Instrukcja zarządzania systemem informatycznym

w Zespole Szkół w Kaszczorze

Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz. U. z 2016 r. poz. 922) Ustawa z dnia 26 czerwca 1974 r. Kodeks Pracy (t.j. Dz. U. z 2016 r., poz. 1666)

Rozporządzenie MPiPS z dnia 28 maja 1996 r. w sprawie zakresu prowadzenia przez pracodawców dokumentacji w sprawach związanych ze stosunkiem pracy oraz sposobu prowadzenia akt osobowych pracownika (Dz.U. z 1996 r. Nr 62, poz. 286 z późn. zm.)

Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 w sprawie krajowych ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U.z 2016 poz.113)

§ 1

1. Obszarem do przetwarzania danych osobowych z użyciem sprzętu komputerowego są:

- sekretariat,
- gabinet dyrektora,
- gabinet wicedyrektora,
- księgowość,
- gabinet pedagoga szkolnego,
- biblioteka szkolna,
- świetlica szkolna
- klaso-pracownie

2. Przebywanie osób nieuprawnionych wewnątrz obszaru, o którym mowa w pkt.1 jest dopuszczalna tylko w obecności osób zatrudnionych przy przetwarzaniu tych danych i za zgodą Administratora danych.

3. Administrator danych określa hasła użytkowania komputerów dla przetwarzania danych osobowych. Zmiana hasła jest wymuszana automatycznie przez system.

4. Stosuje się aktywną ochronę antywirusową. Za dokonywanie skanowania systemu w poszukiwaniu złośliwego oprogramowania i aktualizację bazy wirusów odpowiada użytkownik stacji roboczej.

5. Procedura rozpoczęcia i zakończenia pracy:

- na stanowiskach, na których przetwarzane są dane osobowe ekrany monitorów powinny być tak ustawione, aby osoby nieupoważnione nie miały dostępu do informacji na nich wyświetlanych,
- uruchomienie komputera odpowiednim hasłem,

- upewnienie się, że osoby nieupoważnione nie mają możliwości wglądu do danych,
- w razie przerwania pracy zastosowanie nieaktywności użytkownika (wygaszacz ekranu chroniony hasłem),
- upewnienie się czy dane zostały zarejestrowane, aby uniknąć utraty danych z powodu awarii,
- podczas nieobecności osób zatrudnionych przy informatycznym przetwarzaniu danych osobowych pomieszczenia, w których są przetwarzane dane, nie mogą być udostępniane osobom postronnym bez zgody Administratora danych,
- zakończenie pracy związanej z przetwarzaniem danych osobowych powinno odpowiadać wszystkim regułom bezpieczeństwa informacji.

6. Kopie informatyczne, wydruki tworzy się w miarę potrzeb. Odpowiedzialnym za wykonanie kopii danych jest pracownik odsługujący dany program przetwarzający dane. Okresowo kopie zapisuje się na dysku zewnętrznym przechowywanym w zamkniętej szafie.

7. Nośniki danych oraz wydruki, które nie są przeznaczone do udostępniania, przechowuje się w zamykanej szafie, do której dostęp mają tylko osoby uprawnione. Dokumenty niepotrzebne zawierające dane osobowe niszczy się w niszczarce znajdującej się w sekretariacie szkoły.

8. Kopie zapasowe zbiorów danych okresowo sprawdza się pod kątem przydatności. Okresową weryfikację przeprowadza administrator.

9. Administrator danych sprawdza stan urządzeń, zawartość zbiorów danych osobowych i wielkość ich naruszenia.

10. Dane uzupełnia się w oparciu o kopie awaryjne.

§ 2

Postępowanie w przypadku naruszenia bezpieczeństwa danych

1. Naruszeniem zabezpieczenia danych osobowych jest każdy stwierdzony fakt nieuprawnionego ujawnienia danych osobowych, udostepnienia lub umożliwienia dostępu osobom nieupoważnionym, zabrania danych przez osobę nieupoważnioną, uszkodzenia lub usunięcia, a w szczególności:

- Nieautoryzowany dostęp do danych,
- Nieautoryzowane modyfikacje lub zniszczenie danych,
- Udostepnienie danych nieautoryzowanym podmiotom,

- Nielegalne ujawnienie danych,
- Pozyskiwanie danych z nielegalnych źródeł.

2. W przypadku stwierdzenia naruszenia bezpieczeństwa danych, każdy pracownik jest zobowiązany przerwać przetwarzanie danych osobowych i niezwłocznie zgłosić ten fakt administratorowi.
3. Administrator oraz osoby przez niego upoważnione podejmują wszelkie działania mające na celu:
    - Minimalizację negatywnych skutków zdarzenia,
    - Wyjaśnienie okoliczności zdarzenia,
    - Zabezpieczenie dowodów zdarzenia,
    - Umożliwienie dalszego bezpiecznego przetwarzania danych.

4. Nieprzestrzeganie zasad postepowania w przypadku naruszenia ochrony danych osobowych stanowi naruszenie obowiązków pracowniczych i może być przyczyną odpowiedzialności dyscyplinarnej określonej w Kodeksie Pracy.

§ 3

1. Raz w roku, w terminie wyznaczonym przez dyrektora przeprowadzony zostanie audyt wewnętrzny w zakresie bezpieczeństwa informacji.

§ 4

Instrukcja wchodzi w życie z dniem podpisania.

Dyrektor Zespołu Szkół w Kaszczorze