Instrukcja zarządzania RODO

w Szkole Podstawowej im. Tony’ego Halika w Górznej

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 przechowywaną w pomieszczeniach zabezpieczono w szafach zamykanych na klucz.

3. Procedura nadawania uprawnień do przetwarzania danych osobowych.

Celem procedury jest minimalizacja ryzyka przetwarzania danych przez osoby nieupoważnione.

1. Dostęp do systemów informatycznych nadawany jest każdemu użytkownikowi w formie indywidualnego identyfikatora (loginu).
2. Nadawanie, zmiana, odbieranie uprawnień użytkownika do systemów informatycznych odbywa się na polecenie przełożonych (lub innych osób upoważnionych) z użyciem formularza nadawana uprawnień.
3. Za wykonanie czynności nadawania, zmiany, odbierania uprawnień użytkownikowi odpowiada administrator.
4. Obowiązuje zasada minimalizacji uprawnień.
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 minimum 8–znakowe, zmieniane co 30 dni. Użytkownicy są zobowiązani do samodzielnej zmiany hasła).
2. Zastosowano mechanizm blokady dostępu po xxx próbach nieudanego logowania się
3. Hasła administracyjne zdeponowane są w bezpiecznym miejscu.
4. W przypadku utraty uprawnień przez osobę administrującą systemem należy niezwłocznie zmienić hasła, do których miała dostęp.
5. W przypadkach awaryjnych (np. nieobecność administratora) hasło może być przekazane decyzją Dyrektora osobie zastępującej administratora.

6. Po ustaniu sytuacji awaryjnej, Administrator jest zobowiązany do zmiany hasła.

5. Utylizacja elektronicznych nośników i wydruków oraz czyszczenie danych

1. Podlegające likwidacji uszkodzone lub przestarzałe nośniki są niszczone w sposób fizyczny bądź zutylizowane w specjalistycznej firmie.
2. Nośniki informacji muszą być wyczyszczone specjalistycznym oprogramowaniem zanim zostaną przekazane poza obszar organizacji .
3. Dokumentacja papierowa niszczona jest w niszczarkach.

6. Procedura zabezpieczenia systemu informatycznego

6.1. Bezpieczeństwo przetwarzania danych poza organizacją

1. Stosuje się szyfrowanie (veracrypt) 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.
4. Sprzęt mobilny (laptopy) zabezpieczono mechanizmem uwierzytelniania.

6.2. 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.

6.3. Zabezpieczenia infrastruktury IT

1. Na stacjach roboczych zastosowano „zahasłowane wygaszacze ekranu”, aktywowane po kilku minutach nieaktywności użytkownika.
2. Ustawienie monitorów uniemożliwiające wgląd w dane przez osoby postronne.

6.4. Zabezpieczenia aplikacji

1. Przechowywanie zaszyfrowanych danych w chmurze.
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.

7. Procedura wykonywania przeglądów i konserwacji

1. Administrator odpowiada za optymalizację zasobów IT.
2. Administrator 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. Rekomendowane jest korzystanie z serwisu, który dokonuje napraw on-site.
6. Czynności konserwacyjne i naprawcze wykonywane przez osoby nieposiadające upoważnień do przetwarzania danych (np. specjalistów z firm zewnętrznych) muszą być wykonywane pod nadzorem osób upoważnionych .