ZARZĄDZENIE NR 05/2016
DYREKTORA SZKOŁY PODSTAWOWEJ
Z ODDZIAŁAMI INTEGRACYJNYMI NR 20
im. HARCERZY BUCHALIKÓW w RYBNIKU
z dnia 01.09.2016 r.

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,
- § 3 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 20 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 Dyrektora poprzez zapewnienie 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 września 2001 roku o dostępie do informacji*	[redacted]

§ 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.
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.

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

§ 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. Traci moc dotychczas obowiązująca „Polityka bezpieczeństwa danych osobowych” wprowadzona zarządzeniem nr 14/2010 Dyrektora Szkoły Podstawowej nr 20 im. Harcerzy Buchalików w Rybniku z dnia 28.12.2010 r.
2. Wprowadza się „Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych”, która stanowi załącznik nr 18 do zarządzenia. Traci moc dotychczas obowiązująca „Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych” wprowadzona zarządzeniem nr 15/2010 Dyrektora Szkoły Podstawowej nr 20 im. Harcerzy Buchalików w Rybniku z dnia 28.12.2010 r.

§ 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 podpisania, za wyjątkiem § 14, który wchodzi w życie z dniem 1 stycznia 2017 roku.