Załącznik do Zarządzenia
nr 15/2022 z dnia 19.12.2022 r.
Dyrektora Przedszkola nr 6 w Elblągu

Instrukcja Zarządzania Systemem Informatycznym

Przedszkole nr 6
w Elblągu

Elbląg, 2022 r.

SPIS TREŚCI

§ 1
Postanowienia ogólne

1. Niniejszy dokument stanowi instrukcję zarządzania systemem informatycznym w Przedszkolu nr 6 przy ul. Browarna 13 82-300 Elbląg, zwaną dalej Instrukcją i jest wypełnieniem obowiązku wynikającego z art. 24 ust. 1 i ust. 2 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 r. 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 lub RODO) oraz Rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych.
2. Instrukcja określa sposób zarządzania systemem informatycznym, wykorzystywanym do przetwarzania danych osobowych i informacji, w celu ich zabezpieczenia przed zagrożeniami, w tym zwłaszcza przed ich udostępnieniem osobom nieupoważnionym, nieautoryzowaną zmianą, utratą, uszkodzeniem lub zniszczeniem.
3. W Instrukcji zostały uregulowane procedury:
   a) nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemach informatycznych oraz wskazanie osób odpowiedzialnych za te czynności;
   b) rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu;
   c) tworzenia kopii zapasowych zbiorów danych oraz określenie programów i narzędzi programowych służących do ich przetwarzania wraz z określeniem sposobu, miejsca i okresu ich przechowywania;
   d) wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych;
   e) metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem;
   f) sposoby zabezpieczenia systemu informatycznego przed działalnością oprogramowania szkodliwego oraz dostępem do nich osób nieupoważnionych.
4. Instrukcja ma zastosowanie do każdego zbioru danych i informacji:
   a) przetwarzanych w systemach informatycznych w Placówce i wszystkich jej komórek organizacyjnych,
   b) zapisanych w formie elektronicznej na zewnętrznych nośnikach.
5. Do stosowania postanowień Instrukcji obowiązani są wszyscy pracownicy i inne osoby, które otrzymują dostęp do systemów informatycznych Administratora Danych.
6. Przed przystąpieniem do pracy przez pracownika lub innej osoby zatrudnionej w jednostce obowiązkowe jest zapoznanie się z regulacjami dotyczącymi przetwarzania danych w jednostce, w szczególności z:
   a) Polityką bezpieczeństwa przetwarzania Danych Osobowych i Informacji;
   b) Instrukcją Zarządzania Systemem Informatycznym;
7. Fakt zapoznania się z regulacjami, o których mowa w pkt 2, potwierdzany jest poprzez podpisanie oświadczenia o zachowaniu poufności informacji uzyskiwanych w związku z przetwarzaniem danych osobowych oraz zapoznaniu się z zasadami przetwarzania danych.
8. Instrukcja wraz z Polityką Bezpieczeństwa Informacji podlega regularnym przeglądom i aktualizacji min. 1 raz w roku kalendarzowym.
9. Zgodnie z § 20 ust. 2 pkt 14 rozporządzenia Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych min. 1 raz w roku Administrator Danych przeprowadza wewnętrzny audyt dot. bezpieczeństwa informacji.

§ 2
Definicje

1. **Administrator Danych**– Przedszkole nr 6 z siedzibą w Elblągu, ul. Browarna 13 reprezentowane przez dyrektora – Dorotę Szepczyńską- decydujący o celach i środkach przetwarzania danych osobowych, odpowiedzialny za nadzór nad przestrzeganiem zasad ochrony danych osobowych w jednostce oraz wykonujący zadania w zakresie zarządzania i bieżącego nadzoru nad systemem informatycznym;
2. **bezpieczeństwo informacji** – stan, w którym informacja jest chroniona przed wieloma różnymi zagrożeniami w taki sposób, niezależnie od tego, jaką formę informacja przybiera lub za pomocą jakich środków jest udostępniana lub przechowywana, zawsze powinna być w odpowiedni sposób chroniona; bezpieczeństwo informacji oznacza w szczególności zachowanie: poufności, integralności, dostępności i rozliczalności;
3. **dane osobowe (dane)** – oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej;
4. **hasło** – ciąg znaków literowych, cyfrowych lub innych, znany jedynie użytkownikowi;
5. **login** – ciąg znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym;
6. **integralność danych** – właściwość zapewniająca, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany;
7. **instrukcja** – niniejsza Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, zwana dalej Instrukcją;
8. **kopia bezpieczeństwa** – kopie plików danych lub plików programowania tworzone na nośnikach wymiennych lub dysku twardym komputera w celu ich odtworzenia w przypadku utraty lub uszkodzenia danych;
9. **odbiorca danych** – każdy, komu udostępniane są dane osobowe, z wyłączeniem:
   a) osoby, której dane dotyczą,
   b) osoby upoważnionej do przetwarzania danych,
   c) organów państwowych lub organów samorządu terytorialnego, którym dane są udostępniane w związku z prowadzonym postępowaniem;
10. **osoba upoważniona do przetwarzania danych osobowych** – osoba, która upoważniona została do przetwarzania danych osobowych przez Administratora Danych na piśmie;
11. **poufność danych** – właściwość zapewniająca, że dane nie są udostępniane nieupoważnionym podmiotom;
12. **proces zarządzania bezpieczeństwem systemów informatycznych** – całość działań organizacyjno-technicznych i prawnych podejmowanych przez jednostkę mających na celu właściwą ochronę informacji oraz minimalizację skutków w przypadku incydentów bezpieczeństwa;
13. **przetwarzanie danych** – operacja lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taka 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;
14. **przetwarzający dane** – podmiot, któremu zostało powierzone przetwarzanie danych osobowych na podstawie umowy, zgodnie z art. 28 RODO;
15. **system informatyczny (system)** – sprzęt komputerowy, oprogramowanie, dane eksploatowane w zespole współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych;

16. **trwałe usunięcie informacji** – sposób postępowania z nośnikiem informacji mający na celu usunięcie zapisanych na nim informacji tak, aby ich odtworzenie w całości lub w części było niemożliwe;
17. **ustawa** – ustawę z 10.05.2018 r. o ochronie danych osobowych;
18. **uwierzytelnianie** – działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu;
19. **użytkownik** – osoba upoważniona do przetwarzania danych osobowych, której nadano login i przyznano hasło;
20. **zagrożenie** – stan faktyczny, który może spowodować naruszenie bezpieczeństwa informacji;

§ 3
Korzystanie z systemu informatycznego oraz metody i środki uwierzytelniające

1. Instrukcję stosuję się do stacji roboczych, komputerów przenośnych, pozostałych urządzeń mobilnych (telefony, tablety), serwerów, sieci informatycznej oraz pozostałych elementów systemu informatycznego.
2. Stacje robocze, komputery przenośne oraz pozostałe urządzenia mobilne działające w systemie informatycznym posiadają możliwość blokowania dostępu do tego systemu lub możliwość zastosowania zabezpieczonego hasłem wygaszacza ekranu, automatycznie uruchamianego po okresie max. 5 minut braku aktywności użytkownika.
3. Oprogramowanie używane w systemie informatycznym jest chronione przed jakąkolwiek niekontrolowaną modyfikacją, nieautoryzowanym usunięciem oraz kopiowaniem.
4. W systemie informatycznym jest używane wyłącznie oprogramowanie licencjonowane przez posiadacza praw autorskich. Oprogramowanie może być używane tylko zgodnie z prawami licencji.
5. Użytkownicy systemu informatycznego przetwarzającego dane osobowe wykorzystują w procesie uwierzytelnienia indywidualne loginy i hasła.
6. Login jest jednoznacznie nadawany użytkownikowi, nie podlega zmianie i nie może być wykorzystywany przez osoby trzecie, w tym innych użytkowników tego systemu.
7. Użytkownik wprowadza hasło do systemu w sposób uniemożliwiający zapoznanie się z nim przez osoby trzecie. W przypadku podejrzenia zapoznania się z hasłem przez osobę nieuprawnioną użytkownik jest zobowiązany do natychmiastowej zmiany hasła oraz niezwłocznego powiadomienia o tym Administratora Danych.
8. Niedozwolone jest ujawnianie hasła osobom trzecim. Użytkownik ponosi pełną odpowiedzialność za utworzenia hasła i jego przechowywanie.
9. Hasła dostępu do systemu informatycznego muszą posiadać minimum 8 znaków, a także zawierać małe i duże litery, cyfry i znak specjalny.
10. Hasło jest zmieniane przez użytkownika nie rzadziej niż co 30 dni.
11. Za zmianę hasła zgodnie z zasadami niniejszej instrukcji odpowiada użytkownik.
12. Użytkownik jest zobowiązany do niekorzystania z opcji przechowywania hasła w pamięci przeglądarki internetowej, a także niezapisywania hasła w miejscach dostępnych dla osób trzecich.

§ 4
Zasady pracy przy komputerze

1. Przed rozpoczęciem pracy użytkownik obowiązany jest sprawdzić stan urządzeń oraz dokonać oględzin swojego stanowiska pracy w celu wykrycia ewentualnych nieprawidłowości mogących świadczyć o naruszeniu bezpieczeństwa danych osobowych.
2. W pomieszczeniu, w którym przetwarzane są dane osobowe, osoby postronne mogą znajdować się tylko za zgodą Administratora Danych i w towarzystwie pracownika jednostki.
3. Przed osobami postronnymi należy chronić ekrany komputerów (ustawienie monitora powinno uniemożliwiać podgląd), a także wydruki leżące na biurkach oraz w otwartych szafach.
4. Krótkotrwała przerwa w pracy, podczas której użytkownik nie opuszcza stanowiska roboczego, nie wymaga zamykania aplikacji, wylogowania.

5. Każdorazowa zmiana użytkownika stacji roboczej musi poprzedzać wylogowanie się użytkownika, który poprzednio z niej korzystał.

§ 5
Zasady korzystania z urządzeń mobilnych

1. Przetwarzanie danych poza obszarem przetwarzania na urządzeniu mobilnym wymaga zgody Administratora Danych.
2. O ile to możliwe, przy przetwarzaniu danych osobowych na komputerach przenośnych obowiązują procedury określone w niniejszej Instrukcji, dotyczące pracy na komputerach stacjonarnych, w tym: zabezpieczenia dostępu hasłem, zastosowanie oprogramowania i zabezpieczeń analogicznie do rozwiązań przyjętych na stacjonarnych stacjach roboczych.
3. Obowiązuje zakaz używania komputerów przenośnych przez osoby inne niż użytkownicy, którym zostały one powierzone.
4. Korzystanie z urządzeń mobilnych w trakcie pracy zdalnej, powinno odbywać się zgodnie z zasadami Pracy Zdalnej ujętymi w Polityce Bezpieczeństwa Przetwarzania Danych Osobowych i Informacji.
5. Osoba wykorzystująca komputer przenośny, stanowiący własność Administratora Danych, obowiązana jest do:
   a) wykorzystywania go wyłącznie do określonych celów, mieszczących się w zakresie upoważnienia;
   b) nieudostępniania komputera nieupoważnionym osobom;
   c) zachowania szczególnej ochrony przed kradzieżą, zwłaszcza podczas transportu;
   d) zaniechania jakichkolwiek zmian oprogramowania.
6. W przypadku konieczności zmiany, aktualizacji albo naprawy komputera należy zgłosić ten fakt do Administratora Danych.

§ 6
Procedura tworzenia kopii zapasowych oraz sposób i czas przechowywania nośników informacji.

1. Administrator Danych odpowiada za okresowe wykonanie kopii bezpieczeństwa danych gromadzonych w Systemie Informatycznym, przy pomocy przewidzianych przez System Informatyczny narzędzi.
2. Tworzenie kopii zapasowych może wchodzić również w zakres odpowiedzialności usługodawców.
3. Za zewnętrzne nośniki danych uważa się:
   a) dyski CD-R, CD-RW, DVD-R, DVD-RW itp.
   b) twarde dyski wymienne,
   c) pendrive
   d) komputery przenośne,
   e) inne nośniki, służące do przechowywania danych i informacji i mogące być przenoszone niezależnie od sprzętu komputerowego.
4. Nieupoważnieni pracownicy nie mogą wykonywać kopii baz (zbiorów) danych oraz zapisywać - na informatycznych nośnikach danych - danych osobowych, w szczególności dokonywać kopii zapasowej całych zbiorów danych.
5. Wymienne elektroniczne nośniki informacji są przechowywane w pomieszczeniach stanowiących obszar przetwarzania danych osobowych.
6. Po zakończeniu pracy przez użytkowników Systemu Informatycznego wymienne elektroniczne nośniki informacji zawierające dane osobowe są przechowywane w zamykanych szafach biurowych lub kasetkach.
7. Urządzenia, dyski lub inne informatyczne nośniki zawierające dane osobowe, przeznaczone do likwidacji, są pozbawiane przez Administratora Danych zapisu tych danych, a w przypadku, gdy nie jest to możliwe, są uszkadzane w sposób uniemożliwiający ich odczytanie.

8. Dopuszczalne jest zlecenie/powierzenie niszczenia wszelkich nośników danych osobowych wyspecjalizowanym podmiotom zewnętrznym. Podstawą przekazania danych do zniszczenia innemu podmiotowi powinna być w każdym przypadku umowa zawarta na piśmie.
9. Dostęp do wydruków z Systemu Informatycznego zawierających dane osobowe mają wyłącznie osoby do tego upoważnione.
10. Wydruki są przechowywane w miejscu uniemożliwiającym bezpośredni do nich dostęp osobom niepowołanym.

§ 7
Procedura i sposób zabezpieczenia przed oprogramowaniem, którego celem jest nieuprawniony dostęp do zasobów systemu informatycznego oraz postępowanie w przypadku awarii zasilania

1. Na wszystkich komputerach (w tym także komputerach przenośnych) oraz serwerach zostało zainstalowane oprogramowanie antywirusowe oraz oprogramowanie zapobiegające nieuprawnionemu dostępowi do Systemu Informatycznego.
2. W przypadku stwierdzenia wystąpienia nieprawidłowości funkcjonowania systemu Administrator Danych, osoba odpowiedzialna za obsługę informatyczną lub inny upoważniony pracownik zobowiązany jest do podjęcia działań zmierzających do wykrycia źródła pojawienia się problemów w Systemie Informatycznym, jego wyeliminowania, a jeśli jest to niemożliwe – do usunięcia.
3. Sprzęt komputerowy służący do przetwarzania danych osobowych jest wyposażony w urządzenia podtrzymujące zasilanie.
4. W przypadku wystąpienia przerw w dostawie energii elektrycznej Administrator Danych, osoba odpowiedzialna za obsługę informatyczną lub inny upoważniony pracownik zobowiązany jest do:
    a) zakończenia trwających procesów;
    b) zakończenia pracy sprzętu (np. komputera).
    c) kontroli poprawności jego funkcjonowania i działania Systemu Informatycznego.

§ 8
Procedura usuwania awarii sprzętu lub oprogramowania

1. W przypadku wystąpienia awarii Systemu Informatycznego pracownik lub współpracownik, który ją stwierdził zobowiązany jest do zgłoszenia faktu wystąpienia awarii Administratorowi Danych lub osobie odpowiedzialnej za obsługę informatyczną.
2. Administrator Danych lub osoba odpowiedzialna za obsługę informatyczną zobowiązany jest do niezwłocznego podjęcia czynności zmierzających do usunięcia awarii np. poprzez wezwanie serwisu.
3. Po usunięciu awarii Administrator Danych, osoba odpowiedzialna za obsługę informatyczną lub inny upoważniony pracownik zobowiązany jest do:
    a) uruchomienia Systemu Informatycznego;
    b) kontroli poprawności jego funkcjonowania;
    c) kontroli integralności danych.
4. W przypadku stwierdzenia uszkodzenia danych zgromadzonych w Systemie, Administrator Danych, osoba odpowiedzialna za obsługę informatyczną lub inny upoważniony pracownik zobowiązany jest do otworzenia danych z ostatniej posiadanej kopii bezpieczeństwa (backup).
5. W przypadku gdy usunięcie awarii wymaga przekazania sprzętu komputerowego na zewnątrz, przed przekazaniem tego sprzętu Administrator Danych, osoba odpowiedzialna za obsługę informatyczną lub inny upoważniony pracownik zobowiązany jest do usunięcia z dysków twardych wszystkich danych, po ich uprzednim skopiowaniu na inny nośnik. Jeśli z przyczyn technicznych jest to niemożliwe, osoba przekazująca sprzęt ze strony Placówki zobowiązana jest uzyskać od serwisanta protokół przyjęcia danych i zobowiązanie do zachowania ich poufności – wzór oświadczenia o zachowaniu poufności stanowi załącznik nr 1.

§ 9
Procedury wykonywania przeglądów i konserwacji systemu informatycznego oraz informatycznych nośników danych

1. Przegląd i konserwacja Systemu Informatycznego oraz informatycznych nośników danych zawierających dane osobowe dokonywane są poprzez:
   a) sprawdzanie zgodności danych z dokumentami;
   b) analizę zgłaszanych uwag użytkowników.
2. Przeglądu i konserwacji Systemu Informatycznego dokonuje Administrator Danych, osoba odpowiedzialna za obsługę informatyczną lub inny upoważniony pracownik. Dopuszczalne jest zlecenie/powierzenie przeglądów i konserwacji zbiorów danych wyspecjalizowanym podmiotom zewnętrznym na podstawie pisemnych umów.
3. Przekazywane na zewnątrz Informatyczne nośniki danych (komputery, dyski, laptopy), dla celów naprawy czy konserwacji, nie zawierają baz (zbiorów) danych osobowych.

§10
Utylizacja sprzętu informatycznego i nośników danych

1. Celem procedury jest określenie zasad niszczenia wszelkich nośników informatycznych zawierających dane osobowe lub licencjonowane oprogramowanie.
2. Pod pojęciem nośnik informatyczny rozumiemy:
   a) dyski twarde komputerowe i serwerowe wszelkich typów,
   b) płyty CD-R, CD-RW, DVD-R, DVD-RW lub podobne,
   c) pamięci flash (pendrive), karty procesorowe,
   d) dyski przenośne HDD, SSD itp.,
   e) taśmy magnetyczne.
3. Procedura niszczenia dotyczy tych nośników informacji, które zawierają dane przetwarzane na potrzeby jednostki.
4. Poprzez niszczenie nośników rozumieć należy takie ich uszkodzenie mechaniczne, które uniemożliwia jakiekolwiek odzyskanie zapisanych na nich uprzednio informacji.
5. Niszczeniu poddaje się nośnik informatyczny, w przypadku stwierdzenia:
   a) wady lub uszkodzenia wynikającego z eksploatacji, którego naprawa byłaby nieopłacalna,
   b) nie przewiduje się ich dalszego użytkowania,
   c) istnieje prawdopodobieństwo, że dalsze ich użytkowanie może nie spełniać wymogów bezpieczeństwa przechowywania informacji.
6. Niszczenia nośników informatycznych dokonuje komisyjnie przynajmniej dwóch pracowników powołanych przez Administratora Danych.
7. Niszczenia nośników dokonuje się w następujący sposób:
   a) dyski twarde z komputerów i serwerów podlegają zniszczeniu mechanicznemu (zalecane jest niszczenie dysków za pomocą specjalistycznego sprzętu i poddanie ich demagnetyzacji i rozdrobnieniu),
   b) płyty CD-R, CD-RW, DVD, DVD-RW przełamuje się na kilka części lub niszczy w niszczarce przeznaczonej do utylizacji płyt CD,
   c) taśmy magnetyczne wyciąga się z obudowy i przecina na wiele części,
   d) pamięci flash jak i dyski przenośne uszkadza się w podobny sposób jak dyski twarde poprzez zniszczenie mechaniczne.
8. Po zakończeniu niszczenia, sporządzany jest protokół likwidacyjny nośników (załącznik nr 2). Protokół musi zawierać wyszczególnienie zniszczonych nośników wraz z ich opisem, datą likwidacji, nazwiska osób, które tego dokonały. Pod protokołem podpisują się: pracownicy biorący udział w likwidacji nośników oraz Dyrektor jednostki.

§ 11
Ewidencja sprzętu oraz oprogramowania IT

1. Na System informatyczny w Placówce składają się:
    a) Urządzenia, w tym komputery stacjonarne, Komputery przenośne, kserokopiarki
    b) Programy, służące do przetwarzania danych osobowych i informacji – zgodnie z wykazem, o którym mowa w pkt. 3.
2. Elementy Systemu opisane w ust. 1 są wykorzystywane do przetwarzania danych w jednostce. Podlegają one regularnej kontroli w celu zapewnienia bezpieczeństwa przetwarzanych danych.
3. Administrator Danych prowadzi wykaz sprzętu i oprogramowania, służącego do przetwarzania informacji i danych osobowych – według załącznika nr 3.

§ 12
Polityka czystego ekranu

1. Osoba korzystająca z systemu informatycznego jest zobowiązana do zachowania polityki czystego ekranu, tj. zapewnienia, by osoby nieupoważnione nie miały wglądu w treści wyświetlane na monitorach ekranowych lub ekranach komputerów przenośnych.
2. Osoba korzystająca z systemu informatycznego jest zobowiązana do manualnego uruchamia wygaszacza ekranu chronionego hasłem w każdej sytuacji, gdy pozostawia system informatyczny bez nadzoru (nawet na chwilę).
3. Zabronione jest gromadzenie danych osobowych w postaci tzw. zrzutów ekranów z systemu informatycznego, jak i wysyłanie takich informacji poza organizację bez zgody administratora tego systemu.
4. Osoby korzystające z systemu informatycznego powinny zwracać szczególną uwagę na:
    a) ustawienie monitorów lub ekranów komputerów przenośnych w obszarze przetwarzania względem okien (w przypadku blisko siebie sąsiadujących budynków) oraz drzwi wejściowych, przez które mogą wejść osoby nieupoważnione,
    b) uruchamianie komputerów przenośnych poza obszarem przetwarzania w miejscach publicznie dostępnych (np. lotniska, dworce, sale konferencyjne itp.),
    c) osoby nieupoważnione pozostające w obszarze przetwarzania danych bez nadzoru osób upoważnionych.

§ 13
Postępowanie dyscyplinarne

1. Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszego Regulaminu mogą zostać potraktowane jako ciężkie naruszenie obowiązków pracowniczych lub zobowiązań umownych. Wobec osoby, która w przypadku naruszenia zabezpieczeń systemu informatycznego lub uzasadnionego podejrzenia takiego naruszenia nie podjęła działania określonego w niniejszej Instrukcji, a w szczególności nie powiadomiła odpowiedniej osoby zgodnie z określonymi zasadami, można wszcząć postępowanie dyscyplinarne.
2. Kara dyscyplinarna zastosowana wobec osoby uchylającej się od powiadomienia nie wyklucza odpowiedzialności karnej tej osoby zgodnie z obowiązującymi przepisami prawa oraz możliwości wniesienia wobec niej sprawy z powództwa cywilnego przez Administratora Danych o zrekompensowanie poniesionych strat.

Spis załączników:

Załącznik nr 1 wzór oświadczenia o zachowaniu poufności;
Załącznik nr 2 wzór protokołu zniszczenia nośników informatycznych;
Załącznik nr 3 wzór Ewidencji sprzętu i oprogramowania wchodzącego w skład Systemu Informatycznego.

Załącznik nr 1

Elbląg, dnia……

…….
Pieczęć jednostki

WZÓR

OŚWIADCZENIE O ZACHOWANIU POUFNOŚCI
dot. współpracy w zakresie świadczenia usług informatycznych

w związku z wykonaniem usług informatycznych, dnia……

1. Wykonawca zobowiązany jest zapewnić poufności informacji, które uzyskał od Zamawiającego w związku z realizacją niniejszej umowy i nie ujawniać tych informacji bez uprzedniej pisemnej zgody Zamawiającego, w tym niekopiowania, niepowielania ani w jakikolwiek inny sposób nierozpowszechniania jakiejkolwiek części określonych informacji, w których mowa w pkt. 2.
2. Obowiązek zachowania tajemnicy danych Zleceniodawcy, dotyczy w szczególności informacji prawnie chronionych, które to informacje Wykonawca uzyska w trakcie lub w związku z realizacja niniejszej umowy, bez względu na sposób i formę ich utrwalenia lub przekazania.
3. Wykonawca zobowiązany jest do zachowania w tajemnicy wszelkich informacji niepodlegających udostępnienie publicznemu, w tym informacji technicznych i organizacyjnych Przedszkol nr 6 przy ul. Browarna 13 82-300 Elbląg jak również dotyczących systemów i sieci informatycznych, danych osobowych, uzyskanych w trakcie wykonywania niniejszej Umowy oraz podjęcia wszelkich niezbędnych kroków dla zapewnienia, że żadna osoba trzecia nie otrzyma dostępu do tych informacji.
4. Zamawiający zastrzega sobie prawo, że Umowa będzie wykonywana przez Zleceniobiorcę osobiście, bez udziału osób trzecich.

Zleceniobiorca:
Nazwa Firmy/NIP/Pieczęć:……..
Reprezentowana przez:……
Data, podpis:.……

Załącznik nr 2

Elbląg, dnia.....

Protokół
zniszczenia nośników komputerowych

Dnia ..... komisja powołana przez……

w składzie:

a) Przewodniczący: .....
b) Członkowie: .....
.....

dokonała trwałego zniszczenia nośników komputerowych:

L.p.	Nazwa	Sposób zniszczenia	Uwagi

Dokonanie w/w czynności zostaje potwierdzone własnoręcznymi podpisami komisji:

.....

.....

Załącznik nr 3

WZÓR

Ewidencja sprzętu i oprogramowania wchodzącego w skład Systemu Informatycznego

Przedszkola nr 6 przy ul. Browarna 13 82-300 Elbląg

L.P.	AKTYWA	Oprogramowanie	LOKALIZACJA	NR INWENTARZOWY	UŻYTKOWNIK
1.	Komputer stacjonarny	system operacyjny **Windows 10 Pro**, wersja oprogramowania antywirusowego **ESET Internet Security, wersja 13.0.22.0**	Gabinet dyrektora		Dyrektor
2.	Komputer stacjonarny	system operacyjny **Windows 7 Home Premium**, wersja oprogramowania antywirusowego **ESET Internet Security, wersja 13.0.22.0**	Gabinet wicedyrektora i intendenta		Wicedyrektor
3.	Komputer stacjonarny	system operacyjny **Windows 7 Professional**, wersja oprogramowania antywirusowego **ESET Internet Security, wersja 13.0.22.0**	Gabinet wicedyrektora i intendenta		Intendent
4.	Komputer stacjonarny	System operacyjny **Windows XP Professional**, wersja oprogramowania antywirusowego **COMODO ANTIVIRUS**	Gabinet kierownika gospodarczego		Kierownik Gospodarczy
5.	Drukarka		Gabinet dyrektora		Dyrektor
6.	Drukarka		Gabinet wicedyrektora i intendenta		Wicedyrektor
7.	Drukarka		Gabinet wicedyrektora i intendenta		Intendent
8.	Drukarka		Gabinet kierownika gospodarczego		Kierownik Gospodarczy
9.	Ksero		Korytarz II piętro		cała placówka
10.	Router wi-fi	Wifi TP LINK DA 18B6	II piętro		cała placówka