PRZEDSZKOLE
Z ODDZIAŁAMI INTEGRACYJNYMI NR 39
w Rybniku
44-253 Rybnik, Os. Południe 20
NIP 6423148167, Regon 241795560

Zarządzenie nr 2/2023

dyrektora Przedszkola z Oddziałami Integracyjnymi nr 39 w Rybniku

z dnia 29 marca 2023 roku

w sprawie ustanowienia, wdrożenia, eksploatacji, monitorowania, przeglądu, utrzymania i doskonalenia „Systemu zarządzania bezpieczeństwem informacji" w Przedszkolu z Oddziałami Integracyjnymi nr 39 w Rybniku

Na podstawie art. 24 i art. 32 ust. 1 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 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 § 20 ust. 1 rozporządzenia Rady Ministrów z 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.

Ustanawiam „System zarządzania bezpieczeństwem informacji", który stanowi załącznik do zarządzenia.

§ 2.

Wykonanie zarządzenia powierzam pracownikom Przedszkola.

§ 3.

Tracą moc:

1) Zarządzenie nr 5/2015 z 12 czerwca 2015 roku ustanowienia, wdrożenia, eksploatacji, monitorowania, przeglądu, utrzymania i doskonalenia „Systemu zarządzania bezpieczeństwem informacji",

2) Zarządzenie nr 13 z 19 października 2020 roku w sprawie wprowadzenia „Procedury zarządzania ryzykiem naruszenia praw lub wolności osób fizycznych" oraz zmiany „Procedury zarządzania ryzykiem w bezpieczeństwie informacji".

§ 4.

Zarządzenie wchodzi w życie z dniem podpisania.

DYREKTOR
Przedszkola
z Oddziałami Integracyjnymi nr 39
w Rybniku
mgr Anna Kubera

Załącznik do zarządzenia nr 2/2023 – „System zarządzania bezpieczeństwem informacji"

SYSTEM ZARZĄDZANIA BEZPIECZEŃSTWEM INFORMACJI

§ 1.

1. Informacje to aktywa, które, podobnie jak inne aktywa, są niezbędne dla prawidłowego funkcjonowania Przedszkola z Oddziałami Integracyjnymi nr 39 w Rybniku, zwanego dalej Przedszkolem, i z tego powodu podlegają ochronie.
2. Informacja przybiera różne formy – może być wydrukowana lub zapisana na papierze, przechowywana elektronicznie, przesyłana pocztą i za pomocą nośników elektronicznych lub wypowiadana w rozmowie.
3. Bezpieczeństwo informacji oznacza ochronę informacji przed zagrożeniami w celu zapewnienia ciągłości działania, efektywnego wykorzystania informacji i minimalizacji ryzyka.

§ 2.

1. Celem „Systemu zarządzania bezpieczeństwem informacji" jest zapewnienie poufności, dostępności i integralności informacji, niezaprzeczalności odbioru i nadania informacji oraz rozliczalności działań.
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.
5. Niezaprzeczalność odbioru oznacza zdolność systemu informatycznego do udowodnienia, że adresat informacji otrzymał ją w określonym miejscu i czasie.
6. Niezaprzeczalność nadania oznacza zdolność systemu informatycznego do udowodnienia, że nadawca informacji faktycznie ją nadał lub wprowadził do systemu informatycznego
   w określonym miejscu i czasie.

7. Rozliczalność działań oznacza zapewnienie, że wszystkie działania istotne dla przetwarzania informacji zostały zarejestrowane w systemie informatycznym i możliwym jest zidentyfikowanie użytkownika, który działania wykonał.

§ 3.

1. „System zarządzania bezpieczeństwem informacji" został zaprojektowany tak, aby zapewnić adekwatne i proporcjonalne zabezpieczenia, które odpowiednio chronią informacje, oraz uzyskać zaufanie zainteresowanych stron.
2. „System zarządzania bezpieczeństwem informacji" opiera się na modelu planuj – wykonuj – sprawdzaj – działaj (PDCA).
3. „System zarządzania bezpieczeństwem informacji" jest w razie potrzeby poddawany przeglądowi i uaktualniany.
4. „System zarządzania bezpieczeństwem informacji" stosuje każdy pracownik przetwarzający informacje. Przez przetwarzanie informacji należy rozumieć operację lub zestaw operacji wykonywanych na informacji, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie. Przez pracownika należy rozumieć osobę zatrudnioną w Przedszkolu przez mianowanie, na podstawie umowy o pracę, umowy zlecenie lub umowy o dzieło.

§ 4.

Zarządzanie bezpieczeństwem informacji jest realizowane poprzez 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 informatycznych, 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 ryzyka wynikającego z wykorzystania opublikowanych podatności technicznych systemów informatycznych,

g) niezwłocznym podejmowaniu działań po dostrzeżeniu nieujawnionych podatności systemów informatycznych na możliwość naruszenia bezpieczeństwa,

h) kontroli zgodności systemów informatycznych 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 w zakresie bezpieczeństwa informacji, nie rzadziej niż raz w roku.

§ 5.

1. W Przedszkolu wyodrębnia się cztery grupy informacji:
   1) tajemnice ustawowo chronione,
   2) dane osobowe,
   3) informacje o charakterze wewnętrznym (np. organizacyjnym, porządkowym),
   4) pozostałe informacje.
2. Poziom ochrony informacji szacuje się poprzez analizę atrybutów poufności, integralności i dostępności dla rozważanej grupy informacji i przyjmuje się, że:
   1) tajemnice ustawowo chronione, dane osobowe i informacje o charakterze wewnętrznym są informacjami poufnymi, chronionymi przed dostępem nieuprawnionych osób, dostępnymi w sposób nieprzerwany, chronionymi przed nieuprawnioną modyfikacją,
   2) pozostałe informacje są informacjami ogólnodostępnymi lub dostępnymi na wniosek, w sposób nieprzerwany, chronionymi przed nieuprawnioną modyfikacją.
3. W przypadku, kiedy dane osobowe przetwarzane są na podstawie zgody osoby, której dane dotyczą, za uzyskanie zgody odpowiada pracownik, który jako pierwszy przetwarzać będzie te dane.

§ 6.

1. Dostęp do informacji realizowany jest zgodnie z:
   1) zasadą wiedzy uzasadnionej – dostęp do informacji uzasadniony jest potrzebami wynikającymi z pełnionych obowiązków służbowych i wynika wprost z zakresu czynności, opisu stanowiska lub innego dokumentu uzasadniającego dostęp do informacji,
   2) zasadą minimalnych uprawnień – zakres dostępu do informacji nie może wykraczać poza potrzeby wynikające z pełnionych obowiązków i powinien być najmniejszym zbiorem praw dostępu pozwalającym na efektywne pełnienie obowiązków służbowych.
2. Dodatkowo dostęp do danych osobowych może zostać potwierdzony pisemnym upoważnieniem do przetwarzania danych osobowych.
3. Wzór upoważnienia do przetwarzania danych osobowych i odwołania upoważnienia do przetwarzania danych osobowych stanowią załącznik do „Systemu zarządzania bezpieczeństwem informacji". Dopuszcza się stosowanie innego wzoru upoważnienia do przetwarzania danych osobowych i jego odwołania, w szczególności, jeśli wzór taki wynika z obowiązujących Przedszkole umów.
4. Upoważnienie do przetwarzania danych osobowych i jego odwołanie przygotowuje i podpisuje dyrektor.
5. 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 Przedszkola.

§ 7.

1. Osoby, które przetwarzają informacje, powinny przejść obowiązkowe szkolenie z zakresu bezpieczeństwa informacji.
2. Tematyka szkolenia powinna obejmować w szczególności:
   1) aktualny system prawny bezpieczeństwa informacji w Polsce,
   2) wewnętrzne regulacje związane z bezpieczeństwem informacji w Przedszkolu,

3) zagrożenia dla bezpieczeństwa informacji w odniesieniu do specyfiki działalności Przedszkola,
4) role i zadania poszczególnych osób odpowiedzialnych za bezpieczeństwo informacji,
5) zasady udzielania dostępu do informacji,
6) zasady przetwarzania informacji w systemach informatycznych,
7) procedury postępowania w sytuacji naruszenia bezpieczeństwa informacji,
8) odpowiedzialność dyscyplinarna, finansowa i karna za nieprzestrzeganie zasad bezpieczeństwa informacji.

3. Szkolenie, w zależności od potrzeb i możliwości, może zostać przeprowadzone w formie tradycyjnego wykładu, udostępnienia materiałów szkoleniowych, wideokonferencji, kursu
e-learningowego itp.
4. Szkolenie przeprowadza inspektor ochrony danych.

§ 8.

1. Teren Przedszkola zabezpieczony jest monitoringiem wizyjnym.
2. Monitoring wizyjny obejmuje na zewnątrz obejście budynku Przedszkola, a wewnątrz szatnie i aulę. Nagrania obrazu są przechowywane przez okres 7 dni od dnia nagrania.
3. W przypadku, w którym nagrania obrazu stanowią dowód w postępowaniu prowadzonym na podstawie prawa lub Przedszkole powzięło wiadomość, iż mogą one stanowić dowód
w postępowaniu, termin określony w ust. 2 ulega przedłużeniu do czasu prawomocnego zakończenia postępowania.
4. Wejścia do budynku zabezpieczone są zamkami drzwiowymi, a wejście od frontu – dodatkowo domofonem.
5. Pomieszczenia, w których przetwarzane są informacje, wyposażone są w niezależne zamki i pozostają zamknięte podczas nieobecności pracownika.
6. Należy przestrzegać zasad postępowania z kluczami obowiązującymi w Przedszkolu, które zostały określone w odrębnych dokumentach lub przyjęte zwyczajowo, a w szczególności nie można pozostawiać kluczy dostępnych dla osób nieuprawnionych.

7. Drzwi i okna w pomieszczeniach pod nieobecność uprawnionych osób powinny być zamykane, z zastrzeżeniem wymogów sanitarno-higienicznych.

§ 9.

1. Przetwarzając dokumenty zawierające tajemnice ustawowo chronione lub dane osobowe należy stosować zasadę czystego biurka – niewykorzystywane w danej chwili dokumenty należy przechowywać pod zamknięciem, szczególnie jeśli pomieszczenie jest opuszczane, a w przypadku obsługi osoby nieuprawnionej – poza zasięgiem jej wzroku.
2. Dokumenty zawierające tajemnice ustawowo chronione lub dane osobowe po ustaniu ich przydatności do bieżącego przetwarzania oraz braku obowiązku prawnego ich dalszego archiwizowania, podlegają zniszczeniu w przeznaczonych do tego urządzeniach. Niedopuszczalne jest wyrzucanie do kosza na śmieci jakichkolwiek dokumentów zawierających tajemnice ustawowo chronione lub dane osobowe, bez względu na ich zawartość informacyjną czy upływ czasu od ich wytworzenia.
3. Pracownik, którego stanowisko pracy wyposażone jest w tablicę korkową, magnetyczną itp., zobowiązany jest do niezamieszczania na tablicy żadnych tajemnic ustawowo chronionych lub danych osobowych.
4. Nie należy pozostawiać osoby nieuprawnionej w pomieszczeniu bez nadzoru, także wtedy, kiedy stanowisko komputerowe jest wyłączone lub wylogowane, a dokumenty zawierające tajemnice ustawowo chronione lub dane osobowe umieszczone w zamkniętej szafie.

§ 10.

1. Prowadząc rozmowę telefoniczną, w trakcie której przekazywane są tajemnice ustawowo chronione lub dane osobowe, należy zwracać uwagę na możliwość podsłuchania rozmowy telefonicznej przez osoby nieuprawnione znajdujące się w bezpośrednim sąsiedztwie.
2. Nie wolno pozostawiać w automatycznych sekretarkach wiadomości zawierających tajemnice ustawowo chronione lub dane osobowe.

§ 11.

Korzystając z drukarki, kopiarki lub faksu należy być świadomym, że urządzenia te wyposażone są w podręczną pamięć, w której przechowywane są strony na wypadek błędów transmisji lub braku papieru, a drukują zaraz po usunięciu błędu – należy niezwłocznie usuwać dokumenty zawierające tajemnice ustawowo chronione lub dane osobowe.

§ 12.

1. Środki uwierzytelniania dostępu do pracy na komputerze i z wykorzystaniem oprogramowania służącego do przetwarzania informacji to identyfikator użytkownika i hasło dostępu. Zamiast hasła dostępu dopuszczalne jest stosowanie kart chipowych, PIN-ów, czytników linii papilarnych, skanerów twarzy lub tęczówki oka itp.
2. Identyfikator użytkownika jest w sposób jednoznaczny przypisany danemu użytkownikowi. Ewidencję identyfikatorów użytkownika prowadzi informatyk. Przez informatyka należy rozumieć pracownika Centrum Usług Wspólnych w Rybniku, który czuwa nad sprawnym i ciągłym działaniem systemów teleinformatycznych.
3. Użytkownik jest odpowiedzialny za wszystkie czynności wykonane przy użyciu identyfikatora użytkownika, którym się posługuje lub posługiwał.
4. Przydzielanie użytkownikowi uprawnień do kasowania lub dezaktywacji rejestrów zdarzeń zawierających zapisy o jego własnych działaniach jest zabronione.
5. Identyfikator użytkownika po wyrejestrowaniu użytkownika z komputera i oprogramowania służącego do przetwarzania informacji nie może być przydzielony innemu użytkownikowi.
6. Identyfikator użytkownika, który utracił prawo dostępu do pracy na komputerze i z wykorzystaniem oprogramowania służącego do przetwarzania informacji, powinien zostać zablokowany przez informatyka.
7. Informatyk rejestruje użytkownika w komputerze i w oprogramowaniu służącym do przetwarzania informacji poprzez utworzenie identyfikatora użytkownika i nadaje jednorazowe hasło dostępu, które powinno zostać zmienione przy pierwszym logowaniu użytkownika. Zmianę hasła dostępu powinien wymuszać, jeżeli to technicznie możliwe, system operacyjny lub oprogramowanie służące do przetwarzania informacji.
8. Jednorazowe hasło dostępu nie może być przekazywane użytkownikowi za pośrednictwem osób trzecich.

9. Przed rozpoczęciem pracy na komputerze użytkownik sprawdza, czy nie ma oznak fizycznego naruszenia zabezpieczeń.
10. Po uruchomieniu komputera użytkownik powinien się zalogować – wprowadzić przydzielony identyfikator użytkownika i hasło dostępu.
11. Jeżeli w trakcie logowania wystąpi błąd, system nie powinien wskazywać, która część danych jest poprawna lub niepoprawna.
12. W trakcie logowania się do komputera lub oprogramowania służącego do przetwarzania informacji użytkownik nie powinien odchodzić od komputera.
13. Po poprawnym zalogowaniu się, użytkownik rozpoczyna pracę na komputerze lub z wykorzystaniem oprogramowania służącego do przetwarzania informacji.
14. W trakcie pracy ekran monitora komputera powinien być ustawiony w sposób uniemożliwiający osobie nieuprawnionej wgląd lub spisanie informacji wyświetlanych na ekranie monitora, a w przypadku korzystania z funkcji udostępniania ekranu lub podobnej – spisanie, odczytanie, sfotografowanie, skopiowanie, wydrukowanie itp. informacji.
15. Przy każdorazowym opuszczeniu pomieszczenia biurowego, użytkownik powinien zablokować komputer lub wylogować się. Przez pomieszczenie biurowe należy rozumieć pomieszczenia indywidualne lub wnętrza grupowe. W przypadku, gdy dwa pomieszczenia indywidualne lub grupowe połączone są drzwiami należy je traktować jak jedno pomieszczenie biurowe.
16. Blokada komputera następuje po naciśnięciu skrótu klawiszowego Windows + L lub klawiszy Ctrl + Alt + Delete i wybranie opcji „Zablokuj komputer".
17. Zmianę użytkownika komputera każdorazowo powinno poprzedzać wylogowanie się poprzedniego użytkownika.
18. Przed zakończeniem pracy na komputerze użytkownik powinien zapisać wszystkie zmiany, a następnie wylogować się z uruchomionego oprogramowania.
19. 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 itp.),

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 powinno być jednakowe z identyfikatorem użytkownika,
5) hasło dostępu powinno być unikalne, tj. takie, które nie było poprzednio stosowane przez użytkownika,
6) hasło dostępu nie powinno być podatne na atak słownikowy, tj. nie powinno zawierać słów zamieszczonych w słownikach.

20. Hasło dostępu w trakcie wpisywania nie powinno być wyświetlane na ekranie.
21. Hasło dostępu powinno być utrzymywane w tajemnicy, również po utracie jego ważności.
22. Hasło dostępu nie powinno być przechowywane w systemach informatycznych w niechronionej postaci.
23. Hasło dostępu nie powinno być nigdzie zapisywane.
24. Hasło dostępu nie powinno być wprowadzone do jakichkolwiek zautomatyzowanych procesów logowania się do komputera i do oprogramowania służącego do przetwarzania informacji.
25. Hasło dostępu nie powinno być przechowywane w makrach ani przypisane do klawiszy funkcyjnych.
26. Zaleca się zmianę hasła dostępu nie rzadziej niż co 30 dni.
27. Hasło dostępu powinno być zmieniane przez użytkownika.

§ 13.

1. Informacje i oprogramowanie służące do przetwarzania informacji należy zabezpieczać poprzez wykonywanie kopii zapasowych.
2. Kopie zapasowe oprogramowania Optivum wykonywane są automatycznie na serwerze firmy Vulcan.

§ 14.

1. Tajemnice ustawowo chronione i dane osobowe przetwarzane są na nośnikach (telefon komórkowy, pendrive, dysk, pamięć typu flash, zewnętrzny dysk twardy, płyta CD lub

DVD itp.) wyłącznie, gdy istnieje konieczność przeniesienia tajemnic ustawowo chronionych lub danych osobowych w postaci elektronicznej, a wykorzystanie do tego celu sieci Internet jest nieuzasadnione, niemożliwe lub zbyt niebezpieczne.

2. Przetwarzanie tajemnic ustawowo chronionych lub danych osobowych na nośnikach, które nie podlegają kryptograficznej ochronie jest zabronione.
3. Nośniki użyte do przetwarzania tajemnic ustawowo chronionych lub danych osobowych mogą być wykorzystywane do innych celów wyłącznie po skasowaniu danych osobowych lub nadpisaniu za pomocą technik uniemożliwiających ich odtworzenie.
4. Tajemnice ustawowo chronione lub dane osobowe zapisane na nośnikach, które mają być dostępne przez czas dłuższy niż czas życia nośników (zgodnie z danymi producenta), powinny być przechowywane w innym miejscu i w taki sposób, aby uniknąć utraty danych osobowych na skutek pogorszenia się jakości nośników lub utraty właściwości nośników.
5. Nośniki należy przechowywać w zamkniętych szafach lub szufladach w sposób zabezpieczający nośnik przed nieuprawnionym przejęciem i zniszczeniem.
6. Nośniki należy przechowywać zgodnie z zaleceniami producenta.
7. W trakcie transportu nośników należy chronić zawartość przed fizycznym uszkodzeniem, wpływem temperatury, wilgotności, pola elektromagnetycznego, które mogą pogorszyć skuteczność odtworzenia danych osobowych z nośników, w szczególności poprzez opakowanie zgodne z zaleceniami producenta.
8. W trakcie przekazywania nośników należy stosować zasadę dostarczania do rąk własnych odbiorcy osobiście, pocztą tradycyjną, kurierską itp.
9. Użytkowanie nośników poza Przedszkolem to przetwarzanie mobilne.
10. W przypadku przekazania nośników do ponownego użycia, należy skasować zapisane na nośnikach tajemnice ustawowo chronione, dane osobowe i licencjonowane oprogramowanie służące do przetwarzania informacji, do których przyszły użytkownik nie ma dostępu, a w przypadku zbycia lub zniszczenia – wszystkie tajemnice ustawowo chronione, dane osobowe i licencjonowane oprogramowanie służące do przetwarzania informacji podlegają kasowaniu lub nadpisaniu za pomocą technik uniemożliwiających ich odtworzenie.
11. Nośniki należy likwidować poprzez spopielenie, pocięcie lub uszkodzenie w taki sposób, aby nie było możliwe ponowne wykorzystanie nośników.

12. W przypadku niszczenia dokumentów tradycyjnych należy odpowiadające im zapisy na nośnikach usunąć lub zabezpieczyć przed ich odczytaniem, o ile jest to zasadne.

§ 15.

Korzystając z Internetu nie wolno:

1) prowadzić ataków, włamań i innych działań związanych z ingerencją w dane komputerów innych użytkowników oraz komputerów lub urządzeń mobilnych w Internecie, a także świadomego lub nieświadomego prowadzenia innych działań destrukcyjnych,
2) utrudniać lub uniemożliwiać innym użytkownikom korzystanie z Internetu poprzez uruchamianie oprogramowania nadmiernie obciążającego transfer,
3) wprowadzać jakichkolwiek nieuzgodnionych z informatykiem zmian we właściwościach połączeń sieciowych komputera, w szczególności adresu IP, MAC oraz nie rozpowszechniać tych ustawień konfiguracyjnych osobom trzecim,
4) przeglądać stron WWW potencjalnie niebezpiecznych w szczególności zawierających pornografię, hazard lub cracki,
5) wykorzystywać Internetu do prowadzenia działalności niezgodnej z przepisami prawa, w szczególności do rozsyłania niechcianej poczty elektronicznej (spam) oraz wymiany plików w sieciach typu P2P,
6) uruchamiać oprogramowania umożliwiającego przejmowanie zdalnej kontroli nad komputerem lub urządzeniem przenośnym będącym własnością Przedszkola, z zastrzeżeniem § 16 ust. 4.

§ 16.

1. Przy przetwarzaniu mobilnym informacji (poza Przedszkolem z wykorzystaniem urządzeń przenośnych, w tym notebooków, palmtopów, laptopów, tabletów, kart elektronicznych, telefonów komórkowych itp., także prywatnych) należy:
   1) stosować środki uwierzytelniania określone w § 12, o ile jest to technicznie możliwe,
   2) nie korzystać z otwartych sieci internetowych WiFi, tzw. hot spot,
   3) unikać ryzyka podglądania ze strony nieuprawnionych osób, w tym członków rodziny,
   4) nie pozostawiać zalogowanego komputera bez nadzoru, w tym nie dopuszczać do korzystania z zalogowanego komputera przez nieuprawnione osoby, w tym członków rodziny,

5) stosować oprogramowanie antywirusowe określone w § 18,
6) przewozić urządzenia przenośne zgodnie z zaleceniami producenta i jako bagaż podręczny,
7) stosować zalecenia producenta dotyczące ochrony, w tym ochrony przed wystawieniem na silne pola elektromagnetyczne, wpływem temperatury, wilgotności,
8) tworzyć kopie zapasowe na zasadach określonych w § 13, o ile jest to technicznie możliwe,
9) zbędne lub niepotrzebne informacje kasować.

2. Urządzenia przenośne podlegają prewencji programowej i technicznej.
3. O przeprowadzeniu prewencji programowej i technicznej urządzeń przenośnych będących własnością Przedszkola decyduje informatyk, a urządzeń przenośnych niebędących własnością Przedszkola – użytkownik.
4. Wszelkie czynności związane z instalacją oprogramowania i konfiguracją urządzeń przenośnych będących własnością Przedszkola wykonuje informatyk osobiście lub zdalnie z wykorzystaniem oprogramowania do zdalnego zarządzania lub serwis zewnętrzny.

§ 17.

1. W przypadku konieczności wymiany tajemnic ustawowo chronionych lub danych osobowych w postaci elektronicznej (poczta elektroniczna), zalecane jest, jeśli jest to organizacyjnie i technicznie możliwe, korzystanie wyłącznie z formy załączników z uwzględnieniem poniższych zasad:
   1) przetwarzane załączniki zawierające tajemnice ustawowo chronione lub 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.

2. Przesyłając pocztą elektroniczną wiadomości zawierające tajemnice ustawowo chronione lub dane osobowe należy dodatkowo zwracać szczególną uwagę na poprawność adresu poczty elektronicznej adresata.
3. Obierając wiadomości przesłane pocztą elektroniczną nie wolno uruchamiać wykonywalnych załączników (inaczej uruchamialnych; z rozszerzeniem .com i .exe lub z ustawionym atrybutem wykonywalności oznaczonym literą x) dołączonych do wiadomości.
4. W trakcie wysyłania wiadomości pocztą elektroniczną do kilku osób spoza Przedszkola nie należy ujawniać poszczególnych prywatnych adresów mailowych – adresując korespondencję należy korzystać z opcji UDW (lub BCC). W takim przypadku nie wolno korzystać z opcji DO (lub TO) oraz DW (lub CC).

§ 18.

1. Niedopuszczalne jest przetwarzanie informacji w postaci elektronicznej bez stosowania profilaktyki i ochrony przed złośliwym oprogramowaniem, chyba że jest to technicznie niemożliwe.
2. 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, właściwych mechanizmach kontroli dostępu oraz zarządzania zmianami,
   3) stałe monitorowanie komunikatów pochodzących z zainstalowanego oprogramowania antywirusowego,
   4) zakaz korzystania z nieautoryzowanego przez informatyka oprogramowania,
   5) zakaz korzystania z nielegalnego oprogramowania,
   6) zakaz korzystania z sieci Internet bez aktywnej ochrony oprogramowaniem antywirusowym,
   7) sprawdzanie (skanowanie) oprogramowaniem antywirusowym komputerów i elektronicznych nośników informacji, w tym tych otrzymywanych spoza Przedszkola oraz wiadomości elektronicznych,

8) korzystanie z list dyskusyjnych i sprawdzanie stron internetowych zamieszczających informacje o złośliwym oprogramowaniu,
9) tworzenie kopii zapasowych.

3. Oprogramowanie antywirusowe, o którym mowa w § 18 ust. 2 pkt 1), powinno mieć zdolność:
   1) wykrycia i zablokowania każdego rodzaju szkodliwego ataku,
   2) integracji z systemem operacyjnym i kluczowym oprogramowaniem,
   3) ciągłego nadzoru „w tle" nad pracą systemu informatycznego,
   4) kontroli przepływu danych do i z sieci Internet,
   5) kontroli i blokowania niechcianej poczty elektronicznej,
   6) blokowania dostępu do określonych stron i aplikacji internetowych,
   7) analizy nośników,
   8) rejestracji udanych i nieudanych prób dostępu do systemu informatycznego przy wykorzystaniu sieci Internet,
   9) automatycznej aktualizacji wzorców złośliwego oprogramowania.
4. 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.

§ 19.

Informacje należy usuwać permanentnie – także z folderów pn. kosz, pobrane, wymiana itp. lub od razu używać skrótu klawiszowego Shift + Delete.

§ 20.

1. Informatyk utrzymuje aktualność inwentaryzacji środków przetwarzania informacji w formie elektronicznej z wykorzystaniem oprogramowania OSC Inventory.
2. Przez środki przetwarzania rozumie się komputery stacjonarne i przenośne, drukarki, kopiarki, skanery, serwery, faksy, oprogramowanie oraz inne urządzenia służące do przetwarzania informacji.

§ 21.

Informatyk okresowo przegląda rejestry zdarzeń (logi) w celu wykrycia ewentualnych nadużyć. Przeprowadzenie przeglądu powinno zostać udokumentowane.

§ 22.

Informatyk regularnie śledzi i analizuje opublikowane podatności techniczne wykorzystywanego w Przedszkolu oprogramowania.

§ 23.

Wykorzystywane w Przedszkolu oprogramowanie powinno pracować w trybie automatycznych aktualizacji.

§ 24.

Dostęp do plików systemowych i dokumentacji systemowej posiada dyrektor i informatyk.

§ 25.

1. Hasła administratora przechowywane są w kancelarii Przedszkola.
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 informatycznym, w tym nadawania i zabierania uprawnień innym użytkownikom systemu informatycznego.
3. Z hasła administratora korzysta informatyk.
4. Hasło administratora generuje informatyk, chyba, że zostało nadane przez producenta środka przetwarzania informacji i z przyczyn technicznych wygenerowanie hasła administratora nie jest możliwe.
5. Informatyk zapisuje hasło administratora i każde w odrębnej, zaklejonej kopercie przekazuje dyrektorowi. Na każdej kopercie powinna znajdować się data i nazwa systemu informatycznego lub oprogramowania, do którego stosowane jest hasło administratora. Dopuszczalne jest także zapisywanie hasła administratora z wykorzystaniem innego nośnika.
6. W przypadku konieczności awaryjnego użycia hasła administratora, dyrektor wydaje hasło administratora osobie uprawnionej i fakt ten odnotowuje na kopercie wpisując datę.

§ 26.

1. Pracownik w sytuacji dowiedzenia się o potencjalnym naruszeniu bezpieczeństwa informacji 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 jeśli naruszenie bezpieczeństwa dotyczy danych osobowych – także inspektorowi ochrony danych.
2. Przez naruszenie bezpieczeństwa informacji należy rozumieć naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do informacji przesyłanych, przechowywanych lub w inny sposób przetwarzanych.
3. W szczególności jako naruszenie bezpieczeństwa informacji należy zakwalifikować utratę lub kradzież komputera, telefonu komórkowego, pendrive itp., na którym były zapisane informacje, utratę lub kradzież dokumentów papierowych, uzyskanie dostępu do informacji przez osobę, która nie jest do tego uprawniona, atak hackerski skutkujący zniszczeniem, utratą dostępu, zmodyfikowaniem lub ujawnieniem informacji, włamanie do pomieszczenia, w którym przechowywane są informacje, udostępnienie informacji osobom niepowołanym.
4. Podejmowanie przez pracownika jakichkolwiek własnych działań w celu usunięcia potencjalnego naruszenia bezpieczeństwa informacji jest zabronione, chyba że mają na celu ograniczenie skutków potencjalnego naruszenia.
5. W sytuacji dowiedzenia się o potencjalnym naruszeniu bezpieczeństwa informacji dyrektor natychmiast przeprowadza wewnętrzne postępowanie w celu ustalenia okoliczności naruszenia oraz jego skutków, a także podejmuje niezwłoczne działania w celu naprawienia lub zapobieżenia skutkom naruszenia.
6. W przypadku naruszenia bezpieczeństwa 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, których dane dotyczą.

7. Za datę i czas stwierdzenia naruszenia bezpieczeństwa danych osobowych uznaje się moment, w którym ustalono, że doszło z wystarczającą pewnością do naruszenia bezpieczeństwa danych osobowych.
8. Jeśli rodzaj i zasięg naruszenia bezpieczeństwa informacji, zidentyfikowany na którymkolwiek z etapów postępowania, uzasadnia potrzebę powiadomienia organów ścigania, to decyzję o sposobie i terminie powiadomienia podejmuje dyrektor.
9. Przy zachowaniu należytej staranności w odniesieniu do poufności, naruszenie bezpieczeństwa informacji należy wykorzystywać jako element podnoszenia świadomości pracowników, w szczególności jako przykład tego, co może się zdarzyć, jak reagować na takie naruszenia oraz jak unikać ich w przyszłości.
10. Na podstawie analizy zgłoszeń potencjalnych naruszeń bezpieczeństwa informacji, dyrektor, a w przypadku danych osobowych – inspektor ochrony danych tworzy rekomendację dotyczącą szkoleń i doskonalenia zasad bezpieczeństwa informacji.

§ 27.

1. Okresowo przeprowadzana jest analiza ryzyka utraty integralności, dostępności lub poufności informacji oraz analiza ryzyka naruszenia praw i wolności osoby, której dane dotyczą.
2. Ryzyko to wskaźnik stanu lub zdarzenia, które może prowadzić do strat. Ryzyko jest proporcjonalne do prawdopodobieństwa wystąpienia tego zdarzenia i do wielkości strat, które może spowodować.
3. Zarządzanie ryzykiem to skoordynowane działania dotyczące kierowania i nadzorowania Przedszkola w odniesieniu do ryzyka. W ramach zarządzania ryzykiem analizuje się, co może się zdarzyć i jakie mogą być możliwe następstwa, a następnie podejmuje decyzję, co i kiedy należy wykonać, aby zredukować ryzyko do akceptowalnego poziomu.
4. Prawdopodobieństwo ryzyka jest to oczekiwana częstotliwość wystąpienia zdarzenia zdefiniowanego jako ryzyko.
5. Strata, którą może spowodować ryzyko jest to wpływ zdarzenia zidentyfikowanego jako ryzyko na integralność, dostępność lub poufność informacji lub na osoby fizyczne w przypadku naruszenia ich praw i wolności.
6. Ocena ryzyka polega na określeniu prawdopodobieństwa wystąpienia ryzyka i starty, którą może spowodować ryzyko.

§ 28.

1. Oceny utraty integralności, dostępności lub poufności informacji dokonuje się poprzez przyznanie prawdopodobieństwu ryzyka i stracie, którą może spowodować ryzyko odpowiedniej liczby punktów.
2. Punktacja dla prawdopodobieństwa ryzyka utraty integralności, dostępności lub poufności informacji:
   1) prawie pewne – 3 pkt,
   2) możliwe – 2 pkt,
   3) rzadkie – 1 pkt.
3. Punktacja dla straty, którą może spowodować ryzyko utraty integralności, dostępności lub poufności informacji:
   1) utrata integralności, dostępności lub poufności informacji może skutkować co najmniej odpowiedzialnością karną lub wydatkami w kwocie 100.000,00 zł i więcej lub doniesieniami medialnymi w całym kraju – 3 pkt,
   2) utrata integralności, dostępności lub poufności informacji może skutkować co najmniej naruszeniem przepisów prawa lub wydatkami w kwocie od 10.000,00 zł do 100.000,00 zł lub informacjami w mediach ogólnokrajowych – 2 pkt,
   3) utrata integralności, dostępności lub poufności informacji może skutkować co najmniej odpowiedzialnością służbową lub wydatkami w kwocie do 10.000,00 zł lub informacjami w mediach regionalnych – 1 pkt.
4. Oceny ryzyka utraty integralności, dostępności lub poufności informacji dokonuje się odrębnie dla każdej grupy informacji i odrębnie dla utraty integralności, dostępności lub poufności informacji.

§ 29.

1. Oceny ryzyka naruszenia praw i wolności osoby, której dane dotyczą, dokonuje się poprzez przyznanie prawdopodobieństwu ryzyka i stracie, którą może spowodować ryzyko, odpowiedniej liczby punktów.
2. Punktacja dla prawdopodobieństwa ryzyka naruszenia praw i wolności osoby, której dane dotyczą:
   1) prawie pewne – 3 pkt,
   2) możliwe – 2 pkt,

3) rzadkie – 1 pkt.

3. Punktacja dla straty, którą może spowodować ryzyko naruszenia praw i wolności osoby, której dane dotyczą:
   1) naruszenie z bardzo dużym prawdopodobieństwem może skutkować dyskryminacją, kradzieżą tożsamości lub oszustwem dotyczącym tożsamości, stratą finansową, naruszeniem dobrego imienia, naruszeniem poufności danych osobowych chronionych tajemnicą zawodową, nieuprawnionym odwróceniem pseudonimizacji lub wszelką inną znaczną szkodą gospodarczą lub społeczną – 3 pkt,
   2) naruszenie w zależności od kontekstu danego zdarzenia w niektórych przypadkach może skutkować dyskryminacją, kradzieżą tożsamości lub oszustwem dotyczącym tożsamości, stratą finansową, naruszeniem dobrego imienia, naruszeniem poufności danych osobowych chronionych tajemnicą zawodową, nieuprawnionym odwróceniem pseudonimizacji lub wszelką inną znaczną szkodą gospodarczą lub społeczną – 2 pkt,
   3) naruszenie nie będzie wpływało na prawa i wolności osób fizycznych – 1 pkt.
4. Oceny ryzyka naruszenia praw i wolności osoby, której dane dotyczą dokonuje się odrębnie dla utraty integralności, dostępności lub poufności danych osobowych.

§ 30.

Oceny ryzyka występujące w Przedszkolu:

a) ryzyko wysokie – suma przyznanych punktów od 5 do 6. Duża istotność. Konsekwencje poważne. Niezbędne są działania naprawcze,
b) ryzyko średnie – suma przyznanych punktów od 3 do 4. Średnia istotność. Przeciwdziałanie wskazane,
c) ryzyko niskie – suma przyznanych punktów od 1 do 2. Mała istotność. Przeciwdziałanie zależy od decyzji właściciela ryzyka.

§ 31.

1. W przypadku ryzyka wysokiego konieczne jest postępowanie z ryzykiem.
2. Metody postępowania z ryzykiem występujące w Przedszkolu:
   a) unikanie – eliminacja zagrożeń,
   b) przeniesienie – przeniesienie ryzyka na inny podmiot, np. poprzez ubezpieczenie,

c) łagodzenie – podjęcie działań mających na celu zmniejszenie negatywnych skutków wystąpienia zagrożenia,

d) akceptacja – zaakceptowanie istniejącego ryzyka i wstrzymanie reakcji do chwili zaistnienia zagrożenia.

3. Postępowanie z ryzykiem powinno być proporcjonalne do ryzyka tak, aby, w większości przypadków, ryzyko mieć pod kontrolą, a nie je eliminować.
4. Postępując z ryzykiem należy brać pod uwagę w szczególności:
   1) ograniczenia czasowe (zabezpieczenie powinno zostać wdrożone w czasie „życia" informacji lub systemu),
   2) ograniczenia finansowe (zabezpieczenia nie powinny być bardziej kosztowne do wdrożenia lub utrzymania niż strata, którą może przynieść ryzyko, za wyjątkiem sytuacji, gdy osiągnięcie zgodności jest wymagane przepisami prawa),
   3) ograniczenia techniczne,
   4) ograniczenia kulturowe (jeśli pracownicy nie rozumieją zabezpieczenia lub nie akceptują go, to zabezpieczenie staje się z czasem nieskuteczne),
   5) ograniczenia prawne,
   6) łatwość użycia,
   7) ograniczenia przy integrowaniu nowych i istniejących zabezpieczeń.

§ 32.

1. Oceny ryzyka dokonują wyznaczeni przez dyrektora pracownicy.
2. Ocenę ryzyka należy udokumentować.

§ 33.

W przypadku, gdy w związku z udzieleniem zamówienia publicznego lub współpracy dochodzi do przetwarzania informacji, wszelkie wymagania bezpieczeństwa informacji powinny zostać określone w umowie.

§ 34.

Nie rzadziej niż raz w roku powinno się przeprowadzić audyt w zakresie bezpieczeństwa informacji.

§ 35.

Nie rzadziej niż raz w roku dyrektor dokonuje przeglądu „Systemu zarządzania bezpieczeństwem informacji" pod kątem zgodności z przepisami prawa. Przegląd nie musi zostać udokumentowany.

§ 36.

„System zarządzania bezpieczeństwem informacji" jest objęty bezwzględną tajemnicą.

Załącznik do „Systemu zarządzania bezpieczeństwem informacji" – wzór upoważnienia do przetwarzania danych osobowych i wzór odwołania upoważnienia do przetwarzania danych osobowych

Rybnik, ... roku

UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH

Na podstawie § 6 „Systemu zarządzania bezpieczeństwem informacji" upoważniam z/od* ..... *(data)* Panią/Pana* ..... *(imię i nazwisko)* do przetwarzania danych osobowych .....
(cel przetwarzania, np. w ramach wykonywania czynności służbowych itp.).

Administrator

.....
(pieczątka i podpis)

Ja niżej podpisana/podpisany* zobowiązuję się do przetwarzania danych osobowych wyłącznie w zakresie nadanego mi upoważnienia, a także do zachowania w tajemnicy przetwarzanych danych 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 kasować*

Rybnik, ... roku

ODWOŁANIE UPOWAŻNIENIA DO PRZETWARZANIA DANYCH OSOBOWYCH

Na podstawie § 6 „Systemu zarządzania bezpieczeństwem informacji" odwołuję z/od* ..... *(data)* z godziną .....** *(dokłada godzina w układzie 00:00)* upoważnienie do przetwarzania danych osobowych dla Pani/Pana* ..... *(imię i nazwisko).*

Administrator

.....

(pieczątka i podpis)

** niepotrzebne skreślić lub skasować*

***opcjonalnie; jeśli nie – skreślić lub skasować*