Załącznik nr 4 do Zarządzenia nr 12/2018
dyrektora Szkoły Podstawowej im. Jana Pawła II w Chwarstnicy
z dnia 03.09.2018r.

Instrukcja Zarządzania Systemem Informatycznym podczas przetwarzania dokumentacji w postaci tradycyjnej oraz elektronicznej w Szkole Podstawowej im. Jana Pawła II w Chwarstnicy ul. Gryfińska 19, 74-100 Gryfino

Szczegóły dokumentu:

Sporządził:	*Marta Maj* Inspektor Ochrony Danych
Data przekazania:	01.09.2018r.

Historia zmian

Data	Wersja	Utworzona przez	Opis zmiany

Spis treści

1. Charakterystyka systemu. 4
2. Podstawowe pojęcia i skróty. 4
3. Ogólne zasady pracy w systemie. 4
4. Procedury nadawania uprawnień. 4
5. Metody i środki uwierzytelnienia. 5
6. Procedury rozpoczęcia, zawieszenia i zakończenia pracy……5
7. Procedury korzystania ze sprzętu przenośnego……5
8. Zasady bezpiecznej wymiany informacji. 6
9. Procedury tworzenia i sposobu przechowywania kopii zapasowych. 6
10. Sposób zabezpieczenia systemu przed działalnością złośliwego oprogramowania. 7
11. Procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji.....7
12. Podstawy prawne. 7
13. Postanowienia końcowe. 7

1. Charakterystyka systemu.

Sieć informatyczną, w której przetwarzane są dane osobowe stanowią wszystkie pracujące obecne

i przyszłe, komputery stacjonarne, a także urządzenia peryferyjne i sieciowe. Sygnał internetowy dostarczany jest przez usługodawcę internetowego i odpowiednio zabezpieczony.

System zabezpieczony jest oprogramowaniem antywirusowym zainstalowanym na każdym stanowisku.

2. Podstawowe pojęcia i skróty.

Słownik podstawowych pojęć oraz skrótów występujących w niniejszej instrukcji znajduje się

w dokumencie Polityki Bezpieczeństwa Informacji.

3. Ogólne zasady pracy w systemie.

ADO odpowiada za korygowanie niniejszej instrukcji w przypadku uzasadnionych zmian w przepisach prawnych dotyczących przetwarzania danych osobowych w systemach informatycznych, jak również zmian organizacyjno-funkcjonalnych. Przetwarzanie danych w systemie informatycznym może być realizowane wyłącznie poprzez dopuszczone przez ADO do eksploatacji licencjonowane oprogramowanie.

Użytkownikom zabrania się:

a) korzystania ze stanowisk komputerowych podłączonych do sieci informatycznej poza godzinami i dniami pracy bez zgody przełożonego,
b) umożliwiania dostępu do zasobów sieci Internetowej osobom nieuprawnionym,
c) samowolnego instalowania i używania programów komputerowych,
d) udostępniania stanowisk roboczych osobom nieuprawnionym,
e) korzystania z nielicencjonowanego oprogramowania oraz wykonywania jakichkolwiek działań niezgodnych z ustawą o ochronie praw autorskich,
f) używania komputera bez zainstalowanego oprogramowania antywirusowego.

4. Procedury nadawania uprawnień.

Do przetwarzania danych osobowych zgromadzonych w systemie informatycznym jak również

w rejestrach tradycyjnych wymagane jest upoważnienie. Upoważnienie nadaje ADO na podstawie wniosku o nadanie uprawnień. Uprawnienia do pracy w systemie informatycznym odbierane są czasowo, poprzez zablokowanie konta w przypadku:

a) nieobecności użytkownika w pracy trwającej dłużej niż 21 dni kalendarzowych,
b) zawieszenia w pełnieniu obowiązków służbowych.

Uprawnienia do przetwarzania danych osobowych odbierane są trwale w przypadku ustania stosunku pracy. Osoby, które zostały upoważnione do przetwarzania danych, są obowiązane zachować

w tajemnicy te dane osobowe oraz sposoby ich zabezpieczenia nawet w przypadku ustania stosunku pracy.

5. Metody i środki uwierzytelnienia.

System informatyczny przetwarzający dane osobowe wykorzystuje mechanizm identyfikatora i hasła jako narzędzi umożliwiających bezpieczne uwierzytelnienie.

Hasło składa się z co najmniej ośmiu znaków, zawiera co najmniej jedną małą i wielką literę, jedną cyfrę lub jeden znak specjalny. Hasło nie powinno zawierać żadnych informacji, które można skojarzyć z użytkownikiem komputera (imiona najbliższych, daty urodzenia, inicjały, itp.) i nie może być sekwencją kolejnych znaków klawiatury. W przypadku, gdy istnieje podejrzenie, że hasło mogła poznać osoba nieupoważniona, użytkownik zobowiązany jest do zgłoszenia tego faktu Administratorowi Danych Osobowych. Hasło nie może być zapisywane i przechowywane.

Użytkownik nie może udostępniać identyfikatora oraz haseł osobom nieupoważnionym.

6. Procedury rozpoczęcia, zawieszenia i zakończenia pracy.

Każdy użytkownik korzystający z systemu informatycznego przystępując do pracy powinien podać swoje dane dostępu do komputera i systemu, tj. identyfikator i hasło.

Zawieszenie pracy polega na opuszczeniu stanowiska pracy bez wylogowania się i jest dopuszczalne tylko w przypadku pozostania w pomieszczeniu. Użytkownik jest zobowiązany w takiej sytuacji do włączenia wygaszacza ekranu odblokowywanego hasłem.

Zakończenie pracy w systemie następuje poprzez prawidłowe, wymagane przez daną aplikację oraz system operacyjny, wykonanie czynności kończących. Niedopuszczalne jest zakończenie pracy poprzez wyłączenie napięcia zasilającego bez pełnej procedury zamknięcia.

Ekrany monitorów stanowisk komputerowych, na których odbywa się przetwarzanie danych osobowych powinny być w miarę możliwości tak umieszczone, aby uniemożliwić wgląd w dane osobom postronnym przebywającym w pomieszczeniu oraz powinny automatycznie się wyłączać poprzez stosowanie wygaszaczy ekranowych uruchamiających blokadę pracy na komputerze.

Osoba przetwarzająca dane osobowe w przypadku konieczności opuszczenia pomieszczenia, obowiązana jest prawidłowo, zgodnie z instrukcją obsługi systemu, zakończyć pracę w systemie.

7. Procedury korzystania ze sprzętu przenośnego

1. Pracownicy Szkoły Podstawowej w Chwarstnicy, którym powierzono sprzęt mobilny są upoważnieni do wynoszenia go poza obszar przetwarzania, jeśli jest to uzasadnione wykonywanymi obowiązkami. W innych przypadkach lub kiedy wynoszenie ma charakter sporadyczny należy poinformować o tym fakcie przełożonego.
2. Urządzenia mobilne są wyposażone w mechanizmy szyfrujące, jeśli występuje na nich przetwarzanie danych osobowych. Szyfrowanie dysków jest realizowane przez funkcje systemu operacyjnego, dedykowane rozwiązania producenta sprzętu lub zewnętrzne programy.
3. W zależności od wykorzystywanego rozwiązania, użytkownik urządzenia przenośnego może być zobowiązany do wykonania dwustopniowego logowania. W przypadku logowania dwustopniowego, oba hasła muszą spełniać wymagania opisane w niniejszej Instrukcji. Zmiana hasła do odszyfrowania nie jest konieczna co 30 dni – jednak dopuszczalne jest wykorzystywanie jednego hasła do obu logowań.

4. Pracownik jest zobowiązany do zapewnienia odpowiedniej ochrony fizycznej sprzętu mobilnego, w szczególności poprzez niepozostawianie go bez nadzoru oraz bezpieczny transport i eksploatację z uwagą na czynniki środowiskowe, tj. zalanie lub przegrzanie.
5. Należy unikać podłączania się do sieci publicznej za pośrednictwem ogólnodostępnych hotspotów wi-fi. Wykonując pracę poza miejscem przetwarzania, użytkownik powinien ograniczać ryzyko wglądu w wyświetlane informacje osób nieupoważnionych. Dostęp zdalny do sieci wewnętrznej lub poszczególnych systemów informatycznych nie jest realizowany dla pracowników.
6. Dostęp do sprzętu mobilnego powinna mieć jedynie uprawniona osoba. Obowiązuje zakaz dopuszczania osób nieupoważnionych do sprzętu komputerowego.

7. Zasady bezpiecznej wymiany informacji

Przed wysłaniem wiadomości zawierającej dane osobowe, należy się upewnić, że podmiot odbierający jest do nich uprawiony. Wysyłając wiadomości elektroniczne należy sprawdzić poprawność wprowadzonego adresu mailowego oraz załączonych plików.
Weryfikacja wysyłanych treści oraz adresatów dotyczy również innych kanałów komunikacji.
W szczególności, w przypadku faxu, należy zweryfikować obecność osoby odbierającej przy urządzeniu.
Szyfrowanie załączanych plików dokonuje się poprzez ich spakowanie w archiwum oraz ustalenie hasła, np. w programie 7-zip. Hasło do archiwum powinno być przesyłane inną drogą niż zaszyfrowane archiwum.
Wiadomości przychodzące należy zweryfikować poprzez:

a) weryfikację adresu mailowego nadawcy,
b) analizę treści pod kątem prób wyłudzeń informacji,
c) poprawność załączonych w treści linków – przed kliknięciem, poprzez zawieszenie kursora nad linkiem i weryfikacje wyświetlonego adresu.

8. Procedury tworzenia i sposobu przechowywania kopii zapasowych.

Dane osobowe zabezpiecza się poprzez wykonywanie kopii awaryjnych.

Za proces tworzenia kopii programów odpowiedzialny jest użytkownik systemu.

Kopie przechowywane są w zamkniętej szafie w wydzielonym i zabezpieczonym pomieszczeniu.

Nośniki, na których są przechowywane kopie danych osobowych powinny być wyraźnie oznaczone.

Kopie usuwa się niezwłocznie po ustaniu ich użyteczności w sposób uniemożliwiający odtworzenie danych. Użytkownik tworzy wydruki związane z przetwarzaniem danych osobowych wyłącznie

w zakresie i ilości niezbędnej dla celów służbowych w uzgodnieniu z przełożonym.

Wszystkie dokumenty, zestawienia i wydruki zawierające dane osobowe powinny być chronione przed dostępem osób nieupoważnionych.

Użytkownik przechowuje dokumenty w zamkniętej szafie w pomieszczeniu zabezpieczonym przed nieuprawnionym dostępem.

9. Sposób zabezpieczenia systemu przed działalnością złośliwego oprogramowania.

ADO zapewnia ochronę antywirusową. System antywirusowy jest skonfigurowany w sposób zapewniający na bieżąco skanowanie wszystkich informacji przetwarzanych w systemie, a zwłaszcza poczty elektronicznej i stron internetowych.

10. Procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji.

Urządzenia, dyski lub inne elektroniczne nośniki informacji, zawierające dane osobowe, przeznaczone do:

a) likwidacji — pozbawia się wcześniej zapisu tych danych, a w przypadku gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie,
b) przekazania podmiotowi nieuprawnionemu do przetwarzania danych — pozbawia się wcześniej zapisu tych danych, w sposób uniemożliwiający ich odzyskanie,
c) naprawy — pozbawia się wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie albo naprawia się je pod nadzorem wyznaczonego użytkownika przez ADO.

Instalacji, konserwacji oraz napraw sprzętu komputerowego dokonują pracownicy firm wskazanych przez ADO.

Przeglądy i konserwacje systemu oraz nośników informacji służących do przetwarzania danych mogą być wykonywane jedynie przez osoby posiadające upoważnienie wydane przez Administratora Danych Osobowych lub posiadające umowy na powierzenie przetwarzania danych w zakresie konserwacji i napraw.

Wszelkie prace związane z naprawami i konserwacją systemu informatycznego przetwarzającego dane osobowe muszą uwzględniać zachowanie wymaganego poziomu zabezpieczenia tych danych przed dostępem do nich osób nieupoważnionych.

11. Podstawy prawne.

Podstawy prawne niniejszej IZSI znajdują się w dokumencie Polityki Bezpieczeństwa Informacji.

12. Postanowienia końcowe.

W sprawach nieuregulowanych niniejszą IZSI odpowiednie zastosowanie mają reguły i procedury zawarte w dokumentach powiązanych.

Instrukcja Zarządzania Systemem Informatycznym w Szkole Podstawowej w Chwarstnicy wchodzi w życie z dniem podpisania.

……

(podpis Administratora Danych)