Szkoła Podstawowa
z Oddziałami Integracyjnymi nr 36
im. Czesława Miłosza w Rybniku
44-251 Rybnik, ul. Sztolniowa 29 b
NIP 6423203995 Regon 367991029
tel. 32 42 18 228

Zarządzenie nr 7
Dyrektora Szkoły Podstawowej nr 36 im. Czesława Miłosza
w Rybniku
z dnia 25.05.2018 roku

w sprawie zmiany „Systemu zarządzania bezpieczeństwem informacji", „Procedury zarządzania ryzykiem" i „Procedury zarządzania ryzykiem w bezpieczeństwie informacji"

Na podstawie:

- art. 24 ust. 1 i art. 32 ust. 1 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych),
- art. 108a ustawy z dnia 14 grudnia 2016 roku Prawo oświatowe,
- art. 68 ust. 2 pkt. 7 i art. 69 ust. 1 pkt 3 ustawy z dnia 27 sierpnia 2009 roku o finansach publicznych,
- § 20 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. W „Systemie zarządzania bezpieczeństwem informacji":
   1) w § 13 dodaje się ust. 8 w brzmieniu: *Fragmenty obszaru bezpiecznego zabezpieczone są monitoringiem. Zasady funkcjonowania systemu monitoringu wizyjnego, obszar objęty monitoringiem wizyjnym, reguły rejestracji i zapisu informacji oraz sposób ich zabezpieczenia określa „Regulamin funkcjonowania monitoringu", który stanowi załącznik nr 1.*,
   2) skreśla się § 13 ust. 4,
   3) skreśla się § 15,
   4) skreśla się § 20,
   5) w § 32 dodaje się ust. 2 w brzmieniu: *Wymagania dotyczące ochrony fizycznej, kontroli dostępu i wykonywania kopii zapasowych przy pracy na odległość określa „Procedura pracy na odległość", która stanowi załącznik nr 7.*,
   6) skreśla się § 33 ust. 2,
   7) § 34 otrzymuje brzmienie:
      1. *Dokumentacja zawierająca dane osobowe powinna być przechowywana w zamykanych na klucz szafach i szufladach mebli biurowych. Niedopuszczalne jest przechowywanie dokumentacji zawierającej dane osobowe bez jakiegokolwiek zabezpieczenia, np. na otwartych regałach.*

2. *Dokumentacja zawierająca wrażliwe dane osobowe powinna być przechowywana w szafach metalowych o podwyższonej klasie odporności na włamanie i ognioodpornych.*
3. *Dokumentacja zawierająca dane osobowe po ustaniu jej przydatności do bieżącego przetwarzania oraz braku obowiązku prawnego jej dalszego archiwizowania podlega zniszczeniu w przeznaczonych do tego urządzeniach spełniających co najmniej wymagania poziomu P-3 według normy technicznej DIN 66399 lub równoważnej.*
4. *Niedopuszczane jest wyrzucanie do kosza na śmieci jakiejkolwiek dokumentacji zawierającej dane osobowe, bez względu na jej zawartość informacyjną czy upływ czasu od jej wytworzenia.*
5. *Pracownik przy przetwarzaniu danych osobowych zobowiązany jest do stosowania zasady czystego biurka polegającej na przechowywaniu pod zamknięciem nieużywanych danych osobowych umieszczonych na elektronicznych nośnikach informacji lub w postaci papierowej, szczególnie jeśli pomieszczenie biurowe jest opuszczane.*
6. *Pracownik, którego stanowisko pracy wyposażone jest w tablicę korkową, magnetyczną itp., zobowiązany jest do niezamieszczania na tablicy żadnych danych osobowych.*
7. *Pracownik przy przetwarzaniu danych osobowych zobowiązany jest do stosowania zasady czystego ekranu polegającej na:*
   1) *ustawieniu ekranu monitora komputera w sposób uniemożliwiający osobie nieupoważnionej dostęp do danych osobowych 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.*
8. *Niedopuszczalne jest pozostawienie osoby nieupoważnionej do przetwarzania danych osobowych w pomieszczeniu biurowym, w którym przetwarzane są dane osobowe bez nadzoru, także wtedy, kiedy stanowisko komputerowe jest wyłączone lub wylogowane, a dokumentacja papierowa umieszczona w zamkniętej szafie.*

8) § 41 otrzymuje brzmienie: *Dopuszcza się zdalne zarządzanie środkami przetwarzania informacji.*,
9) skreśla się § 44,
10) § 53 otrzymuje brzmienie: *Dyrektor lub wyznaczona przez Dyrektora osoba wprowadza pracowników oraz, gdy jest to wskazane, wykonawców i użytkowników reprezentujących stronę trzecią w obowiązki i zakres odpowiedzialności związane z bezpieczeństwem informacji.*,
11) § 55 otrzymuje brzmienie:

1. *Pracownicy oraz, gdy jest to wskazane, wykonawcy i użytkownicy reprezentujący stronę trzecią podlegają szkoleniu w zakresie bezpieczeństwa informacji.*
2. *Tematyka szkolenia powinna obejmować w szczególności:*
   1) *aktualny system prawny bezpieczeństwa informacji w Polsce i Unii Europejskiej,*
   2) *wewnętrzne regulacje związane z bezpieczeństwem informacji w Szkole,*
   3) *zagrożenia dla bezpieczeństwa przetwarzanych informacji, w odniesieniu do specyfiki działalności Szkoły,*
   4) *role i zadania poszczególnych osób odpowiedzialnych za bezpieczeństwo informacji,*
   5) *zasady udzielania dostępu do informacji i danych osobowych,*
   6) *zasady przetwarzania informacji w systemach teleinformatycznych,*
   7) *procedury postępowania w sytuacji naruszenia bezpieczeństwa przetwarzanych informacji,*
   8) *odpowiedzialność dyscyplinarna i karna za nieprzestrzeganie zasad bezpieczeństwa informacji.*
3. *Zapoznanie pracownika z aktami prawnymi – powszechnymi i wewnętrznymi obowiązującymi w Szkole – musi przybrać formę udostępnienia tych dokumentów na czas niezbędny do osobistego zapoznania z ich treścią.*
4. *Szkolenie przeprowadza Dyrektor lub wyznaczona przez Dyrektora osoba.*
5. *Szkolenie, w zależności od potrzeb, może zostać przeprowadzone w formie tradycyjnego wykładu lub kursu e-learningowego.*
6. *Udział w szkoleniu powinien zostać potwierdzony własnoręcznym podpisem uczestnika lub innym niezaprzeczalnym dowodem jego odbycia.*
7. *Niedopuszczalne jest, aby szkolenie polegało jedynie na zapoznaniu się osoby z aktami prawnymi bez ich objaśnienia i odniesienia do specyfiki przetwarzania informacji w Szkole. W takim przypadku szkolenie zostanie uznane za nieskuteczne.*
8. *Szkolenie powinno być uzupełnione indywidualnymi szkoleniami stanowiskowymi, przeprowadzanymi przez bezpośrednich przełożonych tak, aby zdobytą ogólną wiedzę przełożyć na szczególną specyfikę zakresu zadań danej osoby.*

12) § 60 ust. 3 otrzymuje brzmienie: *W szczególności jako incydent należy zakwalifikować awarię lub inne nienormalne zachowanie systemu teleinformatycznego, a zwłaszcza:*
   1) *utratę usługi, urządzenia lub funkcjonalności,*
   2) *przeciążenie lub niepoprawne działanie systemu teleinformatycznego,*
   3) *niezgodność z procedurami lub zaleceniami,*
   4) *naruszenie ustaleń związanych z bezpieczeństwem fizycznym,*
   5) *niekontrolowane zmiany systemu teleinformatycznego,*
   6) *niepoprawne działanie środków przetwarzania informacji,*
   7) *naruszenie dostępu,*
   8) *nieuprawioną lub nieautoryzowaną modyfikację, zniszczenie lub utratę informacji.*,

9) w § 60 dodaje się ust. 4 w brzmieniu: *Każde potencjalne naruszenie ochrony danych osobowych należy niezwłocznie zgłosić inspektorowi ochrony danych na zasadach*

określonych w „Procedurze postępowania w sytuacjach naruszenia ochrony danych osobowych", która stanowi załącznik nr 15.,

10) w § 60 dodaje się ust. 5 w brzmieniu: *Przez naruszenie ochrony danych osobowych rozumie się naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.,*

13) skreśla się § 67,

14) § 68 ust. 1 otrzymuje brzmienie: *Przynajmniej raz w roku przeprowadza się szacowanie ryzyka w bezpieczeństwie informacji i ryzyka naruszenia praw i wolności osoby, której dane dotyczą, o którym mowa w rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) na zasadach określonych w „Procedurze zarządzania ryzykiem w bezpieczeństwie informacji", mając na uwadze utratę integralności, poufności i dostępności informacji.,*

15) dodaje się § 77 w brzmieniu: *Dokumentacja „Systemu zarządzania bezpieczeństwem informacji" podlega bezwzględnej tajemnicy.*

2. „Regulamin funkcjonowania monitoringu" otrzymuje brzmienie jak w załączniku nr 1 do zarządzenia.
3. „Procedura kontroli dostępu" otrzymuje brzmienie jak w załączniku nr 2 do zarządzenia.
4. „Procedura pracy na odległość" otrzymuje brzmienie jak w załączniku nr 3 do zarządzenia.
5. „Procedura korzystania ze środków wymiany informacji" otrzymuje brzmienie jak w załączniku nr 4 do zarządzenia.
6. „Procedura zarządzania incydentami związanymi z bezpieczeństwem informacji" otrzymuje brzmienie jak w załączniku nr 5 do zarządzenia.
7. „Procedura postępowania w sytuacjach naruszenia ochrony danych osobowych" otrzymuje brzmienie jak w załączniku nr 6 do zarządzenia.
8. Upoważnienia do przetwarzania danych osobowych nadane przed wejściem w życie zarządzenia pozostają w mocy. Z chwilą nadania nowych upoważnień automatycznie tracą ważność – nie mają tu zastosowania zasady odwołania upoważnień określone w „Procedurze kontroli dostępu".

§ 3.

Poszczególne paragrafy i załączniki „Systemu zarządzania bezpieczeństwem informacji" zostają odpowiednio przenumerowane, aby zachować ciągłość numeracji.

§ 4.

1. W „Procedurze zarządzania ryzykiem" § 1 ust. 3 otrzymuje brzmienie: *„Procedura" nie ma zastosowania dla zarządzania ryzykiem w bezpieczeństwie informacji i zarządzania*

ryzykiem naruszenia praw i wolności osoby, której dane dotyczą, o którym mowa w rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych).

2. W „Procedurze zarządzania ryzykiem w bezpieczeństwie informacji":
   1) § 1 ust. 1 otrzymuje brzmienie: : *„Procedura zarządzania ryzykiem w bezpieczeństwie informacji", zwana w dalszej części „Procedurą", określa zasady przeprowadzania okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji i ryzyka naruszenia praw i wolności osoby, której dane dotyczą, o którym mowa w rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), oraz podejmowania działań minimalizujących to ryzyko, stosownie do wyników przeprowadzonej analizy, w Szkole Podstawowej z Oddziałami Integracyjnymi nr 36 im. Czesława Miłosza w Rybniku,*
   2) § 1 ust. 2 pkt 2) otrzymuje brzmienie: *ryzyku – należy przez to rozumieć ryzyko w bezpieczeństwie informacji i ryzyko naruszenia praw i wolności osoby, której dane dotyczą, o którym mowa w rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych).*

§ 5.

Nadzór nad realizacją zarządzenia sprawuje Dyrektor.

§ 6.

Zarządzenie wchodzi w życie z dniem podpisania.

Dyrektor
Szkoły Podstawowej
z Oddziałami Integracyjnymi nr 36
im. Czesława Miłosza w Rybniku
mgr inż. Krzysztof Zaik

Załącznik nr 1 do zarządzenia nr 7 – „Regulamin funkcjonowania monitoringu"

REGULAMIN FUNKCJONOWANIA MONITORINGU

§ 1.

1. „Regulamin funkcjonowania monitoringu", zwany w dalszej części „Regulaminem", określa zasady funkcjonowania systemu monitoringu wizyjnego, obszar objęty monitoringiem, reguły rejestracji i zapisu informacji oraz sposób ich zabezpieczenia w Szkole Podstawowej z Oddziałami Integracyjnymi nr 36 im. Czesława Miłosza w Rybniku.
2. Ilekroć w „Regulaminie" jest mowa o:
   1) Dyrektorze – należy przez to rozumieć Dyrektora Szkoły Podstawowej z Oddziałami Integracyjnymi nr 36 im. Czesława Miłosza w Rybniku lub osobę zastępującą,
   2) Szkole – należy przez to rozumieć Szkołę Podstawową z Oddziałami Integracyjnymi nr 36 im. Czesława Miłosza w Rybniku.

§ 2.

Monitoring zainstalowany jest w celach:
1) zapewnienia porządku publicznego,
2) zapewnienia bezpieczeństwa osób i mienia,
3) wyjaśniania ewentualnych sytuacji konfliktowych,
4) ustalania sprawców czynów niedozwolonych.

§ 3.

1. Monitoring swym zasięgiem obejmuje na zewnątrz obszar wokół budynku Szkoły, parkingi i boisko szkolne (w tym kamera obrotowa) oraz wewnątrz korytarze i salę gimnastyczną.
2. Miejsca objęte monitoringiem wizyjnym są odpowiednio oznaczone.

§ 4.

1. Monitoring funkcjonuje całodobowo.
2. Rejestracji i zapisaniu na nośniku fizycznym podlega tylko obraz (wizja) z kamer systemu monitoringu. Nie rejestruje się dźwięku (fonii).

§ 5.

1. W ramach monitoringu dochodzi do przetwarzania danych osobowych. Administratorem jest Szkoła reprezentowany przez Dyrektora.
2. Nagrania obrazu zawierające dane osobowe zabezpieczone są poprzez zastosowanie odpowiednich środków technicznych i organizacyjnych zapewniających ochronę w taki sposób, aby nie były udostępniane osobom nieupoważnionym, zabrane przez osobę nieuprawnioną, a także by były zabezpieczone przed uszkodzeniem, zniszczeniem lub utratą.

3. Nagrania obrazu zawierające dane osobowe przetwarza się wyłącznie do celów, w których zostały zebrane.
4. Nagrania obrazu zawierające dane osobowe nie są udostępniane podmiotom innym niż uprawnione na podstawie przepisów prawa.

§ 6.

1. Okres przechowywania nagrań obrazu zawierających dane osobowe wynosi 14 dni.
2. Po upływie okresu, o którym mowa w ust. 1, uzyskane w wyniku monitoringu nagrania obrazu zawierające dane osobowe, podlegają zniszczeniu, z wyjątkiem sytuacji, w których nagrania zostały zabezpieczone, zgodnie z odrębnymi przepisami.

§ 7.

W sprawach spornych lub nieuregulowanych w „Regulaminie" decyzję podejmuje Dyrektor.

Załącznik nr 2 do zarządzenie nr 7 – „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 36 im. Czesława Miłosza w Rybniku.
2. Ilekroć w „Procedurze" jest mowa o:
   1) administratorze – należy przez to rozumieć Szkołę Podstawowej z Oddziałami Integracyjnymi nr 36 im. Czesława Miłosza w Rybniku reprezentowaną przez Dyrektora Szkoły Podstawowej z Oddziałami Integracyjnymi nr 36 im. Czesława Miłosza w Rybniku,
   2) Dyrektorze – należy przez to rozumieć Dyrektora Szkoły Podstawowej z Oddziałami Integracyjnymi nr 36 im. Czesława Miłosza w Rybniku lub osobę zastępującą,
   3) informatyku – należy przez to rozumieć pracownika Szkoły Podstawowej z Oddziałami Integracyjnymi nr 36 im. Czesława Miłosza w Rybniku, wykonawcę lub użytkownika reprezentującego stronę trzecią, który czuwa nad sprawnym i ciągłym działaniem systemu teleinformatycznego,
   4) użytkowniku – należy przez to rozumieć pracownika Szkoły Podstawowej z Oddziałami Integracyjnymi nr 36 im. Czesława Miłosza 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 36 im. Czesława Miłosza w Rybniku,
   5) Szkole – należy przez to rozumieć Szkołę Podstawową z Oddziałami Integracyjnymi nr 36 im. Czesława Miłosza 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.

Środki uwierzytelniania dostępu do pracy na komputerze i z wykorzystaniem oprogramowania służącego do przetwarzania informacji to identyfikator użytkownika i hasło dostępu.

§ 4.

1. Identyfikator użytkownika jest w sposób jednoznaczny przypisany danemu użytkownikowi. Wykaz identyfikatorów użytkownika przypisanych poszczególnym użytkownikom prowadzi Dyrektor lub wyznaczona przez Dyrektora osoba.
2. Użytkownik jest odpowiedzialny za wszystkie czynności wykonane przy użyciu identyfikatora użytkownika, którym się posługuje lub posługiwał.
3. Identyfikator użytkownika nie powinien być zmieniany, a po wyrejestrowaniu użytkownika z systemu teleinformatycznego nie może być przydzielony innemu użytkownikowi.
4. Identyfikator użytkownika, który utracił prawo dostępu do pracy na komputerze i z wykorzystaniem oprogramowania służącego do przetwarzania informacji, należy niezwłocznie zablokować.
5. W Szkole nie stosuje się identyfikatorów grupowych użytkownika.

§ 5.

Każdy identyfikator użytkownika zabezpieczony jest hasłem dostępu.

§ 6.

1. Obowiązują następujące zasady tworzenia hasła dostępu:
   1) hasło dostępu nie powinno składać się z żadnych danych personalnych (imienia, nazwiska, adresu zamieszkania użytkownika lub najbliższych osób) lub ich fragmentów ani być oparte na prostych skojarzeniach (numer telefonu, data urodzenia),
   2) hasło dostępu powinno składać się z co najmniej 8 znaków, zawierać małe i wielkie litery oraz cyfry lub znaki specjalne,
   3) hasło dostępu nie powinno składać się z identycznych znaków lub ciągu znaków z klawiatury,
   4) hasło dostępu nie może być jednakowe z identyfikatorem użytkownika,
   5) hasło dostępu musi być unikalne, tj. takie, które nie było poprzednio stosowane przez użytkownika,
   6) hasło dostępu nie może być podatne na atak słownikowy, tj. nie może zawierać słów zamieszczonych w słownikach.
2. Hasło dostępu w trakcie wpisywania nie może być wyświetlane na ekranie.
3. Użytkownik jest zobowiązany do utrzymania hasła dostępu w tajemnicy, również po utracie jego ważności.
4. Hasło dostępu nie może być przechowywane w systemach teleinformatycznych w niechronionej postaci.
5. Hasło dostępu nie może być zapisywane na papierze, w pliku lub urządzeniu przenośnym.
6. Hasło dostępu nie może być wprowadzone do jakichkolwiek zautomatyzowanych procesów logowania się na komputer i w oprogramowaniu służącemu do przetwarzania informacji.

7. Hasło dostępu nie może być przechowywane w markach ani przypisane do klawiszy funkcyjnych.
8. Hasło dostępu musi być zmieniane nie rzadziej niż co 30 dni. Jeżeli zmiana hasła dostępu nie jest możliwa w wymaganym czasie, należy jej dokonać w najbliższym możliwym terminie. Zmiana hasła po jego deklarowanym okresie ważności i jakość hasła dostępu są wymuszane przez komputer lub oprogramowanie służące do przetwarzania informacji.
9. Hasło dostępu jest zmieniane przez użytkownika.
10. W przypadku podejrzenia złamania poufności hasła dostępu lub bezpieczeństwa systemu teleinformatycznego, użytkownik zobowiązany jest niezwłocznie zmienić hasło dostępu i poinformować o tym fakcie Dyrektora.

§ 7.

1. Informatyk rejestruje użytkownika w komputerze i w oprogramowaniu służącym do przetwarzania informacji poprzez utworzenie identyfikatora użytkownika i nadaje jednorazowe hasło dostępu, które musi zostać zmienione przy pierwszym logowaniu użytkownika. Zmianę hasła dostępu wymusza komputer lub oprogramowanie służące do przetwarzania informacji.
2. Jednorazowe hasło dostępu nie może być przekazywane użytkownikowi za pośrednictwem osób trzecich lub niechronionych wiadomości poczty elektronicznej.
3. Jednorazowe hasło dostępu, zastępcze lub tymczasowe informatyk nadaje po uprzedniej weryfikacji tożsamości użytkownika.
4. Informatyk usuwa użytkownika z komputera lub z oprogramowania służącego do przetwarzania informacji poprzez trwałe usunięcie identyfikatora użytkownika.

§ 8.

Hasło domyślne nadane przez producenta należy zmienić w trakcie pierwszego uruchomienia komputera lub instalacji oprogramowania służącego do przetwarzania informacji.

§ 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.
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.

§ 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.

Informatyk przynajmniej raz w roku sprawdza oraz usuwa lub blokuje zbędne identyfikatory użytkowników.

§ 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 § 9 „Procedury kontroli dostępu" w związku z art. 29 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) upoważniam Panią/Pana* ... *(imię i nazwisko)* do przetwarzania danych osobowych ... *(cel przetwarzania, np. w ramach wykonywania czynności służbowych, pełnienia funkcji społecznej, w celu przeprowadzenia kontroli itp.).*

Administrator

.....
(pieczątka i podpis)

Oświadczam, że zostałam zapoznana/zostałem zapoznany* z zasadami przetwarzania i ochrony danych osobowych określonymi w przepisach prawa powszechnych i procedurach wewnętrznych obowiązujących w Szkole Podstawowej z Oddziałami Integracyjnymi nr 36 im. Czesława Miłosza w Rybniku. Zobowiązuję się do zachowania w tajemnicy przetwarzanych danych osobowych oraz sposobów ich zabezpieczenia.

Oświadczam, że jestem świadoma/świadomy* odpowiedzialności dyscyplinarnej, finansowej i karnej wynikającej z niewłaściwego postępowania przy przetwarzaniu danych osobowych.

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 § 9 „Procedury kontroli dostępu" w związku z art. 29 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) odwołuję z dniem ... *(data)* upoważnienie do przetwarzania danych osobowych dla Pani/Pana* ... *(imię i nazwisko)*.

Administrator

.....

(pieczątka i podpis)

** niepotrzebne skreślić lub skasować*

Załącznik nr 3 do zarządzenia nr 7 – „Procedura pracy na odległość"

PROCEDURA PRACY NA ODLEGŁOŚĆ

§ 1.

1. „Procedura pracy na odległość", zwana w dalszej części „Procedurą", określa wymagania dotyczące ochrony fizycznej, kontroli dostępu i wykonywania kopii zapasowych przy pracy na odległość dla Szkoły Podstawowej z Oddziałami Integracyjnymi nr 36 im. Czesława Miłosza w Rybniku.
2. Ilekroć w „Procedurze" jest mowa o:
   1) Dyrektorze – należy przez to rozumieć Dyrektora Szkoły Podstawowej z Oddziałami Integracyjnymi nr 36 im. Czesława Miłosza w Rybniku lub osobę zastępującą,
   2) pracy na odległość – należy przez to rozumieć przetwarzanie informacji będących własnością Szkoły Podstawowej z Oddziałami Integracyjnymi nr 36 im. Czesława Miłosza w Rybniku z wykorzystaniem środków przetwarzania informacji niebędących własnością Szkoły Podstawowej z Oddziałami Integracyjnymi nr 36 im. Czesława Miłosza w Rybniku,
   3) Szkole – należy przez to rozumieć Szkołę Podstawową z Oddziałami Integracyjnymi nr 36 im. Czesława Miłosza w Rybniku.

§ 2.

W Szkole obowiązuje zakaz pracy na odległość bez wcześniejszej zgody Dyrektora. Zgoda może być wydana ustnie, ale nie może być domniemana lub dorozumiana – musi być wyrażona wprost.

§ 3.

1. W pracy na odległość należy zwracać szczególną uwagę na to, aby nie naruszyć bezpieczeństwa informacji, w szczególności:
   1) należy stosować środki uwierzytelniania określone w „Procedurze kontroli dostępu",
   2) należy tworzyć kopie zapasowe informacji na zasadach określonych w „Procedurze tworzenia kopii zapasowych",
   3) w miejscach publicznych, salach spotkań i innych niechronionych miejscach należy zachować ostrożność, w tym:
      a) unikać ryzyka podglądania ze strony nieuprawnionych osób,
      b) nie dopuszczać do korzystania z informacji i ze środków przetwarzania informacji przez nieuprawnione osoby,
      c) nie pozostawiać informacji i środków przetwarzania informacji bez nadzoru i, tam gdzie jest to możliwe, fizycznie zabezpieczyć przed dostępem nieuprawnionych osób,

4) zbędne lub niepotrzebne informacje należy skasować lub nadpisać za pomocą technik uniemożliwiających ich odtworzenie. Nie dopuszcza się standardowego formatowania.

2. Zgubienie lub kradzież środka przetwarzania informacji wykorzystywanego do pracy na odległość traktowane jest jako incydent związany z bezpieczeństwem informacji i należy wtedy postępować zgodnie z „Procedurą zarządzania incydentami związanymi z bezpieczeństwem informacji".

§ 4.

W pracy na odległość nie dopuszcza się przetwarzania danych osobowych.

§ 5.

Szkoła nie ponosi odpowiedzialność za legalność środków przetwarzania informacji i oprogramowania służącego do przetwarzania informacji wykorzystywanych w pracy na odległość.

§ 6.

Nadzór nad realizacją „Procedury" sprawuje Dyrektor.

Załącznik nr 4 do zarządzenia nr 7 – „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 36 im. Czesława Miłosza w Rybniku.
2. Ilekroć w „Procedurze" mowa o:
   1) Dyrektorze – należy przez to rozumieć Dyrektora Szkoły Podstawowej z Oddziałami Integracyjnymi nr 36 im. Czesława Miłosza w Rybniku lub osobę zastępującą,
   2) informatyku – należy przez to rozumieć pracownika Szkoły Podstawowej z Oddziałami Integracyjnymi nr 36 im. Czesława Miłosza 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 36 im. Czesława Miłosza 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 konieczności wymiany danych osobowych w postaci elektronicznej, dopuszczalne jest wyłącznie w formie załączników, z uwzględnieniem poniższych zasad:
   1) przetwarzane załączniki zawierające dane osobowe podlegają zabezpieczeniu kryptograficznemu z użyciem algorytmu AES256 lub silniejszego, uzgodnionego pomiędzy nadawcą i odbiorcą (np. oprogramowanie archiwizujące z wbudowanym algorytmem szyfrującym),
   2) hasło zabezpieczające (klucz szyfrujący), zapewniające ochronę przed nieuprawnionym odszyfrowaniem załącznika, składa się z co najmniej 8 znaków,
   3) nadawca, po uzyskaniu od odbiorcy potwierdzenia otrzymania zabezpieczonych załączników, przekazuje odbiorcy hasło zabezpieczające (klucz szyfrujący) poprzez przesłanie go innym kanałem niż poczta elektroniczna, w szczególności w drodze połączenia telefonicznego, z zachowaniem zasad i środków zabezpieczających przed ujawnieniem hasła podmiotom nieuprawnionym.

§ 5.

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

1) nieautoryzowanym dostępem do wbudowanych pamięci w celu odzyskania wiadomości,
2) rozmyślnym lub przypadkowym programowaniem faksów w taki sposób, aby wysyłały wiadomości pod określone numery,
3) 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 mieć pewność z kim rozmawia i 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 5 do zarządzenia nr 7 – „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 36 im. Czesława Miłosza w Rybniku.
2. Ilekroć w „Procedurze" jest mowa o:
   1) Dyrektorze – należy przez to rozumieć Dyrektora Szkoły Podstawowej z Oddziałami Integracyjnymi nr 36 im. Czesława Miłosza w Rybniku lub osobę zastępującą,
   2) informatyku – należy przez to rozumieć pracownika Szkoły Podstawowej z Oddziałami Integracyjnymi nr 36 im. Czesława Miłosza 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 36 im. Czesława Miłosza w Rybniku.

§ 2.

1. Incydent związany z bezpieczeństwem informacji, zwany w dalszej części incydentem, jest to pojedyncze zdarzenie lub seria niepożądanych lub niespodziewanych zdarzeń związanych z bezpieczeństwem informacji, które stwarzają znaczne prawdopodobieństwo zakłócenia funkcjonowania Szkoły i zagrażają bezpieczeństwu informacji.
2. W szczególności jako incydent należy zakwalifikować awarię lub inne nienormalne zachowanie systemu teleinformatycznego, a zwłaszcza:
   1) utratę usługi, urządzenia lub funkcjonalności,
   2) przeciążenie lub niepoprawne działanie systemu teleinformatycznego,
   3) niezgodność z procedurami lub zaleceniami,
   4) naruszenie ustaleń związanych z bezpieczeństwem fizycznym,
   5) niekontrolowane zmiany systemu teleinformatycznego,
   6) niepoprawne działanie środków przetwarzania informacji,
   7) naruszenie dostępu,
   8) nieuprawioną lub nieautoryzowaną modyfikację, zniszczenie lub utratę informacji.

§ 3.

1. Pracownik Szkoły, wykonawca lub użytkownik reprezentujący stronę trzecią zobowiązany jest niezwłocznie zgłosić Dyrektorowi każdy incydent.
2. Zgłoszenia incydentu należy dokonać na formularzu zgłoszenia zdarzenia związanego z bezpieczeństwem informacji lub ustnie. Wzór formularza zgłoszenia zdarzenia związanego z bezpieczeństwem informacji stanowi załącznik do „Procedury".
3. W przypadku zgłoszenia ustnego Dyrektor lub wyznaczony przez Dyrektora pracownik wypełnia formularz zgłoszenia zdarzenia związanego z bezpieczeństwem informacji.
4. Wypełniając formularz zgłoszenia zdarzenia związanego z bezpieczeństwem informacji należy w szczególności odnotować wszystkie ważne szczegóły, takie jak typ niezgodności, błąd działania, wiadomość z ekranu czy dziwne zachowanie.

§ 4.

1. Podejmowanie przez pracownika, wykonawcę lub użytkownika reprezentującego stronę trzecią jakichkolwiek własnych działań w celu usunięcia incydentu w systemie teleinformatycznym jest zabronione.
2. Samodzielna próba usunięcia incydentu w systemie teleinformatycznym stanowi naruszenie podstawowych obowiązków pracowniczych i skutkuje odpowiedzialnością dyscyplinarną.

§ 5.

1. Po otrzymaniu zgłoszenia incydentu Dyrektor dokonuje wstępnej analizy incydentu.
2. Jeśli w ocenie Dyrektora incydent wpłynął na bezpieczeństwo informacji w systemie teleinformatycznym, niezwłocznie zawiadamia informatyka, a w przypadku, gdy dotyczył danych osobowych – inspektora ochrony danych.
3. Dyrektor wraz z informatykiem i, w przypadku danych osobowych, z inspektorem ochrony danych rozpatrują incydent uwzględniając następujące obszary:
   1) charakter incydentu,
   2) ilość obszarów dotkniętych incydentem,
   3) możliwość ograniczenia potencjalnego rozprzestrzenienia się incydentu,
   4) szacunkowy czas i zasoby potrzebne do zlikwidowania skutków incydentu i przywrócenie stanu informacji do poziomu sprzed incydentu,
   5) szacunkowy poziom szkód finansowych, prawnych i wizerunkowych.

§ 6.

1. Informatyk, aby ograniczyć skutki incydentu w systemie teleinformatycznym, może zablokować część systemu teleinformatycznego.
2. Jeśli sytuacja wymaga wyłączenia części sytemu teleinformatycznego potrzebnej do realizacji zadań ustawowych, informatyk uzgadnia z Dyrektorem działanie, uwzględniając czas, w którym Szkoła może funkcjonować bez systemu teleinformatycznego, stopień narażenia informacji na zagrożenie i zasoby potrzebne dla działań, które należy podjąć.

§ 7.

W przypadku, gdy zasięg incydentu wykracza poza system teleinformatyczny Szkoły, Dyrektor informuje o tym fakcie dostawcę usługi.

§ 8.

W przypadku każdego incydentu należy zweryfikować:

1) rzeczywiste uprawnienia pracowników, wykonawców lub użytkowników reprezentujących stronę trzecią do dostępu do pomieszczeń,
2) rzeczywiste zasoby, którymi dysponują pracownicy, wykonawcy lub użytkownicy reprezentujących stronę trzecią,
3) rzeczywiste uprawnienia pracowników, wykonawców lub użytkowników reprezentujących stronę trzecią w systemach teleinformatycznych.

§ 9.

1. W przypadku wykrycia próby nieautoryzowanego dostępu do serwera poprzez połączenie sieciowe należy:
   1) sprawdzić aktywne połączenia sieciowe na firewall oraz na serwerze,
   2) sprawdzić działające procesy na firewall i na serwerze,
   3) w przypadku podejrzanych połączeń lub procesów – odłączyć zewnętrzne interfejsy na firewall,
   4) sprawdzić ostatnio wgrane do serwera pliki,
   5) sprawdzić ostatnio uruchamiane polecenia i procesy,
   6) sprawdzić logi.
2. W przypadku, gdy próba nieautoryzowanego dostępu do serwera nastąpiła ze Szkoły, nie naruszono zasobów na serwerze oraz można określić sprawcę to należy zakończyć procedurę.
3. W przypadku, gdy nie miał miejsca przypadek, o którym mowa w ust. 2, należy zabezpieczyć komputer osoby podejrzanej, skontrolować integralność wszystkich systemów teleinformatycznych i w razie jej naruszenia odtworzyć w każdym z nich stan sprzed zdarzenia z kopii zapasowej.

§ 10.

1. W przypadku wykrycia próby nieautoryzowanego dostępu do komputera należy:
   1) sprawdzić, poprzez polecenie netstat, aktualnie aktywne połączenia sieciowe na komputerze, do którego nastąpiła próba nieautoryzowanego dostępu,
   2) odłączyć kabel sieciowy od komputera, do którego nastąpiła próba nieautoryzowanego dostępu,
   3) odłączyć system biurowy Windows od sieci Internet i sprawdzić uprawnienia do poszczególnych katalogów oraz udostępniane zasoby,
   4) sprawdzić logi,

5) sprawdzić konta i grupy dostępne w domenie Windows i na komputerze, do którego nastąpiła próba nieautoryzowanego dostępu.

2. W przypadku, gdy próba nieautoryzowanego dostępu do komputera nastąpiła z konta użytkownika, należy skontaktować się z tą osobą i wyjaśnia sytuację.
3. Jeżeli nie miał miejsca przypadek, o którym mowa w ust. 2, należy:
   1) sprawdzić fora dyskusyjne i strony internetowe dotyczące bezpieczeństwa systemu Windows oraz zainstalowanego oprogramowania – w przypadku, gdy zostały wykryte nowe błędy bezpieczeństwa zainstalować niezbędne uaktualnienia na wszystkich komputerach, których może dotyczyć błąd,
   2) wyjąć dyski twarde z komputera i zainstalować nową kopię systemu na innym dysku, jeżeli nadużycie nastąpiło z określonego konta lub komputera.
   3) jeżeli zachodzi podejrzenie, że zostały zmodyfikowane pliki systemowe lub pliki zainstalowanych programów zainstalować nową kopię systemu lub odtworzyć z kopii zapasowej.

§ 11.

1. W przypadku utraty danych z serwera należy:
   1) sprawdzić, poprzez polecenie netstat, aktualnie aktywne połączenia sieciowe,
   2) wyjąć kabel sieciowy z serwera, jeżeli pojawiłoby się jakieś podejrzane połączenie,
   3) sprawdzić logi.
2. Jeżeli w wyniku podjętych działań można jednoznacznie stwierdzić, że utrata danych nie jest wynikiem celowego i nieuprawnionego działania należy odtworzyć dane z kopii zapasowej.

§ 12.

1. W przypadku wykrycia obcego procesu na serwerze należy:
   1) sprawdzić, poprzez polecenie netstat, aktualnie aktywne połączenia sieciowe,
   2) wyjąć kabel sieciowy z serwera, jeżeli pojawiłoby się jakieś podejrzane połączenie,
   3) sprawdzić kto uruchomił i jak długo działa podejrzany proces i spróbować sprawdzić co proces robi,
   4) sprawdzić jakie pliki zostały ostatnio wgrane na serwer,
   5) sprawdzić logi,
   6) sprawdzić historię poleceń,
   7) jeżeli w wyniku podjętych działań nie można jednoznacznie wykluczyć, że działający proces nie jest obcym, potencjalnie niebezpiecznym procesem to należy kontynuować procedurę. W przeciwnym wypadku należy zakończyć procedurę,
   8) usunąć proces,
   9) skontrolować integralność systemu plików wszystkich systemów. W momencie stwierdzenia naruszenia odtworzyć z kopii zapasowych stan wszystkich systemów sprzed zdarzenia,

10) w czasie odtwarzania stanu poszczególnych systemów należy monitorować procesy i połączenia na dostępnych serwerach.

§ 13.

1. W przypadku nieautoryzowanego dostępu do systemu firewall poprzez połączenie sieciowe należy:
   1) sprawdzić aktualne aktywne połączenia sieciowe na poszczególnych elementach systemu firewall,
   2) sprawdzić logi poszczególnych elementów systemu firewall,
   3) sprawdzić reguły dostępu do poszczególnych elementów systemu firewall,
   4) w przypadku, gdy doszło do skanowania systemu firewall z sieci Internet ustalić nowe reguły blokujące dostęp z podejrzanego adresu do systemu firewall, a także do chronionych przez niego elementów sieci Szkoły oraz skontaktować się z ABUSE dostawcy usługi,
   5) sprawdzić stronę producentów poszczególnych elementów systemu, listy dyskusyjne i serwisy internetowe dotyczące bezpieczeństwa systemów firewall,
   6) w przypadku, gdy zostały odkryte nowe błędy bezpieczeństwa w użytkowanych elementach systemu firewall sprawdzić, czy na stornie internetowej producenta nie znajdują się poprawki eliminujące wykryte błędy – jeżeli są one dostępne, to należy je zainstalować,
   7) w przypadku, gdy doszło do udanej próby dostępu do poszczególnych elementów systemu firewall lub producent stosowanych systemów zabezpieczeń nie dostarczył niezbędnych poprawek należy spróbować określić, w jaki sposób oraz z jakiego miejsca nastąpił nieuprawniony dostęp do systemu firewall,
   8) zabezpieczyć logi systemu,
   9) w przypadku, gdy nieuprawniony dostęp nastąpił z sieci Internet skontaktować się z ABUSE dostawcy usługi,
   10) w przypadku, gdy nastąpił nieuprawniony dostęp do systemu firewall należy zainstalować kopię zapasową systemu (zarówno systemu operacyjnego jak i oprogramowania firewall) oraz zainstalować wszelkie niezbędne poprawki dostarczane przez producenta lub wezwać serwis producenta,
   11) w przypadku, gdy wykryte zostały luki bezpieczeństwa a producent nie dostarczył jeszcze odpowiednich poprawek wyłączyć system firewall. System ten musi być włączany wyłącznie na czas konieczny do umożliwienia replikacji danych pomiędzy serwerami i komputerami (do replikacji danych należy zestawiać wyłącznie połączenie VPN).
2. Przywrócenie systemu firewall do normalnego działania może nastąpić dopiero po usunięciu wszystkich luk systemowych.

§ 14.

1. Za realizację zadań, o których mowa w § 9 – 13 odpowiada informatyk.

2. Na każdym etapie postępowania informatyk, o ile to możliwe, zbiera materiał dowodowy, zachowując przy tym wszystkie atrybuty bezpieczeństwa.

§ 15.

Jeśli rodzaj i zasięg incydentu, zidentyfikowany na którymkolwiek z etapów postępowania, uzasadnia potrzebę powiadomienia organów ścigania, to decyzję o sposobie i terminie powiadomienia podejmuje Dyrektor.

§ 16.

1. Przy zachowaniu należytej staranności w odniesieniu do poufności, incydenty należy wykorzystywać jako element podnoszenia świadomości użytkowników, w szczególności jako przykład tego, co może się zdarzyć, jak reagować na takie incydenty oraz jak unikać ich w przyszłości.
2. Na podstawie analizy incydentów osoby wyznaczone przez Dyrektora tworzą rekomendację dotyczącą szkoleń i doskonalenia systemu zarządzania bezpieczeństwem informacji.

§ 17.

1. Pracownik Szkoły, wykonawca lub użytkownik reprezentujący stronę trzecią zobowiązany jest niezwłocznie zgłosić Dyrektorowi każdą słabość bezpieczeństwa w systemach teleinformatycznych lub usługach, zwanej w dalszej części słabością.
2. Zgłoszenia słabości należy dokonać na formularzu zgłoszenia zdarzenia związanego z bezpieczeństwem informacji lub ustnie.
3. W przypadku zgłoszenia ustnego Dyrektor lub wyznaczony przez Dyrektora pracownik wypełnia formularz zgłoszenia zdarzenia związanego z bezpieczeństwem informacji.

§ 18.

1. Podejmowanie przez pracownika, wykonawcę lub użytkownika reprezentującego stronę trzecią jakichkolwiek własnych działań w celu dowiedzenia istnienia podejrzewanej słabości jest zabronione.
2. Testowanie słabości stanowi naruszenie podstawowych obowiązków pracowniczych i skutkuje odpowiedzialnością dyscyplinarną.

§ 19.

Po usunięciu incydentu lub słabości, pracownikowi, wykonawcy lub użytkownikowi reprezentującemu stronę trzecią, który zgłosił zdarzenie związane z bezpieczeństwem informacji należy przekazać wyniki obsługi zdarzenia.

§ 20.

Informacje uzyskane z monitorowania i przeglądu incydentów należy oceniać i w razie potrzeby zalecać odpowiednie działania w stosunku do zidentyfikowanych incydentów w celu uniknięcia podobnych zdarzeń w przyszłości.

§ 21.

Nadzór nad realizacją „Procedury" sprawuje Dyrektor.

Załącznik do „Procedury zarządzania incydentami związanymi z bezpieczeństwem informacji" – wzór formularza zgłoszenia zdarzenia związanego z bezpieczeństwem informacji

FORMULARZ ZGŁOSZENIA ZDARZENIA ZWIĄZANEGO Z BEZPIECZEŃSTWEM INFORMACJI

W dniu ..... o godzinie ..... miało miejsce następujące zdarzenie związane z bezpieczeństwem informacji *(zaznaczyć właściwe)*:

- ☐ Utrata usługi, funkcjonalności lub urządzenia
- ☐ Przeciążenie lub niepoprawne działanie systemu informatycznego
- ☐ Niezgodność z procedurami lub zaleceniami
- ☐ Naruszenie ustaleń związanych z bezpieczeństwem fizycznym
- ☐ Niekontrolowane zmiany systemu informatycznego
- ☐ Niepoprawne działanie oprogramowania lub sprzętu
- ☐ Naruszenie dostępu
- ☐ Nieuprawiona lub nieautoryzowana modyfikacja, zniszczenie lub utrata informacji
- ☐ Inne *(opisać jakie)*:

.....

.....

.....

.....

Typ niezgodności lub naruszenia, błąd działania, wiadomość z ekranu, dziwne zachowanie:

.....

.....

.....

.....

Podejmowanie jakichkolwiek własnych działań w celu usunięcia lub testowania zdarzenia jest zabronione. Zdarzenie należy natychmiast zgłosić Dyrektorowi.

Osoba zgłaszająca zdarzenie

.....
(podpis)

Dyrektor

.....
(pieczątka i podpis)

Adnotacje informatyka:

.....

.....

.....

.....

.....

.....

Adnotacje inspektora ochrony danych:

.....

.....

.....

.....

.....

.....

Załącznik nr 6 do zarządzenia nr 7 – „Procedura postępowania w sytuacjach naruszenia ochrony danych osobowych"

PROCEDURA POSTĘPOWANIA W SYTUACJACH NARUSZENIA OCHRONY DANYCH OSOBOWYCH

§ 1.

1. „Procedura postępowania w sytuacjach naruszenia ochrony danych osobowych", zwana w dalszej części „Procedurą", określa zasady zgłaszania potencjalnych naruszeń ochrony danych osobowych oraz sposób zarządzania naruszeniami ochrony danych osobowych w Szkole Podstawowej z Oddziałami Integracyjnymi nr 36 im. Czesława Miłosza w Rybniku.
2. Ilekroć w „Procedurze" jest mowa o Dyrektorze należy przez to rozumieć Dyrektora Szkoły Podstawowej z Oddziałami Integracyjnymi nr 36 im. Czesława Miłosza w Rybniku lub osobę zastępującą.

§ 2.

1. Naruszenie ochrony danych osobowych należy rozumieć jako naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.
2. W szczególności jako naruszenie ochrony danych osobowych należy zakwalifikować utratę lub kradzież komputera, telefonu, pendrive itp., na którym były zapisane dane osobowe, utratę lub kradzież dokumentów papierowych zawierających dane osobowe, uzyskanie dostępu do danych osobowych przez osobę, która nie jest do tego upoważniona, atak hakerski skutkujący zniszczeniem, utratą dostępu, zmodyfikowaniem lub ujawnieniem danych osobowych, włamanie do pomieszczenia, w którym przechowywane są dane osobowe, udostępnienie danych osobowych osobom niepowołanym.

§ 3.

1. Każda osoba w sytuacji dowiedzenia się o potencjalnym naruszeniu ochrony danych osobowych bezzwłocznie, najpóźniej w ciągu jednej godziny, zgłasza ten fakt Dyrektorowi, w szczególności podając wszystkie ważne szczegóły, takie jak rodzaj zdarzenia, typ niezgodności, błąd działania, wiadomość z ekranu czy dziwne zachowanie, a następnie Dyrektor – inspektorowi ochrony danych.
2. Podejmowanie przez pracownika jakichkolwiek własnych działań w celu usunięcia potencjalnego naruszenia jest zabronione, chyba że mają na celu ograniczenie skutków potencjalnego naruszenia.

§ 4.

1. W sytuacji dowiedzenia się o potencjalnym naruszeniu ochrony danych osobowych inspektor ochrony danych natychmiast przeprowadza wewnętrzne postępowanie w celu ustalenia okoliczności naruszenia oraz jego skutków, a także podejmuje niezwłoczne działania w celu naprawienia lub zapobieżenia skutkom naruszenia.
2. W ramach wewnętrznego postępowania, o którym mowa w pkt. 1, należy ustalić:
   1) datę i czas wystąpienia incydentu prowadzącego do naruszenia,
   2) datę i czas dowiedzenia się o incydencie prowadzącym do naruszenia,
   3) opis incydentu, charakter naruszenia oraz opis ustalonych lub potencjalnych skutków naruszenia,
   4) przyczynę powstania incydentu,
   5) kategorię osób, których danych osobowych dotyczy naruszenie,
   6) przybliżoną liczbę osób, których danych osobowych dotyczy naruszenie,
   7) kategorię danych osobowych, których dotyczy naruszenie,
   8) przybliżoną liczbę wpisów (rekordów) danych osobowych, których dotyczy naruszenie,
   9) opis podjętych środków zaradczych lub naprawczych, o ile zostały podjęte,
   10) ocenę ryzyka naruszenia praw i wolności osób fizycznych wynikającego z naruszenia ochrony danych, w tym w szczególności, czy prawdopodobne jest, by konkretne naruszenie skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych lub czy naruszenie może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych w rozumieniu art. 33 i 34 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych),
   11) możliwe konsekwencje naruszenia ochrony danych dla osób fizycznych,
   12) środki, rekomendacje, plany postępowania, które powinny zostać zastosowane w celu zaradzenia naruszeniu ochrony danych, w tym środki w celu zminimalizowania jego ewentualnych negatywnych skutków dla osób, których dane dotyczą.

§ 5.

1. W przypadku naruszenia ochrony danych osobowych Dyrektor bez zbędnej zwłoki – w miarę możliwości nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – zgłasza je Prezesowi Urzędu Ochrony Danych Osobowych, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych.
2. Za datę i czas stwierdzenia naruszenia uznaje się moment, w którym ustalono, że doszło z wystarczającą pewnością do naruszenia ochrony danych osobowych.

3. Jeśli rodzaj i zasięg naruszenia, zidentyfikowany na którymkolwiek z etapów postępowania, uzasadnia potrzebę powiadomienia organów ścigania, to decyzję o sposobie i terminie powiadomienia podejmuje Dyrektor.

§ 6.

1. Przy zachowaniu należytej staranności w odniesieniu do poufności, naruszenie ochrony danych osobowych należy wykorzystywać jako element podnoszenia świadomości użytkowników, w szczególności jako przykład tego, co może się zdarzyć, jak reagować na takie naruszenia oraz jak unikać ich w przyszłości.
2. Na podstawie analizy zgłoszeń potencjalnych naruszeń ochrony danych osobowych inspektor ochrony danych tworzy rekomendację dotyczącą szkoleń i doskonalenia zasad ochrony danych osobowych.

§ 7.

W sprawach nieuregulowanych w „Procedurze" decyzję podejmuje Dyrektor.

§ 8.

Nadzór nad realizacją „Procedury" sprawuje Dyrektor.