Szkoła Podstawowa im. Marii Skłodowskiej-Curie w Starych Bielicach

Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych

Zatwierdził:

……

(data, podpis)

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 Szkołę Podstawową im. Marii Skłodowskiej-Curie w Starych Bielicach 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** – Szkoła Podstawowa im. Marii Skłodowskiej-Curie w Starych Bielicach

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. **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

5. **Zabezpieczenie danych w systemie informatycznym** – wdrożenie i eksploatacja stosowanych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym Przetwarzaniem

6. **Identyfikator** – 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

7. **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:
   - 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,
   - Regulaminem ochrony danych osobowych.
2. Po podpisaniu oświadczenia o zachowaniu poufności (zał. nr 1 do Instrukcji) Administrator danych osobowych lub osoba przez niego upoważniona wydaje pracownikowi Upoważnienie do przetwarzania danych osobowych (zał. nr 2 do Instrukcji) i aktualizuje wykaz osób uprawnionych do przetwarzania danych osobowych.
3. Dostęp do aplikacji i jeżeli jest to wymagane do stacji roboczej nadawany jest pracownikowi w formie indywidualnego identyfikatora (loginu).
4. Wprowadzenie informacji o zakończeniu stosunku pracy odnotowane w systemie kadrowym powoduje automatyczne wygaśnięcie uprawnień do pracy w aplikacjach.
5. W celu nadania / odebrania uprawnień do pracy w systemie SIO Dyrektor wysyła stosowną informację do Ministerstwa Edukacji Narodowej . W przypadku nadawania uprawnień dla Dyrektora do informacji powinien być dołączony dokument potwierdzający powołanie na stanowisko.
6. Przy przydzielaniu uprawnień obowiązuje zasada minimalizacji uprawnień.
7. Identyfikator użytkownika po wyrejestrowaniu z systemu informatycznego nie może być przydzielony innej osobie.
8. 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 4 miesiące.
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. Zabrania się korzystania z funkcji „Zapamiętaj mnie na tym komputerze".
6. 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.
7. Hasło nie może być zapisywane w miejscu dostępnym dla osób nieuprawnionych.
8. Użytkownik nie może udostępnić swojego identyfikatora oraz hasła jak również dostępu do stanowiska roboczego po uwierzytelnieniu w systemie osobom nieuprawnionym.
9. Hasło użytkownika należy utrzymywać w tajemnicy, również po upływie jego ważności.
10. Raz użyty identyfikator nie może być przydzielony innemu użytkownikowi systemu.
11. 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. Za wykonywanie kopii zapasowych danych zgromadzonych w systemie informatycznym są odpowiedzialni pracownik zatrudniony do obsługi informatycznej szkoły.
2. Za wykonywanie kopii zapasowych danych zapisanych w systemie Płatnik, Progman odpowiada użytkownik. Kopia wykonywana jest na serwerze.
3. Kopie zapasowe innych dokumentów zapisanych na komputerach wykonują doraźnie ich użytkownicy.
4. Na początku kolejnego roku szkolnego, ADO lub osoba przez niego upoważniona, zapisuje dane stanowiące dziennik elektroniczny na zewnętrznym nośniku danych, według stanu na dzień zakończenia roku szkolnego. Kopia dziennika elektronicznego Librus powinna być podpisana kwalifikowanym certyfikatem podpisu elektronicznego.
5. Nośniki danych po ustaniu ich użyteczności należy pozbawić danych lub zniszczyć w sposób uniemożliwiający odczyt danych.

IV. Procedura niszczenia nośników elektronicznych i dokumentów papierowych

Celem procedury jest zapewnienie, że osoby nieupoważnione nie będą miały dostępu do informacji zapisanych na nośnikach elektronicznych i w dokumentach papierowych, które utraciły swą przydatność.

1. Każdorazowo przed wycofaniem komputera z eksploatacji lub przeniesieniem na inne stanowisko należy przekazać go Informatykowi, by ten we właściwy sposób usunął informacje zapisane na dysku.
2. W przypadku konieczności przekazania komputera do naprawy, o ile to możliwe należy wyciągnąć z niego dysk twardy. Jeżeli nie ma takiej możliwości, to naprawa odbywa się w siedzibie Administratora danych.
3. Elektroniczne nośniki informacji (dyski twarde z komputerów i serwerów, pendrive, płyty CD / DVD), które nie będą już wykorzystywane z powodu uszkodzenia lub utraty możliwości ich wykorzystania składowane są w wyznaczonym, chronionym miejscu.
4. Okresowo wszystkie nośniki elektroniczne są komisyjnie, fizycznie niszczone przez np. pocięcie, nawiercenia, trwałe uszkodzenie przy użyciu młotka, demagnetyzację.
5. Zniszczenie nośników jest potwierdzone protokołem zniszczenia podpisanym przez osoby uczestniczące w niszczeniu.
6. Doraźnie dokumentacja papierowa niszczona jest w niszczarkach.
7. W przypadku konieczności zniszczenia dużych ilości dokumentacji papierowej jest ona przekazywana do firmy niszczącej dokumenty papierowe. Firma wystawia certyfikat potwierdzający zniszczenie dokumentów.

V. Procedura bezpiecznego korzystania z komputerów przenośnych

Celem procedury jest wskazanie podstawowych zabezpieczeń informatycznych i fizycznych, które powinny być stosowane przy konfiguracji komputera oraz podczas jego użytkowania.

1. Dysk komputera przenośnego powinien być zabezpieczony przez zastosowanie oprogramowania szyfrującego lub powinien być zabezpieczony hasłem. Od tej zasady można odstąpić w przypadku, gdy na dysku nie będą przechowywane dokumenty, które zawierają dane osobowe.
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.