Placówka Opiekuńczo-Wychowawcza Nr 1
44-335 Jastrzębie-Zdrój
ul. Opolska 7/1-2
NIP 633 223 93 90
tel. 32 47 67 406

ZARZĄDZENIE NR 0211.22.2019

Dyrektora Placówek Opiekuńczo – Wychowawczych Nr 1, 2, 3
w Jastrzębiu – Zdroju

z dnia 13 MARCA 2019 r.

w sprawie wprowadzenia Instrukcji zarządzania systemem informatycznym
w Placówkach Opiekuńczo – Wychowawczych Nr 1, 2, 3

z a r z ą d z a m

§ 1

Wprowadzam Instrukcję zarządzania systemem informatycznym w Placówkach Opiekuńczo – Wychowawczych Nr 1, 2, 3

§ 2

Zarządzenie wchodzi w życie z dniem podjęcia z mocą obowiązująca od 2 stycznia 2019 r.

DYREKTOR
Placówek Opiekuńczo-Wychowawczych
Nr 1,2,3
mgr Izabela Grzybek

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM W PLACÓWKACH OPIEKUŃCZO- WYCHOWAWCZYCH NR 1, NR 2 i NR 3 w JASTRZĘBIU-ZDROJU

I. Nadawanie i rejestrowanie uprawnień do przetwarzania danych w systemie informatycznym.

1. Przetwarzać dane osobowe w systemach informatycznych może wyłącznie osoba posiadająca pisemne upoważnienie do przetwarzania danych osobowych nadane przez Administratora danych dale w treści instrukcji zwanego „ADO".
2. Za tworzenie, modyfikację i nadawanie uprawnień kontom użytkowników odpowiada ADO lub wyznaczony informatyk (Administrator Systemu Informatycznego) dalej zwany „ASI".
3. ASI nadaje uprawnienia w systemie informatycznym na podstawie upoważnienia nadanego pracownikowi przez ADO.
4. Usuwanie kont stosowane jest wyłącznie w uzasadnionych przypadkach. Standardowo, przy ustaniu potrzeby utrzymywania konta danego użytkownika ulega ono dezaktywacji w celu zachowania historii jego aktywności.
5. Osoby dopuszczone do przetwarzania danych osobowych zobowiązane są do zachowania tajemnicy w zakresie tych danych oraz sposobów ich zabezpieczenia. Obowiązek ten istnieje również po ustaniu stosunku pracy, co jest równoznaczne z cofnięciem uprawnień do przetwarzania danych osobowych.

II. Zabezpieczenie danych w systemie informatycznym.

1. Ochronę przed awariami zasilania oraz zakłóceniami w sieci energetycznej serwera i stacji roboczych, na których przetwarzane są dane osobowe zapewniają zasilacze UPS.
2. W przypadkach awaryjnych, takich jak nagły brak zasilania, ciągłości funkcjonowania systemu informatycznego podtrzymuje bateria zasilająca serwerowni. W czasie pracy baterii zasilającej ASI dokonuje oceny sytuacji i podejmuje wszelkie niezbędne kroki w celu zachowania integralności danych oraz przywrócenia normalnego funkcjonowania systemu.
3. Oprogramowanie wykorzystywane do przetwarzania danych posiada własny system kont (zabezpieczonych hasłami) i uprawnień. Zmiany hasła jest wymuszona automatycznie przez system lub należy do obowiązków użytkownika konta.
4. **Hasła do systemu stacji roboczych muszą mieć mają długość przynajmniej 12 znaków (duże i małe litery oraz cyfry lub znaki specjalne) i powinny być zmieniane nie rzadziej niż co 30 dni. Hasło nie może być zapisywane lub przechowywane w miejscu dostępnym dla osób nieuprawnionych.**
5. Każdy użytkownik systemu informatycznego zobowiązany jest zapamiętać swoją nazwę użytkownika oraz hasło i nie udostępniać go innym osobom.
6. Użytkownik systemu informatycznego powinien pamiętać o wylogowaniu się po zakończeniu korzystania z usług systemów informatycznych.
7. W przypadku utracenia hasła użytkownik ma obowiązek skontaktować się z Administratorem Danych Osobowych celem uzyskania nowego hasła.

8. Hasła użytkowników uprzywilejowanych posiadających uprawnienia na poziomie administratorów systemów informatycznych objęte są takimi samymi restrykcjami dotyczącymi ich poufności jak pozostałe hasła.
9. System informatyczny przetwarzający dane osobowe powinien posiadać mechanizmy pozwalające na odnotowanie faktu wykonania operacji na danych. W szczególności zapis ten powinien obejmować :
    1) rozpoczęcie i zakończenie pracy przez użytkownika systemu,
    2) operacje wykonywane na przetwarzanych danych,
    3) przesyłanie za pośrednictwem systemu danych osobowych przetwarzanych w systemie
    4) informatycznym innym podmiotom nie będącym właścicielem ani współwłaścicielem systemu,
    5) nieudane próby dostępu do systemu informatycznego przetwarzającego dane osobowe oraz nieudane próby wykonania operacji na danych osobowych,
    6) błędy w działaniu systemu informatycznego podczas pracy danego użytkownika.
10. System informatyczny powinien zapewnić zapis faktu przekazania danych osobowych z uwzględnieniem :
    1) identyfikatora osoby, której dane dotyczą,
    2) osoby przesyłające dane,
    3) odbiorcy danych,
    4) zakresu przekazanych danych osobowych,
    5) daty operacji,
    6) sposobu przekazania danych.
11. Stosuje się aktywną ochronę antywirusową lub w przypadku braku takiej możliwości przynajmniej raz w tygodniu skanowanie całego systemu (w poszukiwaniu „ złośliwego oprogramowania ") na każdym komputerze, na którym przetwarzane są dane osobowe.
12. Za dokonywanie skanowania systemu w poszukiwaniu złośliwego oprogramowania (w przypadku braku ochrony rezydentnej) i aktualizację bazy wirusów odpowiada użytkownik stacji roboczej.

III. Zasady bezpieczeństwa podczas pracy w systemie informatycznym.

1. W celu rozpoczęcia pracy w systemie informatycznym użytkownik :
    1) loguje się do systemu operacyjnego przy pomocy identyfikatora i hasła (autoryzacja użytkownika w bazie usług katalogowych),
    2) loguje się do programów wymagających dodatkowego wprowadzenia unikalnego identyfikatora i hasła.
2. W sytuacji tymczasowego zaprzestania pracy na skutek nieobecności przy stanowisku komputerowym należy uniemożliwić osobom postronnym korzystanie z systemu informatycznego poprzez wylogowanie się z systemu lub uruchomienie wygaszacza ekranu chronionego hasłem.
3. W sytuacji gdy wgląd w wyświetlane na monitorze dane może mieć nieuprawniona osoba należy tymczasowo zmienić widok wyświetlany na monitorze lub obrócić monitor (przymknąć ekran laptopa) w sposób uniemożliwiający wgląd w wyświetlaną treść.

4. Użytkownik wyrejestrowuje się z systemu informatycznego przed wyłączeniem stacji komputerowej poprzez zamknięcie programu przetwarzającego dane oraz wylogowanie się z systemu operacyjnego.
5. Zawieszanie korzystania z systemu informatycznego może nastąpić losowo wskutek awarii lub planowo (np. w celu konserwacji sprzętu). Planowe zawieszenie prac jest poprzedzone poinformowaniem pracowników Przedszkola przez ASI na co najmniej 30 minut przed planowanym zawieszeniem.
6. Pracownik korzystający z systemu informatycznego zobowiązany jest do powiadomienia ADO o:
   1)podejrzeniu naruszenia bezpieczeństwa systemu,
   2)braku możliwości zalogowania się użytkownika na jego konto,
   3)stwierdzeniu fizycznej ingerencji w przetwarzane dane,
   4)stwierdzeniu użytkowania narzędzia programowego lub sprzętowego.
7. Na fakt naruszenia zabezpieczeń systemu mogą wskazywać :
   1)nietypowy stan stacji roboczej (np. brak zasilania, problemy z uruchomieniem),
   2)wszelkiego rodzaju różnice w funkcjonowaniu systemu (np. komunikaty informujące o błędach, brak dostępu do funkcji systemu, nieprawidłowości w wykonywanych operacjach),
   3)różnice w zawartości zbioru danych osobowych (np. brak lub nadmiar danych),
   4)inne nadzwyczajne sytuacje.

IV. Tworzenie kopii zapasowych

1. Dane systemów kopiowane są w trybie tygodniowym (kopie baz danych , kopia awaryjna systemu serwera). Kopie awaryjne danych zapisywanych w programach wykonywane są co tydzień (w ostatni dzień roboczy tygodnia po zakończeniu pracy). Kopie programów i narzędzi programowych służących do przetwarzania danych tworzy się metodą całościową każdorazowo przed aktualizacją na macierzy dyskowej.
2. Odpowiedzialny za wykonanie kopii danych i kopii awaryjnych jest pracownik obsługujący dany program przetwarzający dane. Kopie zbiorów umieszczonych na serwerze wykonywane są automatycznie dedykowanym oprogramowaniem wytworzonym we własnym zakresie.
3. Kopie awaryjne oraz dodatkowe kopie wynikające z np. zmiany platformy sprzętowej zabezpieczane i przechowywane są przez ADO . Osobą odpowiedzialną za wymianę kopii awaryjnych na aktualne jest ASI.
4. Okresową weryfikację kopii bezpieczeństwa pod kątem ich przydatności do odtworzenia danych przeprowadza ASI.
5. Usuwanie kopii danych następuje poprzez bezpieczne kasowanie. Nośniki danych, na których zapisywane są kopie bezpieczeństwa niszczy się trwale w sposób mechaniczny.

V. Udostępnienie danych

Dane osobowe przetwarzane w systemach informatycznych mogą być udostępnione osobom i podmiotom z mocy przepisów prawa oraz na uzasadniony wniosek tylko i wyłącznie za zgodą ADO.

VI. Przeglądy i konserwacja systemów

1. Wszelkie prace związane z naprawami i konserwacją systemu informatycznego przetwarzającego dane osobowe mogą być wykonywane wyłącznie przez pracowników ADO lub przez upoważnionych przedstawicieli wykonawców .
2. Prace wymienione w pkt.1 powinny uwzględniać wymagany poziom zabezpieczenia tych danych przed dostępem do nich osób nieupoważnionych.
3. Przed rozpoczęciem prac wymienionych powyżej przez osoby niebędące pracownikami ADO należy dokonać potwierdzenia tożsamości tych osób.

VII. Niszczenie wydruków i nośników danych

1. Wszelkie wydruki z systemów informatycznych zawierające dane osobowe przechowywane są w miejscu uniemożliwiającym ich odczyt przez osoby nieuprawnione, w zamkniętych szafach lub pomieszczeniach i po upływie ich przydatności są niszczone przy użyciu niszczarek.
2. Usuwanie zapisów na nośnikach danych powinno odbywać się poprzez wymazanie informacji oraz formatowanie nośnika.
3. Uszkodzone nośniki danych przed ich wyrzuceniem należy fizycznie zniszczyć.
4. Po wykorzystaniu wydruki zawierające dane osobowe powinny być niszczone w niszczarce.

VIII. Zasady użytkowania laptopów oraz dysków przenośnych

1. **Dane osobowe lub danych poufne muszą zostać zaszyfrowane na dysku i zabezpieczone co najmniej 12-znakowym hasłem (duże, małe litery i cyfry).**
2. Komputery przenośne są wykorzystywane do prac służbowych. W przypadku konieczności korzystania z komputera przenośnego w innym celu wszystkie dane osobowe muszą być *zabezpieczone hasłem*.
3. W przypadku kradzieży/zgubienia lub naruszenia ochrony danych osobowych osoba upoważniona zobowiązana jest zgłosić zdarzenie/problem ADO.
4. Osoba upoważniona zobowiązana jest do zabezpieczenia komputera przenośnego w czasie transportu, a przede wszystkim:
   1) zaleca się przenoszenie komputera przenośnego w teczce lub aktówce,
   2) zabrania się pozostawiania komputera przenośnego w samochodzie podczas nieobecności osoby upoważnionej.
5. Gdy komputer przenośny jest pozostawiony w miejscu dostępnym dla osób nieupoważnionych, konieczne jest zabezpieczenie hasłem. Dotyczy to przede wszystkim zabezpieczenia komputera przenośnego na stanowisku pracy, podczas przedstawiania prezentacji, szkolenia.
6. Użytkownik komputera przenośnego jest zobowiązany do regularnego tworzenia kopii bezpieczeństwa danych na serwerze. Nośniki z takimi kopiami powinny być przechowywane w miejscu zabezpieczonym przed dostępem osób nieupoważnionych.
7. Pracując na komputerze przenośnym w miejscach publicznych i środkach transportu, osoba upoważniona zobowiązana jest do chronienia wyświetlanych danych osobowych na monitorze przed wglądem osób nieupoważnionych.

DYREKTOR
Placówek Opiekuńczo-Wychowawczych
Nr 1,2,3

……mgr Izabela Czybek……

(Zatwierdzam)