Instrukcja zarządzania RODO

w Szkole Podstawowej im. Jana Brzechwy w Radawnicy

1. Wstęp

Instrukcja stanowi wykaz procedur oraz stosowanych środków technicznych i organizacyjnych mających na celu, zgodnie z Art. 32 RODO, zabezpieczyć przetwarzane dane osobowe przed: przypadkowym lub niezgodnym z prawem zniszczeniem, utratą, modyfikacją danych osobowych, nieuprawnionym ujawnieniem danych osobowych oraz nieuprawnionym dostępem do danych osobowych.

2. Zabezpieczenia fizyczne

1. drzwi do pomieszczeń biurowych, archiwów zamykane są na klucz.
2. dokumentację papierową i nośniki elektroniczne przechowywane w pomieszczeniach zabezpieczono w szafach zamykanych na klucz.
3. stosowany jest system alarmowy.

3. Procedura nadawania uprawnień do przetwarzania danych osobowych

Celem procedury jest minimalizacja ryzyka przetwarzania danych przez osoby nieupoważnione.

1. Do obsługi systemu informatycznego służącego do przetwarzania danych osobowych, może być dopuszczona wyłącznie osoba posiadająca upoważnienie do przetwarzania danych osobowych, wydane przez Dyrektora szkoły.
2. Upoważnienia do przetwarzania danych osobowych, o których mowa w punkcie 1 przechowywane są w teczkach akt osobowych pracowników.
3. Dostęp do systemów informatycznych nadawany jest każdemu użytkownikowi w formie indywidualnego identyfikatora (loginu).
4. Za wykonanie czynności nadawania, zmiany, odbierania uprawnień użytkownikowi odpowiada administrator.
5. Użytkowników obowiązuje zasada pracy na własnym koncie. Zabronione jest umożliwianie innym osobom pracy na koncie innego użytkownika. Zasada ta obowiązuje również administratorów systemów.

4. Metody i środki uwierzytelnienia (polityka haseł)

Celem procedury jest zapewnienie, że do systemów informatycznych przetwarzających dane osobowe mają dostęp jedynie osoby do tego upoważnione.

1. Standard hasła: hasło 8 –znakowe, zmieniane co 30, 60 dni.
2. Zmiana hasła jest wymuszana przez system w przypadku logowania do programów.
3. Użytkownicy są zobowiązani do samodzielnej zmiany hasła w przypadku systemu operacyjnego.
4. Hasło oprócz małych i dużych liter winno zawierać znaki specjalne.
5. Hasło powinno być tak zbudowane, aby nie można było go kojarzyć z użytkownikiem komputera – przykładowo nazwisko, imiona, data urodzin własna, dziecka lub małżonka, imię domowego zwierzaka itp.
6. Zastosowano mechanizm blokady dostępu po 3 próbach nieudanego logowania się
7. Hasło nie może znajdować się w miejscu widocznym oraz nie mogą mieć do niego dostęp osoby nieuprawnione.
8. Raz przypisany login nie może być przydzielony innemu użytkownikowi lub po przerwie (przerwa w zatrudnieniu) w pracy temu samemu pracownikowi.

9. W przypadku utraty uprawnień przez osobę administrującą systemem należy niezwłocznie zmienić hasła, do których miała dostęp.

5. Procedura tworzenia kopii zapasowych

1. Kopie zapasowe (z zawartością plików i baz danych) tworzone są w sposób zautomatyzowany w oparciu o specjalne oprogramowanie.
2. Pełne kopie zapasowe zbiorów danych są tworzone raz w miesiącu.
3. Kopie bezpieczeństwa sporządzane są także dla dokumentacji gromadzonej na dyskach stacji roboczych użytkowników.
4. W przypadku awarii systemu kopie zapasowe zbiorów danych należy okresowo sprawdzać pod kątem ich przydatności do odtworzenia.
5. Informatyk sprawuje nadzór nad poprawnością wykonania kopii zapasowych .
6. Nośniki danych po ustaniu ich użyteczności należy pozbawić danych lub zniszczyć w sposób uniemożliwiający odczyt danych.

6. Utylizacja elektronicznych nośników i wydruków

1. Podlegające likwidacji uszkodzone lub przestarzałe nośniki są niszczone w sposób fizyczny.
2. Dokumentacja papierowa niszczona jest w niszczarkach.

7. Procedura zabezpieczenia systemu informatycznego

7.1. Bezpieczeństwo przetwarzania danych poza organizacją

1. Stosuje się szyfrowanie dysków komputerów przenośnych zawierających dane osobowe, jeśli wynoszone są poza obszar organizacji.
2. Dane osobowe na komputerach przenośnych wynoszonych poza obszar organizacji muszą być przechowywane na zaszyfrowanych partycjach.
3. Dyski przenośne / pendrive wynoszone poza organizację muszą być zaszyfrowane.

7.2. Ochrona przed nieautoryzowanym dostępem do sieci lokalnej

Stosowane zabezpieczenia mają na celu zabezpieczenie systemów informatycznych przed nieautoryzowanym dostępem do sieci lokalnej np. przez programy szpiegujące, hackerów.

1. Dokonuje się konfiguracji urządzeń sieciowych oraz sprzętu IT w celu zabezpieczenia przed nieuprawnionym dostępem do nich.
2. Dokonuje się aktualizacji oprogramowania systemów i aplikacji.
3. Zastosowano system antywirusowy i filtr antyspamowy.
4. Stosowany jest Firewall.
5. Zabrania się ściągania na komputery i nośniki danych oprogramowania z Internetu.
6. Zabrania się nieautoryzowanego instalowania własnego oprogramowania na służbowych komputerach.

7.3. Zabezpieczenia infrastruktury IT

1. Dokonano dezaktywacji nieużywanych gniazd sieciowych.
2. Na stacjach roboczych zastosowano „zahasłowane wygaszacze ekranu”, aktywowane po 10 minutach nieaktywności użytkownika.
3. Ustawienie monitorów uniemożliwiające wgląd w dane przez osoby postronne.

7.4. Zabezpieczenia aplikacji

1. W kluczowych aplikacjach stosuje się terminację sesji.
2. Stosuje się szyfrowanie poczty wychodzącej(SSL).
3. Dla aplikacji webowych stosowane jest szyfrowanie z użyciem protokołu SSL.
4. Formularze kontaktowe na stronach www zabezpieczono protokołem SSL.

8. Procedura wykonywania przeglądów i konserwacji

1. Administrator / Informatyk odpowiada za optymalizację zasobów IT.
2. Administrator / Informatyk odpowiada za identyfikację i przyjmowanie zgłoszeń o nieprawidłowościach oraz za poprawność działania zasobów IT.
3. W przypadku napraw dokonywanych na zewnątrz, z komputerów i urządzeń mobilnych należy usunąć nośniki danych lub usunąć te dane.
4. W przypadku naprawy sprzętu z danymi osobowymi na nośniku wymaga się „usługi bezpiecznej naprawy".
5. Czynności konserwacyjne i naprawcze wykonywane przez osoby nieposiadające upoważnień do przetwarzania danych (np. specjalistów z firm zewnętrznych) muszą być wykonywane pod nadzorem osób upoważnionych.

9. Zalecenia w zakresie przetwarzania danych osobowych sposobem tradycyjnym

1. Miejscem tworzenia, uzupełniania i przechowywania dokumentacji dotyczącej przetwarzania danych osobowych sposobem tradycyjnym są pomieszczenia w szkole: gabinet dyrektora, sekretariat, pokój nauczycielski, pomieszczenie biblioteczne.
2. Osoby prowadzące dokumentację zobowiązane są do zachowania tajemnicy służbowej.
3. Dokumentacji, o której mowa w punkcie 1 nie można wynosić poza teren szkoły.
4. Osoby prowadzące dokumentację zobowiązane są do niezwłocznego poinformowania Administratora danych osobowych o podejrzeniu dostępu do dokumentacji przez osoby nieupoważnione.

10. Ustalenia końcowe

10.1. Osobom korzystającym z systemu informatycznego, w którym przetwarzane są dane osobowe w szkole zabrania się:

1. ujawniania loginu i hasła współpracownikom i osobom z zewnątrz,
2. pozostawiania haseł w miejscach widocznych dla innych osób,
3. udostępniania stanowisk pracy wraz z danymi osobowymi osobom nieuprawnionym,
4. używania oprogramowania w innym zakresie niż pozwala na to umowa licencyjna,
5. kopiowania danych na nośniki informacji, kopiowania na inne systemy celem wynoszenia ich poza szkołę,
6. samowolnego instalowania jakichkolwiek programów komputerowych,
7. używania nośników danych udostępnionych przez osoby postronne, niesprawdzonych, niewiadomego pochodzenia,
8. otwierania załączników i wiadomości poczty elektronicznej od nieznanych nadawców.

10.2. Użytkownikowi nie wolno:

1. wyrzucać dokumentów zawierających dane osobowe (mogą być niszczone tylko w niszczarkach),
2. pozostawiać dokumentów zawierających dane osobowe w drukarkach, kserokopiarkach
3. pozostawiać otwartych pomieszczeń, w których przetwarza się dane osobowe,

4. pozostawiać bez nadzoru osoby trzecie przebywające w pomieszczeniach szkoły, w których przetwarzane są dane osobowe,
5. pozostawiać dokumentów na biurku po zakończonej pracy,
6. przekazywać informacji będącymi danymi osobowymi osobom nieupoważnionym.

10.3. Użytkownik zobowiązany jest do:

1. posługiwania się własnym loginem i hasłem w celu uzyskania dostępu do systemów informatycznych,
2. tworzenia haseł trudnych do odgadnięcia dla innych,
3. używania konta służbowego tylko w celach służbowych,
4. nie zakańczania procesu skanowania przez program antywirusowy na komputerze,
5. zabezpieczenia sprzętu komputerowego przenośnego (laptopy) przed kradzieżą lub nieuprawnionym dostępem do danych.