Załącznik do zarządzenia nr 13/2010/2011– Polityka bezpieczeństwa danych osobowych

POLITYKA BEZPIECZEŃSTWA DANYCH OSOBOWYCH

Polityka bezpieczeństwa danych osobowych powstała w oparciu o przepisy ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych i rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 roku w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych.

Dane osobowe to wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej.

W Gimnazjum nr 2 w Rybniku stosuje się wysoki poziom bezpieczeństwa przetwarzania danych osobowych w systemach informatycznych, ponieważ co najmniej jeden komputer, na którym zainstalowane jest oprogramowanie wykorzystywane do przetwarzania danych osobowych, połączony jest z siecią publiczną.

Wykaz budynków, pomieszczeń lub części pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe

Dane osobowe przetwarzane są w budynku Gimnazjum nr 2 w Rybniku przy ul. Grunwaldzkiej 18, w pomieszczeniach sekretariatu, Dyrektora, Zastępcy Dyrektora i Głównego Księgowego.

Wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych

W Gimnazjum nr 2 w Rybniku dane osobowe przetwarzane są w zbiorach papierowych oraz odpowiadających im systemach i programach informatycznych.

Wykaz zbiorów danych osobowych i programów zastosowanych do ich przetwarzania:

Zbiór danych osobowych	Program zastosowany do ich przetwarzania
Dane uczniów	Nabór Optivum, Sekretariat Optivum
Dane organizacyjne	Arkusz Optivum
Dane pracowników	Kadry Optivum, Płace Optivum
Dane kasowe	Kasa Optivum

Opis struktury zbiorów danych osobowych wskazujących zawartość poszczególnych pól informacyjnych i powiązania między nimi

Zbiór danych „dane uczniów” zawiera następujące pola:

- nazwisko i imiona,
- numer PESEL,
- adres zamieszkania,
- data i miejsce urodzenia,
- imiona i nazwisko rodziców (prawnych opiekunów).

Zbiór danych „dane organizacyjne” zawiera następujące pola:

- nazwisko i imiona,
- numer PESEL,
- płeć,
- data urodzenia,
- staż pracy,
- pełniona funkcja,
- stopień awansu zawodowego,
- wynagrodzenie.

Zbiór danych „dane pracowników” zawiera następujące pola:

- nazwisko i imiona,
- imiona rodziców
- data i miejsce urodzenia
- numer PESEL,
- numer NIP,
- seria i numer dowodu osobistego,
- nazwisko rodowe,
- obywatelstwo,
- oddział NFZ,
- urząd skarbowy,
- adres stałego zameldowania
- adres zamieszkania
- adres korespondencyjny
- wykształcenie,
- staż pracy,
- ilość godzin,
- wynagrodzenie,
- stosunek do służby wojskowej.

Zbiór danych „dane kasowe” zawiera następujące pola:

- nazwisko i imiona lub nazwa firmy,
- adres zamieszkania lub siedziby firmy,
- numer NIP,
- numer REGON lub PESEL,
- dokument tożsamości, jego serię i numer.

Sposób przepływu danych pomiędzy poszczególnymi systemami

Program Nabór Optivum dostarcza dane kandydatów (i odbiera dane przyjętych uczniów) i przesyła je do programu Sekretariat Optivum. Ponadto Sekretariat Optivum przejmuje plany nauczania oddziałów z Arkusza Optivum.

Sekretariat Optivum, Kadry Optivum oraz Arkusz Optivum eksportuje dane do Integratora SIO-Optivum.

Program Kadry Optivum dostarcza dane płacowe do programu Płace Optivum.

Określenie środków technicznych i organizacyjnych niezbędnych do zapewnienia poufności, integralności i rozliczalności przetwarzanych danych

Poufność:

- upoważnienie do przetwarzania danych osobowych,
- rejestr osób upoważnionych do przetwarzania danych osobowych,
- identyfikator użytkownika i hasło dostępu,
- użytkownik musi obowiązek zablokowania stacji roboczej lub wylogowania się z systemu informatycznego służącego do przetwarzania danych osobowych w przypadku czasowego opuszczenia stanowiska pracy,
- zakończenie pracy w systemie służącym do przetwarzania danych osobowych poprzedzone jest zabezpieczeniem przed nieuprawnionym dostępem dodatkowych nośników danych, takich jak dyskietki, płyty CD i inne, zawierających dane osobowe,
- nośniki informatyczne zawierające dane osobowe lub kopie systemów informatycznych służących do przetwarzania danych osobowych są przechowywane w sposób uniemożliwiający ich utratę, uszkodzenie lub dostęp osób nieuprawnionych,
- przed ich likwidacją nośników informatycznych zawierających dane osobowe lub kopie zapasowe systemów informatycznych służących do przetwarzania danych osobowych dane osobowe zostają usunięte lub uszkodzone w sposób uniemożliwiający ich odczyt,
- po upływie okresu użyteczności lub przechowywania, dane osobowe zostają skasowane lub zniszczone tak, aby nie było możliwe ich odczytanie,
- zakaz wynoszenia poza pomieszczenia stanowiące obszar przetwarzania danych osobowych elektronicznych nośników informacji zawierających dane osobowe oraz kopie zapasowe,

- elektroniczne nośniki informacji zawierających dane osobowe oraz kopie zapasowe, a także wydruki i inne dokumenty zawierające dane osobowe przechowywane są w zamykanych szafach w pomieszczeniach stanowiących obszar przetwarzania danych osobowych, w sposób zabezpieczający je przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem i zniszczeniem,
- uszkodzony lub zużyty nośnik informacji zwierający dane osobowe zostaje fizycznie zniszczony tak, aby nie było możliwe odczytanie danych osobowych,
- dane osobowe przesyłane poprzez sieć Internet zabezpieczone są poprzez środki kryptograficznej ochrony,
- przeglądy i konserwacje sprzętu komputerowego oraz nośników informacji służących do przetwarzania danych osobowych, przeprowadzane są w pomieszczeniach stanowiących obszar przetwarzania danych osobowych,
- w przypadku przekazywania do naprawy sprzętu komputerowego z zainstalowanym systemem informatycznym służącym do przetwarzania danych osobowych lub nośnikiem informacji służących do przetwarzania danych osobowych, powinien on zostać pozbawiony danych osobowych przez fizyczne wymontowanie dysku lub skasowanie danych lub naprawa powinna zostać przeprowadzona w obecności administratora danych,
- ekrany komputerów umieszczone są w sposób uniemożliwiający obserwację przetwarzania danych przez osoby postronne,
- dokumenty papierowe i zewnętrze nośniki komputerowe, gdy nie są używane, a szczególnie poza godzinami pracy, przechowywane są w zamykanych szafach lub innego rodzaju zabezpieczanych meblach,
- fotokopiarki zostają zablokowane lub w inny sposób chronione przed nieuprawnionym użyciem poza normalnymi godzinami pracy,
- każdy dokument zawierający dane osobowe lub inne dane umożliwiające identyfikację osób, po ustaniu jego użyteczności przenosi się do archiwum lub o ile nie podlega archiwizacji – usuwa się w niszczarce do papieru,
- elektroniczne archiwa danych osobowych zgromadzone na płytach CD lub DVD są przechowywane w zabezpieczonym miejscu innej strefy pożarowej.

Integralność:
- upoważnienie do przetwarzania danych osobowych,
- użytkownik musi obowiązek zablokowania stacji roboczej lub wylogowania się z systemu informatycznego służącego do przetwarzania danych osobowych w przypadku czasowego opuszczenia stanowiska pracy,
- zakończenie pracy w systemie służącym do przetwarzania danych osobowych poprzedzone jest zabezpieczeniem przed nieuprawnionym dostępem dodatkowych nośników danych, takich jak dyskietki, płyty CD i inne, zawierających dane osobowe,
- uszkodzony lub zużyty nośnik informacji zwierający dane osobowe zostaje fizycznie zniszczony tak, aby nie było możliwe odczytanie danych osobowych,

- dane osobowe przesyłane poprzez sieć Internet zabezpieczone są poprzez środki kryptograficznej ochrony,
- w przypadku przekazywania do naprawy sprzętu komputerowego z zainstalowanym systemem informatycznym służącym do przetwarzania danych osobowych lub nośnikiem informacji służących do przetwarzania danych osobowych, powinien on zostać pozbawiony danych osobowych przez fizyczne wymontowanie dysku lub skasowanie danych lub naprawa powinna zostać przeprowadzona w obecności administratora danych.
- sieć komputerowa skanowana jest dynamicznie pod kątem występowania wirusów komputerowych,
- kluczowe systemy chronione są przez systemy podtrzymania napięcia UPS,
- niemożliwe jest zalogowanie się do systemu jako anonimowy użytkownik.

Rozliczalność:
- identyfikator użytkownika i hasło dostępu,
- zakaz przydzielania identyfikatora danego użytkownika innemu użytkownikowi, nawet po wyrejestrowaniu tego pierwszego z systemu informatycznego służącego do przetwarzania danych osobowych,
- zakaz wykonywania jakichkolwiek operacji w systemie informatycznym służącym do przetwarzania danych osobowych z wykorzystaniem identyfikatora i hasła dostępu innego użytkownika,
- w systemie informatycznym służącym do przetwarzania danych osobowych odnotowywane są informacje o odbiorcach danych, a w szczególności imię i nazwisko lub nazwa odbiorcy, data udostępnienia oraz zakres udostępnienia.