SZKOŁA PODSTAWOWA Nr 2
im. Ks. Jana Twardowskiego
ul. Boh. Monte Cassino 25
15-873 Białystok
tel. 85 742 03 04
Reg. 000735227, NIP 542-20-73-403

REGULAMIN PRACY W SIO

1. Dostęp do bazy danych SIO przez osoby upoważnione będzie następował po zalogowaniu do systemu teleinformatycznego. Użytkownik SIO jest więc obowiązany posiadać dane dostępowe, obejmujące identyfikator użytkownika SIO (login) i hasło, które otrzyma po spełnieniu warunków procedury przyznawania danych dostępowych.
2. Dane dostępowe przyznaje minister, kurator oświaty, wójt gminy (burmistrz, prezydent miasta), starosta powiatu i marszałek województwa lub osoby przez nich upoważnione. Udzielenie upoważnienia do przyznawania danych dostępowym wymaga **formy pisemnej** pod rygorem nieważności.
3. Osoba upoważniona może upoważnić do dostępu do bazy danych SIO pracownika lub pracowników jednostki, którą kierują. W tym przypadku upoważnienie wymaga również formy pisemnej pod rygorem nieważności, a dane dostępowe osobie upoważnionej przyznaje osoba udzielająca upoważnienia.
4. Dane dostępowe będą przyznawane na wniosek osoby upoważnionej składany w postaci elektronicznej. Wniosek składa się w postaci elektronicznej, za pomocą aplikacji internetowej SIO. Na adres poczty elektronicznej osoby, której mają być przyznane dane dostępowe jest przesyłana informacja o wpływie wniosku i o rozpoczęciu jego rozpatrywania. Organ przyznający dane dostępowe rozpatruje wniosek **w terminie 5 dni roboczych** od dnia wysłania informacji.
5. Przetwarzanie danych osobowych w SIO może odbywać się wyłącznie w ramach wykonywania zadań służbowych (zakres uprawnień wynika z zakresu tych zadań).
6. W celu zapobiegania nieautoryzowanemu dostępowi do informacji lub kradzieży informacji i środków jej przetwarzania stosuje się **politykę czystego biurka**. Ważne dokumenty (np. z wydruku SIO) i nośniki zawierające dane osobowe nie powinny pozostać niezabezpieczone w czasie nawet chwilowej nieobecności w pokoju. Pokój należy zamknąć w sposób uniemożliwiający dostęp dla osób nieuprawnionych. Po zakończeniu pracy ważne dokumenty komputerowe i nośniki z danymi osobowymi zawierające dane osobowe z systemu SIO powinny być przechowywane w szafach, a pokoje powinno się zamykać. Szczególną uwagę należy zwrócić na drukarki sieciowe i kserokopiarki dostępne dla większej liczby pracowników. Pracownicy powinni odbierać takie dokumenty natychmiast po wykonaniu przez urządzenie zleconego zadania. Nie powinny one pozostawać dostępne ani dla obcych osób ani dla pracowników nieposiadających stosownych uprawnień.
7. Administrator wprowadza **Polityka czystego ekranu, która** ma na celu zabezpieczenie przed nieautoryzowanym dostępem do systemu informatycznego i zabezpieczeniem przed ujawnieniem informacji chronionych w SIO. Każdorazowe odejście od stanowiska pracy powinno być poprzedzone wylogowaniem się lub zablokowaniem dostępu do systemu tak, aby niemożliwe było uzyskanie nieautoryzowanego dostępu do systemu. W tym celu każdy komputer ma

wprowadzony system automatycznego uruchamiania się wygaszania ekranu i wylogowania użytkownika. Po zakończeniu pracy należy zamknąć aktywne aplikacje oraz wyrejestrować się (wylogować się) z systemu lub też zablokować dostęp do systemu.

8. Mając świadomość, że żadne zabezpieczenie techniczne nie gwarantuje stuprocentowego bezpieczeństwa danych, konieczne jest, aby każdy użytkownik mający styczność z przetwarzanymi danymi, świadom odpowiedzialności, postępował zgodnie z przyjętymi w dokumencie „Polityka Ochrony Danych: zasadami i minimalizował zagrożenie wynikające z błędów ludzkich. Ochrona danych osobowych w systemie SIO obowiązuje wszystkie osoby, które mają dostęp do informacji zbieranych, przetwarzanych oraz przechowywanych, bez względu na zajmowane stanowisko oraz miejsce wykonywania jak również charakter stosunku pracy. Osoby mające dostęp do danych osobowych są zobligowane do stosowania niezbędnych środków zapobiegających ujawnieniu tych danych osobom nieupoważnionym. Dlatego też zastosowano następujące rozwiązania:

   a) dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe w SIO zabezpieczony jest za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora (login) użytkownika oraz hasła

   b) Zastosowano środki ochrony przed szkodliwym oprogramowaniem takim, jak np. robaki, wirusy, konie trojańskie, rootkity

   c) Użyto system Firewall do ochrony dostępu do sieci komputerowej

   d) Zainstalowano wygaszacze ekranów na stanowiskach, na których przetwarzane są dane osobowe

   e) Zastosowano mechanizm automatycznej blokady dostępu do systemu informatycznego służącego do przetwarzania danych osobowych w przypadku dłuższej nieaktywności pracy użytkownika.

   Szczegółowe środki ochrony technicznej systemu informatycznego, jak również wszystkie niezbędne informacje dotyczące jego pracy oraz zasad użytkowania zawarte są w dokumencie Polityka Ochrony Danych w punkcie 15.

Zapoznałam/em się z treścią Regulaminu pracy w SIO i zobowiązuje się do przestrzegania zasad w nim zawartych.

.....

czytelny podpis użytkownika

Rozporządzenie Ministra Edukacji Narodowej w sprawie procedury przyznawania danych dostępowych do bazy danych systemu informacji oświatowej

Dyrektor
Szkoły Podstawowej Nr 2
im. ks. Jana Twardowskiego
w Białymstoku
mgr Halina Puchalska