ZESPÓŁ OBSŁUGI OŚWIATY
I REKREACJI
89-100 Nakło n. Not,
ul. Krzywoustego 7A, skr. p. 55
tel. 52 519 01 59, fax 52 519 01 54
NIP 558-16-04-646, Reg: 092499195

**ZARZĄDZENIE nr ZOOR.IK-0110-5/2013**
**Dyrektora Zespołu Obsługi Oświaty i Rekreacji w Nakle nad Notecią**
z dnia 15.11.2013 r.

**w sprawie**: wprowadzenia Polityki Bezpieczeństwa Informacji i wyznaczenia Administratora Bezpieczeństwa Informacji (ABI)

Na podstawie przepisów:

1. Ustawy z dnia 23 kwietnia 1964r. Kodeks Cywilny (Dz. U. Nr 16 poz. 93 z późniejszymi zmianami)
2. Ustawy z dnia 06 czerwiec 1997r. Kodeks Karny (Dz. U. Nr 88 poz. 553))
3. Ustawa z 26 czerwca 1974r. Kodeks Pracy Ujednolicony tekst ustawy (Dz. U. z 1988r Nr 21 poz. 94)
4. Ustawy z dnia 29 sierpnia 1997r. o ochronie danych osobowych (Dz. U. Nr 133 poz 883)
5. Rozporządzenia Ministra Sprwa Wewnętrznych i Administracji z dnia 29 kwietnia 2004r w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100 poz. 1024)

**Zarządzam co następuje:**

**§1**

Wprowadzam do użytkowania i przestrzegania przez wszystkich pracowników Zespołu Obsługi Oświaty i Rekreacji w Nakle nad Notecią dokumentację określająca Politykę Bezpieczeństwa w zakresie odnoszącym się do sposobu przetwarzania danych osobowych oraz środków ich ochrony:

1. Polityka Bezpieczeństwa Informacji – Zasady ogólne
2. Instrukcja zarządzania systemem informatycznym Ochrony Danych Osobowych

**§2**

Z dniem 15.11.2013 r. powołuje się:

**1. Administratora Bezpieczeństwa Informacji (ABI)**:

- **Arnold Paszta**

1) Administrator Bezpieczeństwa Informacji ma obowiązek:

a) Opracowania Polityki Bezpieczeństwa Informacji oraz Instrukcji przetwarzania danych osobowych w systemach informatycznych
b) nadzorowania przestrzegania zasad zabezpieczenia technicznego i organizacyjnego zapewniających ochronę przetwarzanych danych osobowych,

c) kontrolowania pracowników i innych osób upoważnionych pod względem wykonywania przez nich obowiązków związanych z ochroną przetwarzanych danych osobowych,
d) wykonywania kontroli pod względem skuteczności zastosowanych środków organizacyjnych i fizycznych mających na celu zachowanie poufności oraz integralności danych osobowych,
e) wykonywania kontroli w zakresie przechowywania i archiwizacji dokumentów papierowych zawierających dane osobowe, pod względem prawidłowego zabezpieczenia tych dokumentów,
f) prowadzenia ewidencji osób upoważnionych do przetwarzania danych osobowych.
g) podejmowania działań w przypadku naruszeń ochrony danych osobowych, w tym przywrócenie stanu prawidłowego, zidentyfikowanie przyczyn naruszenia i osób odpowiedzialnych, przedstawienie wniosków Dyrektorowi ZOOR:
h) inicjowania i podejmowanie przedsięwzięć w zakresie doskonalenia bezpieczeństwa ochrony danych osobowych,
i) nadzorowanie rejestracji zbiorów Danych osobowych

2) W przypadku stwierdzenia nieprawidłowości w zakresie zabezpieczenia danych osobowych Administrator Bezpieczeństwa Informacji ma obowiązek:

a) pouczać i instruować osoby, które dopuściły się uchybień, a także raportować o błędach do Dyrektora ZOOR mając na celu przywrócenie stanu prawidłowego,
b) zwracać się do Dyrektora ZOOR o dokonanie zmian w zakresie stosowanych zabezpieczeń organizacyjnych i technicznych,
c) przedstawiać Dyrektorowi ZOOR raporty dotyczące stanu zabezpieczenia danych osobowych, w tym propozycję poprawiające bezpieczeństwo danych oraz wnioski dotyczące odpowiedzialności osób winnych uchybień,

**2. Administratora Systemu Informatycznego (ASI):**

**- Jacek Zawodniak**

1) Administrator Systemu Informatycznego ma obowiązek:

a) zarządza systemem informatycznym, w którym przetwarzane są dane osobowe, posługując się hasłem dostępu do wszystkich stacji roboczych z pozycji administratora,
b) przeciwdziała dostępowi osób niepowołanych do systemu informatycznego, w którym przetwarzane są dane osobowe,
c) na wniosek ABI/ AD przydziela każdemu użytkownikowi identyfikator oraz hasło do systemu informatycznego oraz dokonuje ewentualnych modyfikacji uprawnień, a także usuwa konta użytkowników zgodnie z zasadami określonymi w instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych,
d) nadzoruje działanie mechanizmów uwierzytelniania użytkowników oraz kontroli dostępu do danych osobowych,
e) podejmuje działania w zakresie ustalania i kontroli identyfikatorów dostępu do systemu informatycznego,
f) wyrejestrowuje użytkowników na polecenie Administratora Danych lub Administratora Bezpieczeństwa Informacji
g) zmienia w poszczególnych stacjach roboczych hasła dostępu, ujawniając je wyłącznie danemu użytkownikowi oraz, w razie potrzeby, administratorowi bezpieczeństwa informacji lub administratorowi danych,
h) w sytuacji stwierdzenia naruszenia zabezpieczeń systemu informatycznego informuje ABI o naruszeniu i współdziała z nim przy usuwaniu skutków naruszenia,
i) prowadzi szczegółową dokumentację naruszeń bezpieczeństwa danych osobowych

przetwarzanych w systemie informatycznym,

j) sprawuje nadzór nad wykonywaniem napraw, konserwacją oraz likwidacją urządzeń komputerowych, na których zapisane są dane osobowe, nad wykonywaniem kopii zapasowych, ich przechowywaniem oraz okresowym sprawdzaniem pod kątem ich dalszej przydatności do odtwarzania danych w przypadku awarii systemu informatycznego,

k) podejmuje działania służące zapewnieniu niezawodności zasilania komputerów, innych urządzeń mających wpływ na bezpieczeństwo przetwarzania danych oraz zapewnieniu bezpiecznej wymiany danych w sieci wewnętrznej i bezpiecznej teletransmisji.

**§3**

Traci moc zarządzenie Dyrektora ZOOR w Nakle nad Notecią nr 8/2010 z dnia 27.12.2010 r. w sprawie wprowadzenia polityki bezpieczeństwa informacji oraz instrukcji zarządzania systemami informatycznymi.

**§4**

Zarządzenie wchodzi w życie z dniem podpisania.

DYREKTOR
mgr Zbigniew Boczan