PRZEDSZKOLE "MIŚ"
W PNIEWACH
ul. Dworcowa 23, 62-045 Pniewy
tel. 61 29 11 216
NIP 7871967080 REGON 631578839

Załącznik nr 17 do Polityki ochrony danych osobowych

Regulamin ochrony danych osobowych

w Przedszkolu „Miś" w Pniewach

Regulamin ochrony danych osobowych stanowi wykaz podstawowych obowiązków z zakresu przestrzegania zasad ochrony danych osobowych zgodnie z przepisami RODO dla:

- Pracowników
- Współpracowników
- Pracowników podmiotów trzecich, posiadających dostęp do danych osobowych przetwarzanych przez Administratora / Podmiot przetwarzający
- Użytkowników systemów informatycznych z dostępem do danych osobowych przetwarzanych przez Administratora / Podmiot przetwarzający

Zasady użytkowania sprzętu IT

1. Za sprzęt IT rozumie się: komputery stacjonarne, monitory, drukarki, skanery, ksera, laptopy, tablety i smartfony.
2. W przypadku, gdy użytkownik przetwarzający dane osobowe korzysta ze sprzętu IT, zobowiązany jest do jego ochrony przed jakimkolwiek zniszczeniem lub uszkodzeniem
3. Użytkownik ma obowiązek natychmiast zgłosić zagubienie, utratę lub zniszczenie powierzonego mu sprzętu IT.
4. Samowolne otwieranie, demontaż sprzętu IT, instalowanie dodatkowych urządzeń lub podłączanie jakichkolwiek niezatwierdzonych urządzeń do systemu informatycznego jest zabronione.
5. Użytkownik jest zobowiązany do uniemożliwienia osobom niepowołanym wglądu do danych wyświetlanych na monitorach komputerowych , stosowanie „Polityki czystego ekranu".
6. Przed czasowym opuszczeniem stanowiska pracy, użytkownik zobowiązany jest wywołać blokowany hasłem wygaszacz ekranu lub wylogować się z systemu bądź z programu
7. Po zakończeniu pracy, użytkownik zobowiązany jest:
   -wylogować się z programu, systemu informatycznego, a jeśli to wymagane, przyjęte wyłączyć sprzęt komputerowy;
   -zabezpieczyć stanowisko pracy, w szczególności wszelkie nośniki magnetyczne i optyczne na których znajdują się dane osobowe.
8. Użytkownik jest zobowiązany do usuwania plików z nośników do których mają dostęp inni użytkownicy nieupoważnieni do dostępu do takich plików.
9. Jeśli użytkownik jest uprawniony do niszczenia nośników, powinien trwale zniszczyć sam nośnik lub trwale usunąć z niego dane.
10. Na komputerach przenośnych przeznaczonych do zewnętrznych prezentacji multimedialnych nie powinny, o ile jest to możliwe, znajdować się dane osobowe
11. W przypadku kradzieży lub zgubienia komputera przenośnego, Użytkownik powinien natychmiast powiadomić bezpośredniego przełożonego, ASI, IDO zaznaczając jednocześnie, jakiego rodzaju dane były na tym urządzeniu przechowywane.
12. Użytkownik zobowiązany jest do zabezpieczenia komputera przenośnego w czasie transportu, a w szczególności:
    -zaleca się przenoszenie go w specjalnym futerale torbie ukrywającej fakt transportu komputera przenośnego
    -zabrania się pozostawiania komputera przenośnego w samochodzie podczas postoju w miejscu publicznym bez nadzoru
    -podczas jazdy samochodem zaleca się przechowywanie komputera przenośnego pod tylnym siedzeniem kierowcy
13. W przypadku, gdy komputer przenośny pozostawiony jest w miejscu dostępnym dla osób nieupoważnionych, Użytkownik jest zobowiązany do stosowania linki zabezpieczającej.

14. W przypadku pozostawiania komputerów przenośnych w biurze zaleca się umieszczanie ich po zakończeniu pracy w zamykanych szafkach.
15. Użytkownik komputera przenośnego jest zobowiązany do regularnego tworzenia kopii bezpieczeństwa danych na serwerze lub na określonych nośnikach. Nośniki z takimi kopiami powinny być przechowywane w bezpiecznym miejscu, z uwzględnieniem ochrony przed dostępem.
16. Pracując na komputerze przenośnym w miejscach publicznych i środkach transportu, Użytkownik zobowiązany jest chronić wyświetlane na monitorze informacje przed wglądem osób nieupoważnionych.

Uprawnienia

1. Każdy użytkownik z dostępem do danych osobowych musi posiadać swój własny indywidualny identyfikator (login).
2. Użytkownik otrzymuje dostęp i odpowiednie uprawnienia do zasobów i aplikacji na polecenie przełożonych, tak zwane konto.
3. Użytkownicy nie mają prawa do samodzielnej zmiany uprawnień.
4. Użytkowników obowiązuje zasada pracy wyłącznie na własnym koncie.
5. Zabronione jest udostępnianie innym osobom dostępu do swojego konta.

Polityka haseł

1. Hasła powinny składać się z co najmniej 8 znaków.
2. Hasła powinny zawierać duże litery + małe litery + cyfry + 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 znaków.
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 najmniej co 30 dni.
7. Jeżeli system nie wymusza zmiany haseł, użytkownik zobowiązany jest do samodzielnej zmiany hasła w wymagany sposób.

Zabezpieczenie dokumentacji papierowej

1. Pracownicy są zobowiązani do stosowania „Polityki czystego biurka". Polega ona na zabezpieczaniu, zamykaniu dokumentów np. w szafach, biurkach, pomieszczeniach przed kradzieżą lub wglądem osób nieupoważnionych po godzinach pracy lub podczas ich nieobecności w trakcie godzin pracy.
2. Upoważnieni pracownicy zobowiązani są do niszczenia dokumentów i wydruków w niszczarkach lub utylizacji ich w specjalnych pojemnikach z przeznaczeniem do bezpiecznej utylizacji.
3. Zabrania się pozostawiania dokumentów z danymi osobowymi poza zabezpieczonymi pomieszczeniami.
4. Zabrania się wyrzucania niezniszczonych dokumentów na śmietnik lub porzucania ich na zewnątrz.

Zasady wynoszenia nośników na zewnątrz

1. Użytkownicy nie mogą wynosić na zewnątrz organizacji sprzętu IT, wymiennych elektronicznych nośników informacji z zapisanymi danymi osobowymi bez zgody.
2. Dane osobowe wynoszone poza organizację muszą być zaszyfrowane poprzez szyfrowanie nośnika, zahasłowanie plików zgodnie z przyjętymi zasadami dotyczącymi haseł.
3. Należy zapewnić bezpieczne przewożenie dokumentacji papierowej w plecakach, teczkach.

4. Należy korzystać ze sprawdzonych firm kurierskich.
5. W przypadku, gdy dokumenty przewozi pracownik, zobowiązany jest do zabezpieczenia przewożonych dokumentów przed zagubieniem i kradzieżą, dostępem osób trzecich.

Zasady korzystania z sieci Internet

1. Użytkownik zobowiązany jest do korzystania z sieci Internet 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 osoby upoważnionej, ASI i tylko w uzasadnionych przypadkach.
3. Użytkownik ponosi odpowiedzialność za szkody spowodowane przez oprogramowanie instalowane z sieci Internet.
4. Zabrania się wchodzenia na strony, na których prezentowane są informacje o charakterze przestępczym, hackerskim, pornograficznym, lub innym zakazanym przez prawo.
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 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 lub podania naszych loginów i haseł, PIN-ów, numerów kart płatniczych przez sieć Internet.

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 wykorzystywać mechanizmy kryptograficzne.
3. W przypadku zabezpieczenia plików hasłem, obowiązuje minimum 8 znaków: duże i małe litery i cyfry lub znaki specjalne, hasło należy przesłać odrębnym mailem lub inną metodą np. telefonicznie lub SMS-em.
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. Nie należy otwierać załączników w mailach nawet od rzekomo znanych nam nadawców bez weryfikacji tegoż nadawcy.
7. Bez weryfikacji wiarygodności nadawcy, nie należy „klikać" na hiperlinki w mailach, gdyż mogą to być hiperlinki do stron zainfekowanych lub niebezpiecznych.
8. Należy zgłaszać bezpośredniemu przełożonemu, ASI przypadki podejrzanych emaili.
9. Użytkownicy nie powinni rozsyłać „niezawodowych" emaili w formie „łańcuszków szczęścia".
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 nie powinni rozsyłać, maili zawierających załączniki o dużym rozmiarze.
12. Użytkownicy powinni okresowo kasować niepotrzebne maile.
13. Mail służbowy jest przeznaczony wyłącznie do wykonywania obowiązków służbowych.
14. Zakazuje się wysyłania korespondencji służbowej na prywatne skrzynki pocztowe pracowników lub innych osób.
15. Użytkownicy mają prawo korzystać z poczty mailowej dla celów prywatnych wyłącznie okazjonalnie i powinno być to ograniczone do niezbędnego minimum.
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.
19. Użytkownik bez zgody nie ma prawa wysyłać wiadomości zawierających dane osobowe dotyczące pracowników, klientów, dostawców lub kontrahentów za pośrednictwem sieci Internet, w tym przy użyciu prywatnej elektronicznej skrzynki pocztowej.

Ochrona antywirusowa

1. Użytkownicy zobowiązani są do skanowania plików wprowadzanych z zewnętrznych nośników programem antywirusowym.
2. Zakazane jest wyłączanie systemu antywirusowego podczas pracy systemu informatycznego.
3. W przypadku stwierdzenia zainfekowania systemu lub pojawienia się komunikatów infekcji użytkownik obowiązany jest poinformować niezwłocznie o tym fakcie bezpośredniego przełożonego ASI.

Instrukcja postępowania w przypadku naruszenia ochrony danych osobowych

1. Każda osoba upoważniona do przetwarzania danych osobowych zobowiązana jest do powiadomienia w przypadku stwierdzenia lub podejrzenia naruszenia ochrony danych osobowych bezpośrednio przełożonego, ASI, IDO.
2. Do sytuacji wymagających powiadomienia, należą:
   -niewłaściwe zabezpieczenie fizyczne pomieszczeń, urządzeń i dokumentów
   -niewłaściwe zabezpieczenie sprzętu IT, oprogramowania przed wyciekiem, kradzieżą i utratą danych osobowych
   -nieprzestrzeganie zasad ochrony danych osobowych przez pracowników
3. Do incydentów wymagających powiadomienia, należą:
   -zdarzenia losowe zewnętrzne: pożar obiektu, pomieszczenia, zalanie wodą, utrata zasilania, utrata łączności
   -zdarzenia losowe wewnętrzne: awarie serwera, komputerów, twardych dysków, oprogramowania, pomyłki informatyków, użytkowników, utrata, zagubienie danych
   -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:-
   -ślady na drzwiach, oknach i szafach wskazują na próbę włamania
   -dokumentacja jest niszczona bez użycia niszczarki
   -fizyczna obecność w budynku lub pomieszczeniach osób zachowujących się podejrzanie
   -otwarte drzwi do pomieszczeń, szaf, gdzie przechowywane są dane osobowe
   -ustawienie monitorów pozwala na wgląd osób postronnych w dane osobowe
   -wynoszenie danych osobowych w wersji papierowej i elektronicznej na zewnątrz organizacji bez upoważnienia
   -udostępnienie danych osobowych osobom nieupoważnionym w formie papierowej, elektronicznej i ustnej
   -telefoniczne próby wyłudzenia danych osobowych
   -kradzież, zagubienie komputerów lub CD, twardych dysków, Pen-drivów z danymi osobowymi
   -maile zachęcające do ujawnienia identyfikatora, hasła
   -pojawienie się wirusa komputerowego lub niestandardowe zachowanie komputerów
   -hasła do systemów przyklejone są w pobliżu komputera

Poufność i ochrona danych osobowych

1. Każda z osób dopuszczona do przetwarzania danych osobowych jest zobowiązana do:
   -przetwarzania danych osobowych wyłącznie w zakresie i celu przewidzianym w powierzonych zadaniach

-zachowania w tajemnicy danych osobowych przetwarzanych w związku z wykonywaniem powierzonych zadań
-niewykorzystywania danych osobowych w celach niezgodnych z zakresem i celem powierzonych zadań
-zachowania w tajemnicy sposobów zabezpieczenia danych osobowych
-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. Osoba dopuszczona do przetwarzania odbywa szkolenie z zasad ochrony danych osobowych
3. Osoby zapoznane z treścią niniejszego Regulaminu ochrony danych osobowych lub przeszkolone zobowiązane są podpisać stosowne Oświadczenie o 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

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 zobowiązaniami, może też być uznane za naruszenie przepisów karnych zawartych w ogólnym Rozporządzeniu o ochronie danych UE z dnia 27 kwietnia 2016 r. i Ustawie o ochronie danych osobowych z dnia 10 maja 2018 r.

Dyrektor Przedszkola
mgr Katarzyna Kurek-Brzyk