Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych w Zespole Szkół w Sokołowie Młp.

Niniejsza Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, zwana dalej Instrukcją, przyjęta została w celu wykazania, że dane osobowe w systemach informatycznych wykorzystywanych przez Zespół Szkół w Sokołowie Małopolskim przetwarzane są w sposób zgodny z przepisami prawa mającymi zastosowanie do takiej czynności, zgodnie z zasadą art. 5 ust. 1 lit. f) rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 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 (dalej RODO).

Definicje:

1. Administrator Danych – Zespół Szkół w Sokołowie Młp. reprezentowany przez Dyrektora ZS w Sokołowie Młp.
2. Dane osobowe – wszelkie informacje, w tym o stanie zdrowia, dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej.
3. System informatyczny – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji, narzędzi programowych zastosowanych w celu przetwarzania danych
4. Użytkownik – osoba upoważniona przez Administratora Danych do przetwarzania danych osobowych.
5. Przetwarzanie danych – jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w Systemach Informatycznych
6. Zabezpieczenie danych w systemie informatycznym – wdrożenie i eksploatacja stosowanych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem.
7. Identyfikator użytkownika – ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym (użytkownika) w razie ;przetwarzania danych osobowych w takim systemie
8. Hasło – ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w Systemie informatycznym (użytkownikowi)

I. Procedura nadawania i zmiany uprawnień

Celem procedury jest minimalizacja ryzyka przetwarzania danych przez osoby nieupoważnione i ich ujawnienia z powodu braku świadomości konieczności ochrony danych osobowych.

1. Każdy pracownik przed przystąpieniem do przetwarzania danych osobowych musi zapoznać się z:
    - „Instrukcją zarządzania systemem informatycznym”
    - zasadami przetwarzania i ochrony danych osobowych zawartych w Rozporządzeniu 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 (RODO),
    - Polityką ochrony danych osobowych.
2. Administrator danych osobowych lub osoba przez niego upoważniona wydaje pracownikowi Upoważnienie do przetwarzania danych osobowych i aktualizuje wykaz osób uprawnionych do przetwarzania danych osobowych.
3. Po wprowadzeniu danych nowego pracownika do systemu Kadrowego (dane muszą zawierać numer PESEL i adres email) automatycznie tworzone jest nowe konto użytkownika w systemie Vulcan. Użytkownik w czasie pierwszego logowania ustanowią własne hasła zabezpieczające.

4. Dostęp do aplikacji i jeżeli jest to wymagane do stacji roboczej nadawany jest pracownikowi w formie indywidualnego identyfikatora (loginu).
5. Jeżeli pracownik ma dostęp do programów udostępnianych przez podmioty zewnętrzne do uprawnienia i identyfikator zostaje nadany przez administratora systemu.
6. W przypadku zmiany zakresu przydzielonych obowiązków administrator odpowiednio modyfikuje uprawnienia do pracy w aplikacjach dziedzinowych.
7. W przypadku zmiany stanowiska, związanej z odebraniem uprawnień do pracy na programach udostępnianych przez podmioty zewnętrzne Administrator danych osobowych powiadamia o tym fakcie odpowiednie instytucje i doprowadza do odebrania uprawnień i wyrejestrowania użytkownika z systemu.
8. Przy przydzielaniu uprawnień obowiązuje zasada minimalizacji uprawnień.
9. Identyfikator użytkownika po wyrejestrowaniu z systemu informatycznego nie może być przydzielony innej osobie.
10. Użytkowników obowiązuje zasada pracy z użyciem własnego loginu. Zabroniona jest praca w jakimkolwiek elemencie systemu informatycznego na loginie innego użytkownika.

II. Polityka haseł (metody i środki uwierzytelniania)

Stosowanie polityki haseł zapewnia, że do systemów informatycznych, w których są przetwarzane dane osobowe mają dostęp tylko osoby do tego upoważnione. W przypadku komputerów ogólnodostępnych, na dyskach których nie zapisuje się plików zawierających dane osobowe, nie stosuje się uwierzytelnienia do komputera. Administrator stosuje następujące wymogi w stosunku do budowy hasła, jego użytkowania i przechowywania:

1. Użytkownik komputera i aplikacji, w celu uwierzytelnienia podaje indywidualny login i hasło.
2. Hasło użytkownika powinno mieć minimum 8 znaków, zawierać co najmniej jedną dużą i jedną małą literę jedną cyfrę i znak specjalny.
3. Hasło powinno być zmieniane co miesiąc nawet, jeżeli aplikacja tego nie wymaga i nie powtarzać się częściej niż co 6 miesięcy.
4. Hasła wpisywane z klawiatury nie mogą pojawiać się na ekranie monitorów w formie jawnej.
5. Hasła dostępu do aplikacji, przy każdym logowaniu, powinny być wpisywane z klawiatury.
6. Zabrania się korzystania z funkcji „Zapamiętaj mnie na tym komputerze”.
7. Hasło nie powinno zawierać żadnych informacji, które można kojarzyć z użytkownikiem komputera np. osobiste dane użytkownika, tj. nazwisko, inicjały, imiona, marka lub nr rejestracyjny samochodu itp.
8. Hasło nie może być zapisywane w miejscu dostępnym dla osób nieuprawnionych.
9. Użytkownik nie może udostępnić swojego identyfikatora oraz hasła jak również dostępu do stanowiska roboczego po uwierzytelnieniu w systemie osobom nieuprawnionym.
10. Hasło użytkownika należy utrzymywać w tajemnicy, również po upływie jego ważności.
11. Raz użyty identyfikator nie może być przydzielony innemu użytkownikowi systemu.

12. W przypadku, gdy istnieje podejrzenie, że hasło mogła poznać osoba nieuprawniona, użytkownik zobowiązany jest do natychmiastowej zmiany hasła, lub w razie problemów do powiadomienia o tym fakcie Administratora Danych Osobowych.

III. Procedura tworzenia kopii zapasowych

Celem procedury jest zapewnienie, że w przypadku awarii dysku lub zakłócenia spójności lub dostępności danych z różnych powodów istnieje możliwość ich odtworzenia.

1. Kopie zapasowe danych zgromadzonych w systemie informatycznym Vulcan zabezpiecza firma Vulcan.
2. Kopie zapasowe i doraźne lokalnej Bazy Danych SIO, sporządza sekretarz szkoły.
3. Kopie zapasowe bazy danych PŁATNIK sporządza księgowa, raz w miesiącu.
4. Doraźne kopie plików, tworzonych poza aplikacjami, zawierających dane osobowych, wykonują użytkownicy komputerów, na których pliki zostały utworzone. Wykonanie kopii doraźnych nie jest obowiązkowe. Użytkownik sam decyduje o wykonaniu tych kopii.
5. Wszystkie kopie zapasowe wykonane są na nośnikach zewnętrznych będących własnością szkoły.
6. Wszystkie tematy zajęć muszą być uzupełnione w iDzienniku z dniem zakończenia zajęć edukacyjnych w danym roku szkolnym, za ich uzupełnienia odpowiada nauczyciel realizujący zajęcia.
7. Wszystkie informacje o uczniach muszą być uzupełnione w eDzienniku z dniem zakończenia zajęć edukacyjnych, za ich uzupełnienie odpowiada wychowawca oddziału.
8. W terminie 10 dni od zakończenia roku szkolnego, administrator eDziennika zapisuje dane stanowiące dziennik elektroniczny na zewnętrznym nośniku danych, według stanu na dzień zakończenia roku szkolnego. Kopia eDziennika powinna być podpisana kwalifikowanym certyfikatem podpisu elektronicznego.
9. Nośniki danych po ustaniu ich użyteczności należy pozbawić danych lub zniszczyć w sposób uniemożliwiający odczyt danych.

IV. Sposób, miejsce i okres przechowywania elektronicznych nośników zawierających dane osobowe i kopii zapasowych

1. Kopie zapasowe wykonywane są na pendrive lub dysku wymiennym.
2. Kopie zapasowe i doraźne przechowuje się w zamkniętych meblach biurowych w miejscu wykonania kopii.
3. Zabrania się pozostawiania nośników, zawierających kopie zapasowe w komputerach.
4. Kopie eDziennika przechowuje się Zakładowej Składnicy Akt.

V. Ochrona przed oprogramowaniem złośliwym

1. Na komputerach zainstalowane są programy antywirusowe. Przy konfiguracji programu antywirusowego określa się między innymi zasady:
   - aktualizacji baz antywirusowych,
   - skanowania komputera programem antywirusowym.

2. Za konfigurację programu antywirusowego odpowiada informatyk lub inna osoba upoważniona przez Administratora Danych Osobowych.
3. Użytkownikowi komputera zabrania się dokonywania zmiany ustawień programu antywirusowego.
4. W przypadku, gdy na komputerze pojawią się jakiekolwiek komunikaty pochodzące od programu antywirusowego, użytkownik ma obowiązek powiadomić o tym fakcie ADO lub administratora systemu.

VI. Procedury wykonywania przeglądów i konserwacji sprzętu oraz nośników informacji służących do przetwarzania danych

1. Za wykonanie przeglądów i konserwacji komputerów odpowiada administrator systemu. Obowiązki administratora systemu pełni wyznaczona przez ADO osoba.

VII. Stosowane środki ochrony nośników zawierających dane osobowe

1. W przypadku konieczności przekazania do naprawy komputera, na którym przetwarzane były dane osobowe, o ile to możliwe należy wyciągnąć z niego dysk twardy.
2. Każdorazowo przed wycofaniem komputera z eksploatacji lub przeniesieniem komputera na inne stanowisko należy przekazać do administratorowi systemu, by ten nadpisał informacje znajdujące się na dyskach komputera.
3. Wymienne nośniki informacji, przed wyrzuceniem lub przekazaniem ich do firmy utylizacyjnej powinny być fizycznie zniszczone.
4. Proces fizycznego zniszczenia nośników informacji powinien być nadzorowany przez wyznaczone przez ADO osoby.
5. Z procesu fizycznego zniszczenia nośników powinien powstać protokół.
6. Wydruki komputerowe i wymienne nośniki informacji zawierające dane osobowe powinny być przechowywane w zamykanych szafach.

VIII. Procedura bezpiecznego korzystania z komputerów przenośnych

1. Dysk komputera przenośnego powinien być zabezpieczony przez zastosowanie oprogramowania szyfrującego.
2. Komputera przenośnego nie należy pozostawiać bez nadzoru w miejscach publicznych, między innymi w samochodzie czy przechowalni bagażu.
3. Z komputera przenośnego należy korzystać w sposób minimalizujący ryzyko dostępu do przetwarzanych danych przez osoby nieupoważnione.
4. Przy korzystaniu z komputera przenośnego w miejscach publicznych i w środkach transportu publicznego należy chronić informacje wyświetlane na monitorze przed wglądem osób nieuprawnionych.
5. Zabrania się dopuszczania osób nieupoważnionych do korzystania z komputera przenośnego na którym przetwarzane są dane osobowe.
6. W przypadku kradzieży lub zagubienia komputera przenośnego należy bezzwłocznie powiadomić Administratora Danych.