akta osobowe” zawiera następujące pola:
- imię (imiona) pracownika,
- nazwisko pracownika,
- nazwisko rodowe pracownika,
- imiona rodziców pracownika,
- nazwisko rodowe matki pracownika,
- data urodzenia pracownika,
- miejsce urodzenia pracownika,
- obywatelstwo pracownika,
- numer ewidencyjny PESEL pracownika,
- numer identyfikacji podatkowej NIP pracownika,
- adres zamieszkania pracownika,
- adres do korespondencji pracownika,
- telefon pracownika,
- wykształcenie pracownika,
- wykształcenie uzupełniające pracownika,
- przebieg dotychczasowego zatrudnienia,
- dodatkowe uprawnienia, umiejętności, zainteresowania pracownika,
- imię dziecka pracownika,
- nazwisko dziecka pracownika,
- data urodzenia dziecka pracownika,
- stosunek do powszechnego obowiązku obrony,
- stopień wojskowy,
- numer specjalności wojskowej,
- przynależność ewidencyjna do WKU,

- numer książeczki wojskowej,
- przydział mobilizacyjny do sil zbrojnych RP,
- imię osoby, którą należy zawiadomić w razie wypadku,
- nazwisko osoby, którą należy zawiadomić w razie wypadku,
- adres osoby, którą należy zawiadomić w razie wypadku,
- telefon osoby, którą należy zawiadomić w razie wypadku,
- seria i numer dowodu osobistego,
- składniki wynagrodzenia pracownika,
- informacje na temat zdolności lub niezdolności pracownika do pracy,
- informacje na temat stanu cywilnego pracownika.

Zbiór danych „kadry" zawiera następujące pola:
- imię pracownika,
- nazwisko pracownika,
- data urodzenia pracownika,
- numer ewidencyjny PESEL pracownika,
- adres zamieszkania pracownika,
- imię dziecka pracownika,
- nazwisko dziecka pracownika,
- data urodzenia dziecka pracownika,
- numer ewidencyjny PESEL dziecka pracownika,
- wykształcenie pracownika,
- przebieg zatrudnienia pracownika,
- składniki wynagrodzenia pracownika,
- stan zdrowia pracownika,
- stan cywilny pracownika.

Zbiór danych „lista płac" zawiera następujące pola:
- imię pracownika,
- nazwisko pracownika,
- numer ewidencyjny PESEL pracownika,
- kod oddziału NFZ,
- wymiar etatu pracownika,
- składniki wynagrodzenia pracownika i potrącenia.

Zbiór danych „wniosek o przyznanie świadczenia z zakładowego funduszu świadczeń socjalnych" zawiera następujące pola:
- imię (imiona) wnioskodawcy,
- nazwisko wnioskodawcy,
- adres zamieszkania wnioskodawcy,

- informacje na temat sytuacji rodzinnej wnioskodawcy,
- informacje na temat sytuacji życiowej wnioskodawcy,
- informacje na temat sytuacji materialnej wnioskodawcy.

Zbiór danych „protokół z przebiegu prac komisji kwalifikacyjnej" zawiera następujące pola:
- data posiedzenia komisji kwalifikacyjnej,
- miejsce posiedzenia komisji kwalifikacyjnej,
- imiona członków komisji kwalifikacyjnej,
- nazwiska członków komisji kwalifikacyjnej,
- imiona osób, które uczestniczyły w pracach komisji kwalifikacyjnej w charakterze obserwatora,
- nazwiska osób, które uczestniczyły w pracach komisji kwalifikacyjnej w charakterze obserwatora,
- pytania zadane nauczycielowi w czasie rozmowy kwalifikacyjnej oraz informacje o udzielonych przez nauczyciela odpowiedziach,
- uzyskane przez nauczyciela oceny punktowe,
- średnia arytmetyczna punktów,
- uzasadnienie rozstrzygnięcia komisji kwalifikacyjnej.

Zbiór danych „zaświadczenie o uzyskaniu akceptacji komisji kwalifikacyjnej" zawiera następujące pola:
- nazwa organu, który powołał komisje kwalifikacyjną,
- imię nauczyciela,
- nazwisko nauczyciela,
- data urodzenia nauczyciela,
- miejsce urodzenia nauczyciela,
- data uzyskania akceptacji komisji kwalifikacyjnej,
- stopień awansu zawodowego, na który nauczyciel uzyskał akceptację,
- numer zaświadczenia,
- miejscowość wydania zaświadczenia,
- data wystawienia zaświadczenia.

Zbiór danych „akt nadania stopnia awansu zawodowego nauczyciela" zawiera następujące pola:
- nazwa organu nadającego stopień awansu zawodowego nauczyciela,
- data złożenia wniosku o podjęcie postępowania kwalifikacyjnego,
- numer zaświadczenia o uzyskaniu akceptacji komisji kwalifikacyjnej,
- data zaświadczenia o uzyskaniu akceptacji komisji kwalifikacyjnej,
- nazwa organu, który powołał komisję kwalifikacyjną,
- imię nauczyciela,

- nazwisko nauczyciela,
- data urodzenia nauczyciela,
- miejsce urodzenia nauczyciela,
- stopień awansu zawodowego nauczyciela kontraktowego albo dyplomowanego,
- poziom wykształcenia oraz informację o posiadanym przygotowaniu pedagogicznym,
- nazwa organu odwoławczego,
- numer aktu nadania,
- miejscowość wystawienia aktu nadania,
- data wystawienia aktu nadania.

Zbiór danych „protokół powypadkowy ucznia" zawiera następujące pola:
- imiona członków zespołu powypadkowego,
- nazwiska członków zespołu powypadkowego,
- stanowiska członków zespołu powypadkowego,
- imię poszkodowanego,
- nazwisko poszkodowanego,
- adres zamieszkania poszkodowanego,
- nazwa i adres placówki oświatowej, do której uczęszcza poszkodowany,
- rodzaj wypadku,
- rodzaj urazu i jego opis,
- udzielona pomoc,
- miejsce wypadku,
- rodzaj zajęć,
- opis wypadku z podaniem jego przyczyn,
- imię osoby sprawującej opiekę nad poszkodowanym w chwili wypadku,
- nazwisko osoby sprawującej opiekę nad poszkodowanym w chwili wypadku,
- imiona świadków wypadku,
- nazwiska świadków wypadku,
- adres zamieszkania świadków wypadku,
- data podpisania protokołu.

Zbiór danych „rejestr wypadków uczniów" zawiera następujące pola:
- imię (imiona) poszkodowanego,
- nazwisko poszkodowanego,
- klasa, do której uczęszcza poszkodowany,
- data wypadku,
- rodzaj wypadku,
- miejsce wypadku,
- rodzaj zajęć, w trakcie których doszło do wypadku,
- rodzaj urazu,

- opis urazu,
- okoliczności wypadku,
- udzielona pomoc,
- środki zapobiegawcze, wydane zarządzenia.

Zbiór danych „protokół ustalenia okoliczności i przyczyn wypadku przy pracy" zawiera następujące pola:
- nazwa pracodawcy,
- adres pracodawcy,
- NIP pracodawcy,
- REGON pracodawcy,
- imiona członków zespołu powypadkowego,
- nazwiska członków zespołu powypadkowego,
- stanowiska lub funkcje członków zespołu powypadkowego,
- imię poszkodowanego,
- nazwisko poszkodowanego,
- data urodzenia poszkodowanego,
- miejsce urodzenia poszkodowanego,
- imię ojca poszkodowanego,
- adres zamieszkania poszkodowanego,
- numer ewidencyjny PESEL poszkodowanego,
- kod zawodu wykonywanego przez poszkodowanego,
- informacje na temat zgłoszenia wypadku,
- informacje na temat obrażeń, jakich doznał poszkodowany,
- informacje na temat przyczyn wypadku,
- imiona świadków wypadku,
- nazwiska świadków wypadku,
- adres zamieszkania świadków wypadku,
- informacje na temat skutków wypadku,
- informacje na temat rodzaju wypadku,
- informacje na temat wniosków i zaleceń profilaktycznych.

Zbiór danych „rejestr wypadków pracowników" zawiera następujące pola:
- imię poszkodowanego,
- nazwisko poszkodowanego,
- data wypadku,
- miejsce wypadku,
- informacje dotyczące skutków wypadku dla poszkodowanego,
- data sporządzenia protokołu ustalenia okoliczności i przyczyn wypadku przy pracy,
- stwierdzenie, czy wypadek jest wypadkiem przy pracy,

- data przekazania do Zakładu Ubezpieczeń Społecznych wniosku o świadczenia z tytułu wypadku przy pracy,
- liczba dni niezdolności do pracy,
- inne informacje, których zamieszczenie jest celowe, w tym wnioski i zalecenia profilaktyczne zespołu powypadkowego.

Zbiór danych „system informacji oświatowej" zawiera następujące pola:
- imię (imiona) ucznia,
- nazwisko ucznia,
- numer ewidencyjny PESEL ucznia,
- płeć ucznia,
- data urodzenia ucznia,
- kraj pochodzenia ucznia,
- status ucznia,
- numer i data wydania opinii o potrzebie wczesnego wspomagania rozwoju,
- numer i data wydania orzeczenia o potrzebie zajęć rewalidacyjno-wychowawczych,
- numer i data wydania orzeczenia o potrzebie kształcenia specjalnego,
- informacja o rodzaju niepełnosprawności,
- miejsce zamieszkania ucznia,
- klasa, semestr i oddział, do którego uczęszcza uczeń,
- rodzaj oddziału, do którego uczęszcza uczeń,
- korzystanie z indywidualnego nauczania,
- realizowanie indywidualnego programu lub toku nauki,
- korzystanie z dodatkowej bezpłatnej nauki języka polskiego oraz nauki języka i kultury kraju pochodzenia,
- spełnianie obowiązku szkolnego lub obowiązku nauki poza szkołą,
- informacja, jakiego języka obcego uczeń się uczy,
- uczestniczenie w nauce języka mniejszości narodowej, etnicznej lub języka regionalnego, z określeniem nazwy tego języka,
- uzyskanie tytułu laureata albo finalisty olimpiady przedmiotowej oraz laureata konkursu lub zawodów na szczeblu co najmniej powiatu,
- uzyskanie albo nieuzyskanie promocji,
- korzystanie z przedłużonego okresu nauki na etapie edukacyjnym,
- ukończenie albo nieukończenie szkoły,
- uczestniczenie w zajęciach rozwijających zainteresowania i uzdolnienia,
- uzyskanie karty rowerowej lub motorowerowej,
- korzystanie z bezpłatnego transportu lub zwrotu kosztów przejazdu,
- wypadki, którym uległ uczeń będąc pod opieką szkoły, z określeniem rodzaju wypadku, miejsca, w którym zdarzył się wypadek, rodzaju zajęć, w czasie których wypadek miał miejsce, oraz przyczyny wypadku,

- korzystanie przez ucznia z pomocy materialnej o charakterze motywacyjnym,
- data rozpoczęcia i data zakończenia nauki w szkole,
- wyniki sprawdzianu,
- informacja o spełnianiu obowiązku rocznego przygotowania przedszkolnego przez uczęszczanie do przedszkola za granicą lub przy przedstawicielstwie dyplomatycznym innego państwa w Polsce lub informacja o przyczynie niespełniania tego obowiązku,
- informacja o spełnianiu obowiązku szkolnego przez uczęszczanie do szkoły za granicą lub przy przedstawicielstwie dyplomatycznym innego państwa w Polsce lub informacja o przyczynie niespełniania tego obowiązku,
- informacja o objęciu ucznia pomocą psychologiczno-pedagogiczną udzielaną przez szkołę, z określeniem form tej pomocy,
- informacja o uczestniczeniu ucznia w zajęciach wychowania do życia w rodzinie,
- imię (imiona) nauczyciela,
- nazwisko nauczyciela,
- numer ewidencyjny PESEL nauczyciela,
- płeć nauczyciela,
- data urodzenia nauczyciela,
- kraj pochodzenia nauczyciela,
- wykształcenie,
- przygotowanie pedagogiczne,
- posiadane kwalifikacje do nauczania,
- staż pracy, w tym staż pracy pedagogicznej,
- forma i wymiar zatrudnienia,
- zajmowane stanowiska i sprawowane funkcje,
- rodzaje i wymiar prowadzonych zajęć lub innych wykonywanych obowiązków,
- przyczyny nieprowadzenia zajęć,
- stopień awansu zawodowego oraz dane dotyczące uzyskania kolejnego stopnia awansu zawodowego,
- dane o wysokości wynagrodzenia, z wyszczególnieniem jego składników i ich wysokości, w tym składników nieperiodycznych, oraz dodatków i ich wysokości,
- data nawiązania stosunku pracy oraz data rozwiązania albo wygaśnięcia stosunku pracy.

Zbiór danych „arkusz organizacji pracy szkoły” zawiera następujące pola:
- liczba pracowników (etaty pedagogiczne i etaty administracji i obsługi), w tym urlopy zdrowotne, oddelegowania do pracy w związkach zawodowych, uzupełniające etaty w szkole i w innej placówce,
- liczba stanowisk kierowniczych,
- liczba nauczycieli w podziale na stopnie awansu zawodowego, przystępujących do postępowań kwalifikacyjnych lub egzaminacyjnych w roku szkolnym, którego dotyczy

arkusz, ze wskazaniem terminu złożenia przez nauczycieli wniosków o podjęcie tych postępowań,
- imię (imiona) pracownika,
- nazwisko pracownika,
- płeć pracownika,
- data urodzenia pracownika,
- numer ewidencyjny PESEL pracownika,
- wynagrodzenie pracownika,
- staż pracy pracownika,
- ogólna liczba godzin zajęć edukacyjnych finansowanych ze środków przydzielonych przez organ prowadzący,
- liczba godzin i rodzaj zajęć prowadzonych przez poszczególnych nauczycieli,
- liczba uczniów (w tym z orzeczeniami poradni psychologiczno-pedagogicznej),
- liczba oddziałów,
- zajęcia dodatkowe realizowane przez nauczycieli,
- powierzenie dodatkowych funkcji nauczycielom.

Zbiór danych „dziennik korespondencji" zawiera następujące pola:
- imię adresata,
- nazwisko adresata ,
- adres zamieszkania adresata,
- opis sprawy.

Zbiór danych „rejestr skarg i wniosków" zawiera następujące pola:
- imię osoby składającej skargę,
- nazwisko osoby składającej skargę,
- adres zamieszkania osoby składającej skargę,
- opis przedmiotu skargi.

Zbiór danych „rejestr wniosków o udostępnienie informacji publicznej" zawiera następujące pola:
- imię osoby składającej wniosek o udostępnienie informacji publicznej,
- nazwisko osoby składającej wniosek o udostępnienie informacji publicznej,
- adres zamieszkania osoby składającej wniosek o udostępnienie informacji publicznej,
- adres poczty elektronicznej osoby składającej wniosek o udostępnienie informacji publicznej,
- opis przedmiotu wniosku o udostępnienie informacji publicznej.

Zbiór danych „karta wycieczki (imprezy)" zawiera następujące pola:
- cel i założenia programowe wycieczki (imprezy),

- trasa wycieczki (imprezy),
- termin wycieczki (imprezy),
- ilość dni wycieczki (imprezy),
- klasa lub grupa,
- liczba uczestników wycieczki (imprezy),
- imię kierownika wycieczki (imprezy),
- nazwisko kierownika wycieczki (imprezy),
- liczba opiekunów,
- środek lokomocji,
- imiona opiekunów wycieczki (imprezy),
- nazwiska opiekunów wycieczki (imprezy),
- harmonogram wycieczki (imprezy).

Zbiór danych „orzeczenie lekarskie” zawiera następujące pola:
- miejscowość wystawienia orzeczenia lekarskiego,
- data wystawienia orzeczenia lekarskiego,
- numer orzeczenia lekarskiego,
- rok wystawienia orzeczenia lekarskiego,
- imię nauczyciela,
- nazwisko nauczyciela,
- data urodzenia nauczyciela,
- miejsce urodzenia nauczyciela,
- numer ewidencyjny PESEL nauczyciela lub nazwa i numer dokumentu tożsamości,
- adres zamieszkania nauczyciela,
- okres na jaki udzielono urlop dla poratowania zdrowia.

Powiązania pomiędzy poszczególnymi polami informacyjnymi nie występują.

Załącznik nr 4 do „Polityki bezpieczeństwa” – sposób przepływu danych pomiędzy poszczególnymi systemami

SPOSÓB PRZEPŁYWU DANYCH POMIĘDZY POSZCZEGÓLNYMI SYSTEMAMI

Przepływ danych pomiędzy poszczególnymi systemami nie występuje.

Załącznik nr 18 do zarządzenia nr 206/2015/2016 – „Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych”

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM SŁUŻĄCYM DO PRZETWARZANIA DANYCH OSOBOWYCH

§ 1.

„Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych”, zwana w dalszej części „Instrukcją”, określa procedury nadawania uprawnień do przetwarzania danych osobowych i rejestrowania tych uprawnień w systemie informatycznym służącym do przetwarzania danych osobowych oraz wskazuje osoby odpowiedzialnej za te czynności, stosowane metody i środki uwierzytelniania oraz procedury związane z ich zarządzaniem i użytkowaniem, procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu informatycznego służącego do przetwarzania danych osobowych, procedury tworzenia kopii zapasowych zbiorów danych osobowych oraz programów i narzędzi programowych służących do ich przetwarzania, sposób, miejsce i okres przechowywania elektronicznych nośników informacji zawierających dane osobowe oraz kopie zapasowe, sposób odnotowywania informacji o odbiorcach danych osobowych, procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych osobowych w Szkole Podstawowej z Oddziałami Integracyjnymi nr 1 im. Janusza Korczaka w Rybniku.

§ 2.

Procedury nadawania uprawnień do przetwarzania danych osobowych i rejestrowania tych uprawnień w systemie informatycznym służącym do przetwarzania danych osobowych oraz wskazanie osoby odpowiedzialnej za te czynności określa „Procedura kontroli dostępu”.

§ 3.

Stosowane metody i środki uwierzytelniania oraz procedury związane z ich zarządzaniem i użytkowaniem określa „Procedura kontroli dostępu”.

§ 4.

Procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu informatycznego służącego do przetwarzania danych osobowych określa „Procedura rozpoczęcia, zawieszenia i zakończenia pracy na komputerze”.

§ 5.

Procedury tworzenia kopii zapasowych zbiorów danych osobowych oraz programów i narzędzi programowych służących do ich przetwarzania określa „Procedura tworzenia kopii zapasowych”.

§ 6.

Sposób, miejsce i okres przechowywania elektronicznych nośników informacji zawierających dane osobowe oraz kopii zapasowych określa „Procedura zarządzania nośnikami elektronicznymi”.

§ 7.

Sposób zabezpieczenia systemu informatycznego służącego do przetwarzania danych osobowych przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego służącego do przetwarzania danych osobowych określa „Procedura ochrony przed złośliwym oprogramowaniem”.

§ 8.

W systemie informatycznym służącym do przetwarzania danych osobowych odnotowywane są informacje o odbiorcach danych, a w szczególności imię i nazwisko lub nazwa odbiorcy, data udostępnienia oraz zakres udostępnienia.

§ 9.

Procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych osobowych określa „Procedura wykonywania przeglądów, konserwacji i napraw komputerów, nośników i oprogramowania służących do przetwarzania informacji”.

§ 10.

Nadzór nad realizacją „Instrukcji” sprawuje Dyrektor Szkoły Podstawowej z Oddziałami Integracyjnymi nr 1 im. Janusza Korczaka w Rybniku.

Załącznik nr 19 do zarządzenia nr 206/2015/2016 – przykłady typowych zagrożeń

PRZYKŁADY TYPOWYCH ZAGROŻEŃ

	dane niepodlegające udostępnianiu – art. 5 ustawy z dnia 6 września 2001 roku o dostępie do informacji publicznej	

Załącznik nr 20 do zarządzenia nr 206/2015/2016 – przykłady podatności

PRZYKŁADY PODATNOŚCI

	dane niepodlegające udostępnianiu – art. 5 ustawy z dnia 6 września 2001 roku o dostępie do informacji publicznej	

Załącznik nr 21 do zarządzenia nr 206/2015/2016 – „Procedura postępowania z hasłami administratora”

PROCEDURA POSTĘPOWANIA Z HASŁAMI ADMINISTRATORA

§ 1.

1. „Procedura postępowania z hasłami administratora”, zwana w dalszej części „Procedurą”, określa zasady przechowywania i korzystania z haseł administratora w Szkole Podstawowej z Oddziałami Integracyjnymi nr 1 im. Janusza Korczaka w Rybniku.
2. Ilekroć w „Procedurze” mowa o:
   1) Dyrektorze – należy przez to rozumieć Dyrektora Szkoły Podstawowej z Oddziałami Integracyjnymi nr 1 im. Janusza Korczaka w Rybniku lub osobę zastępującą,
   2) informatyku – należy przez to rozumieć pracownika Szkoły Podstawowej z Oddziałami Integracyjnymi nr 1 im. Janusza Korczaka w Rybniku, wykonawcę lub użytkownika reprezentującego stronę trzecią, który czuwa nad sprawnym i ciągłym działaniem systemu teleinformatycznego.

§ 2.

1.	*dane niepodlegające udostępnianiu – art. 5 ustawy z dnia 6 września 2001 roku o dostępie do informacji publicznej*	
2.	*dane niepodlegające udostępnianiu – art. 5 ustawy z dnia 6 września 2001 roku o dostępie do informacji publicznej*	

§ 3.

1.	*dane niepodlegające udostępnianiu – art. 5 ustawy z dnia 6 września 2001 roku o dostępie do informacji publicznej*	
2.	*dane niepodlegające udostępnianiu*	

	– art. 5 ustawy z dnia 6 września 2001 roku o dostępie do informacji publicznej	
3.	*dane niepodlegające udostępnianiu – art. 5 ustawy z dnia 6 września 2001 roku o dostępie do informacji publicznej*	
4.	*dane niepodlegające udostępnianiu – art. 5 ustawy z dnia 6 września 2001 roku o dostępie do informacji publicznej*	
5.	*dane niepodlegające udostępnianiu – art. 5 ustawy z dnia 6 września 2001 roku o dostępie do informacji publicznej*	

§ 4.

Nadzór nad realizacją „Procedury” sprawuje Dyrektor.