WYCIĄG

BEZWZGLĘDNE ZASADY

OCHRONY DANYCH OSOBOWYCH

Z

POLITYKI BEZPIECZEŃSTWA INFORMACJI

zgodne z RODO

PARAFIA RZYMSKOKATOLICKA
pw. Św. Katarzyny Aleksandryjskiej w Grybowie
NIEPUBLICZNE PRZEDSZKOLE PARAFIALNE
Z ODDZIAŁEM INTEGRACYJNYM
im. Świętych Dzieci Fatimskich
ul. Dębowa 11, 33-330 Grybów - tel. 18 445 02 62 (w. 36)
NIP 7381035185 REGON 381037210

Niepubliczne Przedszkole Parafialne z Oddziałem integracyjnym im. Świętych Dzieci Fatimskich w Grybowie

I. ZASADY ZARZĄDZANIA UPRAWNIENIAMI PODCZAS PRACY

1. Każdy użytkownik przetwarzający dane osobowe musi posiadać swój własny indywidualny identyfikator (login) do logowania się.
2. Tworzenie kont użytkowników wraz z uprawnieniami wykonuje informatyk na polecenie Administratora danych.
3. Użytkownik nie może samodzielnie zmieniać swoich uprawnień.
4. Użytkownikowi zabrania się umożliwianie innym osobom pracy na swoim koncie posiadającym indywidualny identyfikator użytkownika.
5. Zabrania się pracy wielu użytkowników na wspólnym koncie.
6. Użytkownik rozpoczyna pracę z użyciem identyfikatora i hasła.
7. Użytkownik jest zobowiązany do powiadomienia Administratora o próbach logowania się do systemu osoby nieupoważnionej, jeśli system to sygnalizuje.
8. W przypadku, gdy użytkownik podczas próby zalogowania się zablokuje system, zobowiązany jest powiadomić o tym informatyka.
9. Użytkownik jest zobowiązany do uniemożliwienia osobom niepowołanym (np. pracownikom innych działów) wglądu do danych wyświetlanych na monitorach - tzw. Polityka czystego ekranu.
10. Przed czasowym opuszczeniem stanowiska pracy, użytkownik zobowiązany jest wywołać blokowany hasłem wygaszacz ekranu lub wylogować się z systemu (WINDOWS + L). Jeżeli tego nie uczyni, po upływie **5** minut system automatycznie aktywuje wygaszacz.
11. Zabrania się uruchamiania jakiejkolwiek aplikacji lub programu na prośbę innej osoby, o ile nie została dopuszczona do użytkowania. Dotyczy to zwłaszcza programów przesłanych za pomocą poczty elektronicznej lub wskazanych w formie odnośnika internetowego.
12. Po zakończeniu pracy, użytkownik zobowiązany jest:
    a) wylogować się z systemu informatycznego, a następnie wyłączyć sprzęt komputerowy
    b) zabezpieczyć stanowisko pracy, w szczególności wszelką dokumentację oraz nośniki magnetyczne i optyczne, na których znajdują się dane osobowe.

DYREKTOR PRZEDSZKOLA
Marta Wojtarowicz
.....
mgr Marta Wojtarowicz

(Podpis ADO)

II. ZASADY BEZPIECZNEGO UŻYTKOWANIA SPRZĘTU IT, DYSKÓW, PROGRAMÓW

1. Użytkownik przetwarzający dane osobowe korzystający ze sprzętu IT zobowiązany jest do jego zabezpieczenia przed zniszczeniem lub uszkodzeniem.
   Za sprzęt IT rozumie się: komputery stacjonarne, monitory, drukarki, skanery, ksera, laptopy, służbowe tablety i smartfony.

2. Użytkownik jest zobowiązany zgłosić zagubienie, utratę lub zniszczenie powierzonego mu Sprzętu IT.

3. Samowolne instalowanie, otwieranie (demontaż) Sprzętu IT, instalowanie dodatkowych urządzeń (np. twardych dysków, pamięci) do lub podłączanie jakichkolwiek niezatwierdzonych urządzeń do systemu informatycznego jest zabronione.

4. Użytkownik jest zobowiązany do uniemożliwienia osobom niepowołanym (np.pracownikom innych działów) wgląd do danych wyświetlanych na monitorach komputerowych - tzw. zasada czystego ekranu.

5. Przed czasowym opuszczeniem stanowiska pracy, użytkownik zobowiązany jest wywołać blokowany hasłem wygaszacz ekranu (WINDOWS + L) lub wylogować się z systemu bądź z programu.

6. Po zakończeniu pracy, użytkownik zobowiązany jest:
   a. wylogować się z systemu informatycznego, a jeśli to wymagane - następnie wyłączyć sprzęt komputerowy
   b. zabezpieczyć stanowisko pracy, w szczególności wszelkie nośniki magnetyczne i optyczne na których znajdują się dane osobowe
   c. dokumentację papierową należy zamknąć w szafie lub zamykanym na klucz biurku **- tzn. polityka czystego biurka.**

7. Jeśli użytkownik jest uprawniony do niszczenia nośników, powinien trwale zniszczyć sam nośnik lub trwale usunąć z niego dane (np. zniszczenie płyt DVD w niszczarce, zniszczenie twardego dysku, pendrive młotkiem).

8. Użytkownicy komputerów przenośnych na których znajdują się dane osobowe lub z dostępem do danych osobowych przez internetzobowiązani są do stosowania zasad bezpieczeństwa zawartych w Regulaminie użytkowania komputerów przenośnych.

DYREKTOR PRZEDSZKOLA
Marta Wojtarowicz
mgr Marta Wojtarowicz

.....

(Podpis ADO)

III. ZASADY ZARZĄDZANIA HASŁAMI

1. Hasła powinny składać się z min. 8 znaków.
2. Hasła powinny zawierać duże litery + małe litery + cyfry (lub znaki specjalne).
3. Hasła nie mogą być łatwe do odgadnięcia. Nie powinny być powszechnie używanymi słowami. W szczególności nie należy jako haseł wykorzystywać: dat, imion i nazwisk osób bliskich, imion zwierząt, popularnych dat, popularnych słów, typowych zestawów: 123456.
4. Hasła nie powinny być ujawnianie innym osobom. Nie należy zapisywać haseł na kartkach i w notesach, nie naklejać na monitorze komputera, nie trzymać pod klawiaturą lub w szufladzie.
5. W przypadku ujawnienia hasła - należy natychmiast go zmienić.
6. Hasła muszą być zmieniane co **30** dni.
7. Jeżeli system nie wymusza zmiany haseł, użytkownik zobowiązany jest do samodzielnej zmiany hasła.
8. Użytkownik systemu w trakcie pracy w aplikacji może zmienić swoje hasło.
9. Użytkownik zobowiązuje się do zachowania hasła w poufności, nawet po utracie przez nie ważności.
10. Zabrania się używania w serwisach internetowych takich samych lub podobnych haseł jak w systemie komputerowym firmy.
11. Zabrania się stosowania tego samego hasła jako zabezpieczenia w dostępie do różnych systemów.
12. Zabrania się definiowania haseł, w których jeden człon pozostaje niezmienny, a drugi zmienia się według przewidywalnego wzorca (np. Anna001, Anna002, Anna003 itd.). Nie powinno się też stosować haseł, w których któryś z członów stanowi imię, nazwę lub numer miesiąca lub inny możliwy do odgadnięcia klucz.

DYREKTOR PRZEDSZKOLA
mgr Marta Wojtarowicz

.....

(Podpis ADO)

IV. ZASADY PRZETWARZANIA DANYCH – WYNOSZENIA NOŚNIKÓW Z DANYMI POZA OBSZAR JEDNOSTKI

1. Użytkownikom zabrania się wynoszenia na zewnątrz organizacji wymiennych elektronicznych nośników informacji z zapisanymi danymi osobowymi bez zgody Pracodawcy / Zleceniodawcy. Do takich nośników zalicza się: wymienne twarde dyski, pendrive, płyty CD, DVD, pamięci typu Flash.

2. Dane osobowe wynoszone poza organizację muszą być zaszyfrowane (szyfrowane dyski, zahasłowane pliki).

3. W przypadku, gdy dokumenty przewozi pracownik (w plecakach, teczkach), zobowiązany jest do zabezpieczenia przewożonych dokumentów przed zagubieniem i kradzieżą.

4. Pracownicy, przetwarzający dane poza obszarem wyznaczonym są zobowiązani:

1) Pilnować i nie dopuścić do sytuacji, w której akta lub dokumenty pozostawione są bez dozoru w czasie ich przenoszenia oraz przetwarzania poza obszarem wyznaczonym przez Administratora Danych Osobowych.
2) dołożyć wszelkich starań, aby osoby postronne, nie mogły mieć dostępu do dokumentów,
3) przechowywać dokumenty w sposób zabezpieczający je przed przypadkowym uzyskaniem do nich wglądu przez osoby nieupoważnione;
4) po zakończeniu wykonywania pracy w terenie niezwłocznie zwrócić dokumenty do Jednostki, a jeśli nie jest to możliwe przechować je w domu. Przechowywanie dokumentów w domu następuje poprzez ich zamknięcie w sposób uniemożliwiający dostęp osób innych niż upoważniony pracownik.

5. Pracownicy wynoszący dokumenty do domu są zobowiązani do ochrony danych w nich zawartych i w razie ich udostępnienia lub umożliwienia dostępu do nich osobom nieupoważnionym podlegają karze.

DYREKTOR PRZEDSZKOLA
mgr Marta Wojtaszonic
mgr Marta Wojtarowicz

.....

(Podpis ADO)

V. ZASADY KORZYSTANIA Z INTERNETU

1. Użytkownik zobowiązany jest do korzystania z Internetu wyłącznie w celach służbowych.

2. Zabrania się zgrywania na dysk twardy komputera oraz uruchamia jakichkolwiek programów nielegalnych oraz plików pobranych z niewiadomego źródła. Pliki takie powinny być ściągane tylko za każdorazową zgodą informatyka lub Administratora.

3. Użytkownik ponosi odpowiedzialność za szkody spowodowane przez oprogramowanie instalowane z Internetu.

4. Zabrania się wchodzenia na strony, na których prezentowane są informacje o charakterze przestępczym, hackerskim, pornograficznym, lub innym zakazanym przez prawo (na większości stron tego typu jest zainstalowane szkodliwe oprogramowanie infekujące w sposób automatyczny system operacyjny komputera szkodliwym oprogramowaniem)

5. Nie należy w opcjach przeglądarki internetowej włączać opcji autouzupełniania formularzy i zapamiętywania haseł.

6. W przypadku korzystania z szyfrowanego połączenia przez przeglądarkę, należy zwracać uwagę na pojawienie się odpowiedniej ikonki (kłódka) oraz adresu www rozpoczynającego się frazą "https:". Dla pewności należy „kliknąć" na ikonkę kłódki i sprawdzić, czy właścicielem certyfikatu jest wiarygodny właściciel.

7. Należy zachować szczególną ostrożność w przypadku podejrzanego żądania lub prośby zalogowania się na stronę (np. na stronę banku, portalu społecznościowego, e-sklepu, poczty mailowej) lub podania naszych loginów i haseł, PIN-ów, numerów kart płatniczych przez Internet. Szczególnie tyczy się to żądania podania takich informacji przez rzekomy bank.

8. Zabrania się samowolnego podłączania do komputerów modemów, telefonów komórkowych i innych urządzeń dostępowych (np.: typu BlueConnect, iPlus, OrangeGo). Zabronione jest też łączenie się przy pomocy takich urządzeń z Internetem w chwili, gdy komputer użytkownika podłączony jest do sieci firmowej.

DYREKTOR PRZEDSZKOLA
Marta Wojtarowicz
mgr Marta Wojtarowicz

.....

(Podpis ADO)

VI. ZASADY KORZYSTANIA Z POCZTY ELEKTRONICZNEJ

1. Przesyłanie danych osobowych z użyciem maila poza organizację może odbywać się tylko przez osoby do tego upoważnione.

2. W przypadku przesyłania danych osobowych poza organizację należy wysyłać pliki zaszyfrowane/spakowane (np. programem 7 zip, winzipem, winrarem) i zahasłowane, gdzie hasło powinno być przesłane do odbiorcy innym sposobem: telefonicznie lub SMS.

3. W przypadku zabezpieczenia plików hasłem, obowiązuje minimum 8 znaków: duże i małe litery i cyfry lub znaki specjalne.

4. Użytkownicy powinni zwracać szczególną uwagę na poprawność adresu odbiorcy dokumentu.

5. Zaleca się, aby użytkownik podczas przesyłania danych osobowych mailem zawarł w treści prośbę o potwierdzenie otrzymania i zapoznania się z informacją przez adresata.

6. **WAŻNE:** Nie otwierać załączników (.zip, .xlsm, .pdf, .exe) w mailach!!!!! Są to zwykle „wirusy", które infekują komputer oraz często pozostałe komputery w sieci. **WYSOKIE RYZYKO BEZPOWROTNEJ UTRATY DANYCH**

7. **WAŻNE:** Nie wolno „klikać" na hiperlinki w mailach, gdyż mogą to być hiperlinki do stron z „wirusami".Użytkownik „klikając" na taki hiperlink infekuje komputer oraz inne komputery w sieci.
   WYSOKIE RYZYKO BEZPOWROTNEJ UTRATY DANYCH

8. Należy zgłaszać informatykowi przypadki podejrzanych emaili.

9. Użytkownicy nie powinni rozsyłać „niezawodowych" emaili w formie „łańcuszków szczęścia", np. Życzenia Świąteczne adresowane do np.: 230 osób.

10. Podczas wysyłania maili do wielu adresatów jednocześnie, należy użyć metody „Ukryte do wiadomości - UDW". Zabronione jest rozsyłanie maili do wielu adresatów z użyciem opcji „Do wiadomości"!!!!!

11. Użytkownicy powinni okresowo kasować niepotrzebne maile.

12. Mail służbowy jest przeznaczony wyłącznie do wykonywania obowiązków służbowych.

13. Zakazuje się wysyłania korespondencji służbowej na prywatne skrzynki pocztowe pracowników lub innych osób.

14. Użytkownicy mają prawo korzystać z poczty mailowej dla celów prywatnych wyłącznie okazjonalnie i powinno być to ograniczone do niezbędnego minimum.

15. Zabrania się użytkownikom poczty elektronicznej konfigurowania swoich kont pocztowych do automatycznego przekierowywania wiadomości na adres zewnętrzny.

16. Korzystanie z maila dla celów prywatnych nie może wpływać na jakość i ilość świadczonej przez Użytkownika pracy oraz na prawidłowe i rzetelne wykonywanie przez niego obowiązków służbowych.

17. Przy korzystaniu z maila, Użytkownicy mają obowiązek przestrzegać prawa własności przemysłowej i prawa autorskiego.

18. Użytkownicy nie mają prawa korzystać z maila w celu rozpowszechniania treści o charakterze obraźliwym, niemoralnym lub niestosownym wobec powszechnie obowiązujących zasad postępowania.

DYREKTOR PRZEDSZKOLA
Marta Wojtarowicz
mgr Marta Wojtarowicz
.....

(Podpis ADO)

VII. ZASADY OCHRONY ANTYWIRUSOWEJ

1. Użytkownicy zobowiązania są do skanowania plików wprowadzanych z zewnętrznych nośników programem antywirusowym, jeśli system antywirusowy taką funkcje posiada.

2. Zakazane jest wyłączanie systemu antywirusowego podczas pracy systemu informatycznego przetwarzającego dane osobowe.

3. W przypadku stwierdzenia zainfekowania systemu lub pojawienia się komunikatów „np.; Twój system jest zainfekowany!, zainstaluj program antywirusowy". Użytkownik obowiązany jest poinformować niezwłocznie o tym fakcie Informatyka lub Administratora.

DYREKTOR PRZEDSZKOLA
Marta Wojtarowicz
mgr Marta Wojtarowicz
.....

(Podpis ADO)

VIII. ZASADY ZABEZPIECZANIA DOKUMENTACJI PAPIEROWEJ Z DANYMI OSOBOWYMI

1. Wszyscy pracownicy zobowiązani są do przestrzegania tzw. „Zasady czystego biurka".
2. Zasada ta polega na zabezpieczaniu (zamykaniu) dokumentównp. w szafach, biurkach, pomieszczeniach przed kradzieżą lub wglądem osób nieupoważnionych po godzinach pracy lub podczas ich nieobecności w trakcie godzin pracy.
3. Zasada uniemożliwia również wgląd klientom do innej dokumentacji papierowej na biurku gdyż na biurku leżą tylko dokumenty danego klienta/strony.
4. Każdy pracownik zobowiązany jest do przechowywania na biurku tylko tych dokumentów, które są pracownikowi niezbędne w danym momencie pracy do wykonania bieżących zadań.
5. Na biurku nie mogą znajdować się napoje w pojemnikach grożących rozlaniem płynu.
6. Po zakończonej pracy pracownik zobowiązany jest odłożyć wszystkie dokumenty do zamykanej na klucz szafy.
7. Po zakończonej pracy na biurku mogą znajdować się jedynie telefon i przybory biurowe, takie jak: zszywacz, dziurkacz, długopis, itp.
8. Pracownik zobowiązany jest do niszczenia dokumentów niepotrzebnych i wydruków w taki sposób, aby nie było możliwe odtworzenie zawartych w nich informacji, np. w niszczarkach lub przygotowaniu ich do bezpiecznej utylizacji.
9. Zabrania się pozostawiania dokumentów z danymi osobowymi poza zabezpieczonymi pomieszczeniami, np. w korytarzach, na kserokopiarkach, drukarkach, w pomieszczeniach konferencyjnych.
10. Zabrania się wyrzucania niezniszczonych dokumentów na śmietnik lub porzucania ich na zewnątrz, np., na terenach publicznych, miejskich, w lesie.

DYREKTOR PRZEDSZKOLA
Marta Wojtarowicz
mgr Marta Wojtarowicz

.....

(Podpis ADO)

IX. SKRÓCONE ZASADY POSTĘPOWANIA W PRZYPADKU NARUSZENIA DANYCH OSOBOWYCH

1. Każda osoba upoważniona do przetwarzania danych osobowych zobowiązana jest do powiadomieniaPracodawcy w przypadku stwierdzenia lub podejrzenia naruszenia ochrony danych osobowych.

2. Do sytuacji wymagających powiadomienia, należą:
   a. niewłaściwe zabezpieczenie fizyczne pomieszczeń, urządzeń i dokumentów
   b. niewłaściwe zabezpieczenie sprzętu IT, oprogramowania przed wyciekiem, kradzieżą i utratą danych osobowych
   c. nieprzestrzeganie zasad ochrony danych osobowych przez pracowników (np. niestosowanie zasady czystego biurka / ekranu, ochrony haseł, niezamykanie pomieszczeń, szaf, biurek).

3. Do incydentów wymagających powiadomienia, należą:
   a. zdarzenia losowe zewnętrzne (pożar obiektu/pomieszczenia, zalanie wodą, utrata zasilania, utrata łączności)
   b. zdarzenia losowe wewnętrzne (awarie serwera, komputerów, twardych dysków, oprogramowania, pomyłki informatyków, użytkowników, utrata / zagubienie danych)
   c. umyślne incydenty (włamanie do systemu informatycznego lub pomieszczeń, kradzież danych/sprzętu, wyciek informacji, ujawnienie danych osobom nieupoważnionym, świadome zniszczenie dokumentów/danych, działanie wirusów i innego szkodliwego oprogramowania).

4. Typowe przykłady incydentów wymagające reakcji:
   a. ślady na drzwiach, oknach i szafach wskazują na próbę włamania
   b. dokumentacja jest niszczona bez użycia niszczarki
   c. fizyczna obecność w budynku lub pomieszczeniach osób zachowujących się podejrzanie
   d. otwarte drzwi do pomieszczeń, szaf, gdzie przechowywane są dane osobowe
   e. ustawienie monitorów pozwala na wgląd osób postronnych w dane osobowe
   f. wynoszenie danych osobowych w wersji papierowej i elektronicznej na zewnątrz organizacji bez upoważnienia Pracodawcy / Zleceniodawcy
   g. udostępnienie danych osobowych osobom nieupoważnionym w formie papierowej, elektronicznej i ustnej
   h. telefoniczne próby wyłudzenia danych osobowych
   i. kradzież, zagubienie komputerów lub CD, twardych dysków, Pendrive z danymi osobowymi
   j. maile zachęcające do ujawnienia identyfikatora i/lub hasła,
   k. pojawienie się wirusa komputerowego lub niestandardowe zachowanie komputerów
   l. hasła do systemów przyklejone są w pobliżu komputera

DYREKTOR PRZEDSZKOLA
Marta Wojtarowicz
.....
mgr Marta Wojtarowicz

(Podpis ADO)

X. OBOWIĄZUJĄCE ZASADY ZACHOWANIA POUFNOŚCI I OCHRONY DANYCH OSOBOWYCH

1. Każda z osób dopuszczona do przetwarzania danych osobowych jest zobowiązana do:
   a. przetwarzania danych osobowych wyłącznie w zakresie i celu przewidzianym w powierzonych przez Pracodawcę / Zleceniodawcę zadaniach
   b. zachowania w tajemnicy danych osobowych do których ma dostęp w związku z wykonywaniem zadań powierzonych przez Pracodawcę / Zleceniodawcę
   c. niewykorzystywania danych osobowych w celach niezgodnych z zakresem i celem powierzonych zadań przez Pracodawcę / Zleceniodawcę
   d. zachowania w tajemnicy sposobów zabezpieczenia danych osobowych
   e. ochrony danych osobowych przed przypadkowym lub niezgodnym z prawem zniszczeniem, utratą, modyfikacją danych osobowych, nieuprawnionym ujawnieniem danych osobowych, nieuprawnionym dostępem do danych osobowych oraz przetwarzaniem.

2. Jeśli jest to przewidziane, osoba dopuszczona do przetwarzania odbywa szkolenie z zasad ochrony danych osobowych.

3. Osoby zapoznane z treścią niniejszej Zasad ODO lub przeszkolone zobowiązane są podpisać Oświadczenie o zachowaniu poufności.

4. Zabrania się przekazywania bezpośrednio lub przez telefon danych osobowych osobom nieupoważnionym lub osobom których tożsamości nie można zweryfikować lub osobom podszywającym się pod kogoś innego.

5. Zabrania się przekazywania lub ujawniania danych osobom lub instytucjom, które nie mogą wykazać się jasną podstawą prawną do dostępu do takich danych.

6. Zabrania się ujawniania na grupach dyskusyjnych, forach internetowych, blogach itp. jakichkolwiek szczegółów dotyczących funkcjonowania Jednostki/Podmiotu ADO, w tym informacji na temat sprzętu i oprogramowania, z jakiego korzysta Jednostka/Podmiot oraz informacji kontaktowych innych, niż ogólnodostępne w materiałach zewnętrznych.

DYREKTOR PRZEDSZKOLA
Marta Wojtarowicz
.....mgr Marta Wojtarowicz.....

(Podpis ADO)

POSTĘPOWANIE DYSCYPLINARNE

1. **Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu potraktowane będą jako ciężkie naruszenie obowiązków pracowniczych lub naruszenie zasad współpracy.**
2. **Postępowanie sprzeczne z powyższymi zasadami może też być uznane przez Pracodawcę/Zleceniodawcę za naruszenie przepisów karnych zawartych w ogólnym Rozporządzeniu o ochronie danych UE z dnia 27 kwietnia 2016r.**