I. POLITYKA BEZPIECZEŃSTWA OCHRONY DANYCH OSOBOWYCH.

1. Wstęp.

Celem Polityki Bezpieczeństwa jest zapewnienie ochrony DANYCH OSOBOWYCH przetwarzanych przez Bibliotekę Publiczną w Nekli przed wszelakiego rodzaju zagrożeniami, tak wewnętrznymi jak i zewnętrznymi, świadomymi lub nieświadomymi.

Polityka została opracowana zgodnie z wymogami określonymi w § 4 rozporządzenia Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. 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).

Do niniejszej polityki opracowano i wdrożono Instrukcję zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, zwaną dalej „Instrukcją zarządzania systemem informatycznym ODO". Określa ona sposób zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych, ze szczególnym uwzględnieniem zapewnienia ich bezpieczeństwa.

Ochrona danych osobowych jest realizowana poprzez: zabezpieczenia fizyczne, procedury organizacyjne, oprogramowanie systemowe, aplikacje oraz przez użytkowników.

Zastosowane zabezpieczenia mają służyć osiągnięciu powyższych celów i zapewnić:

1. poufność danych - rozumianą jako właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym osobom,
2. integralność danych - rozumianą jako właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany,
3. rozliczalność danych - rozumianą jako właściwość zapewniającą, że działania osoby mogą być przypisane w sposób jednoznaczny tylko tej osobie,
4. integralność systemu rozumianą jako nienaruszalność systemu, niemożność jakiejkolwiek manipulacji, zarówno zamierzonej, jak i przypadkowej.

Niniejszy dokument jest zgodny z następującymi aktami prawnymi:

1. ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity: Dz. U. 2014 r., poz. 1182),
2. oraz aktów wykonawczych wydanych na podstawie ww. ustaw.

2. Definicje.

Przez użyte w Polityce określenia należy rozumieć:

1. Polityka – rozumie się przez to Politykę bezpieczeństwa ochrony danych osobowych w Bibliotece Publicznej Miasta i Gminy Nekla
2. Administrator Danych Osobowych – Magdalena Bielak, decydująca o celach i środkach przetwarzania danych osobowych;
3. Administrator Bezpieczeństwa Informacji (ABI) – Tomasz Powała, wyznaczony przez Dyrektora, odpowiedzialny za organizację ochrony danych osobowych.
4. Ustawa – rozumie się przez to ustawę z dnia 29.sierpnia.1997 r. o ochronie danych osobowych (tekst jednolity: Dz.U. z 20014 r. ,poz.1182)
5. Rozporządzenie – rozumie się przez to rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 3 czerwca 1998 r. w sprawie określenia podstawowych warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz.U. z 1998 r. Nr 80, poz. 521)
6. Dane osobowe (dane) - wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej;
7. Zbiór danych – zestaw danych osobowych posiadający określoną strukturę, prowadzony w/g określonych kryteriów oraz celów;
8. Usuwanie danych – rozumie się przez to zniszczenie danych osobowych lub taką ich modyfikację , która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą,
9. Zgoda osoby, której dane dotyczą – rozumie się przez to oświadczenie woli, którego treścią jest zgoda na przetwarzanie danych osobowych tego, kto składa oświadczenie; zgoda nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści,
10. Baza danych osobowych - zbiór uporządkowanych powiązanych ze sobą tematycznie danych zapisanych np. w pamięci zewnętrznej komputera. Baza danych jest złożona z elementów o określonej strukturze - rekordów lub obiektów, w których są zapisane dane osobowe;
11. Przetwarzanie danych - wykonywanie jakichkolwiek operacji na danych osobowych, np. zbieranie, utrwalanie, opracowywanie, udostępnianie, zmienianie, usuwanie;
12. System informatyczny (system) – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;
13. Administrator systemu - osoba nadzorująca pracę systemu informatycznego oraz wykonująca w nim czynności wymagające specjalnych uprawnień;
14. Użytkownik - pracownik Biblioteki posiadający uprawnienia do pracy w systemie informatycznym zgodnie z zakresem obowiązków służbowych;
15. Zabezpieczenie systemu informatycznego – należy przez to rozumieć wdrożenie stosownych środków administracyjnych, technicznych i fizycznych w celu zabezpieczenia zasobów technicznych oraz ochrony przed modyfikacją, zniszczeniem, nieuprawnionym dostępem i ujawnieniem lub pozyskaniem danych osobowych, a także ich utratą,

16. Nośnik komputerowy (wymienny) – nośnik służący do zapisu i przechowywania informacji, np. taśmy, dyskietki, dyski twarde;

3. Zadania ABI.

Do najważniejszych obowiązków Administratora Bezpieczeństwa Informacji należy:

1. organizacja bezpieczeństwa i ochrony danych osobowych zgodnie z wymogami ustawy o ochronie danych osobowych,
2. zapewnienie przetwarzania danych zgodnie z uregulowaniami niniejszej polityki
3. wydawanie i anulowanie upoważnień do obsługi systemu informatycznego oraz urządzeń wchodzących w jego skład dla osób przetwarzających dane osobowe,
4. prowadzenie „Rejestru osób zatrudnionych przy przetwarzaniu danych osobowych"
5. prowadzenie postępowania wyjaśniającego w przypadku naruszenia ochrony danych osobowych,
6. nadzór nad bezpieczeństwem danych osobowych,
7. kontrola działań komórek organizacyjnych pod względem zgodności przetwarzania danych z przepisami o ochronie danych osobowych,
8. inicjowanie i podejmowanie przedsięwzięć w zakresie doskonalenia ochrony danych osobowych

Administrator Bezpieczeństwa Informacji ma prawo:

1. wstępu do pomieszczeń w których zlokalizowane są zbiory danych i przeprowadzenia niezbędnych badań lub innych czynności kontrolnych w celu oceny zgodności przetwarzania danych z ustawą,
2. żądać złożenia pisemnych lub ustnych wyjaśnień w zakresie niezbędnym do ustalenia stanu faktycznego,
3. żądać okazania dokumentów i wszelkich danych mających bezpośredni związek z problematyką kontroli,
4. żądać udostępnienia do kontroli urządzeń, nośników oraz systemów informatycznych służących do przetwarzania danych,

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

Budynek Biblioteki mieści się przy ulicy Chopina 43/3 w Nekli, oraz w Zespole Szkół w Targowej Górce gdzie mieści się filia Biblioteki. Dane przetwarzane są na parterze I piętrze. Wszystkie te pomieszczenia zabezpieczone są zamkami, a same szafy wyposażone są w zamki.

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

Wykaz zbiorów danych osobowych opisany jest w Załączniku 1 „Wykaz zbiorów danych osobowych".

6. Środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych.

A) Zabezpieczenia organizacyjne:

1. Został wyznaczony administrator bezpieczeństwa informacji nadzorujący przestrzeganie zasad ochrony przetwarzanych danych osobowych
2. została opracowana i wdrożona polityka bezpieczeństwa
3. została opracowana i wdrożona instrukcja zarządzania systemem informatycznym
4. do przetwarzania danych zostały dopuszczone wyłącznie osoby posiadające upoważnienia nadane przez administratora danych
5. prowadzona jest ewidencja osób upoważnionych do przetwarzania danych
6. osoby zatrudnione przy przetwarzaniu danych zostały zaznajomione z przepisami dotyczącymi ochrony danych osobowych oraz w zakresie zabezpieczeń systemu informatycznego
7. osoby zatrudnione przy przetwarzaniu danych osobowych obowiązane zostały do zachowania ich w tajemnicy
8. przetwarzanie danych osobowych dokonywane jest w warunkach zabezpieczających dane przed dostępem osób nieupoważnionych
9. przebywanie osób nieuprawnionych w pomieszczeniach, gdzie przetwarzane są dane osobowe jest dopuszczalne tylko w obecności osoby zatrudnionej przy przetwarzaniu danych osobowych oraz w warunkach zapewniających bezpieczeństwo danych
10. stosuje się pisemne umowy powierzenia przetwarzania danych dla współpracy z podwykonawcami przetwarzającymi dane osobowe, których administratorem danych jest Dyrektor.

B) Zabezpieczenia ochrony fizycznej danych osobowych

Dokumenty przechowywane są w szafkach wyposażonych w zamki.

C) Zabezpieczenia sprzętowe infrastruktury informatycznej i telekomunikacyjnej
Zabezpieczenia stosuje się dla fizycznych elementów systemu, ich połączeń oraz systemów operacyjnych. Szczegółowy opis zabezpieczeń zawarty jest w instrukcji zarządzania systemem informatycznym.

D) Zabezpieczenia narzędzi programowych i baz danych
Zabezpieczenia (techniczne i programowe) stosuje się dla procedur, aplikacji, programów i innych narzędzi programowych przetwarzających dane osobowe. Szczegółowy opis zabezpieczeń zawarty jest w instrukcji zarządzania systemem informatycznym.

7. Instrukcja alarmowa.

Instrukcja definiuje katalog zagrożeń i incydentów zagrażających bezpieczeństwu danych osobowych oraz opisuje sposób reagowania na nie. Celem instrukcji jest minimalizacja skutków wystąpienia incydentów bezpieczeństwa, ograniczenie ryzyka powstania zagrożeń i występowania incydentów w przyszłości.

1. Każdy pracownik Biblioteki w przypadku stwierdzenia zagrożenia lub naruszenia ochrony danych osobowych, zobowiązany jest poinformować bezpośredniego przełożonego lub Administratora Bezpieczeństwa Informacji.
2. Do typowych zagrożeń bezpieczeństwa danych osobowych należą:
    a. niewłaściwe zabezpieczenie fizyczne pomieszczeń, urządzeń i dokumentów
    b. niewłaściwe zabezpieczenie sprzętu IT, oprogramowania przed wyciekiem, kradzieżą i utratą danych osobowych
    c. nieprzestrzeganie zasad ochrony danych osobowych przez pracowników (np. niestosowanie zasady czystego biurka / ekranu, ochrony haseł, niezamykanie pomieszczeń, szaf, biurek)
3. Do typowych incydentów bezpieczeństwa danych osobowych należą:
    a. zdarzenia losowe zewnętrzne (pożar obiektu/pomieszczenia, zalanie wodą, utrata zasilania, utrata łączności)
    b. zdarzenia losowe wewnętrzne (awarie serwera, komputerów, twardych dysków, oprogramowania, pomyłki informatyków, użytkowników, utrata / zagubienie danych)
    c. umyślne incydenty (włamanie do systemu informatycznego lub pomieszczeń, kradzież danych/sprzętu, wyciek informacji, ujawnienie danych osobom nieupoważnionym, świadome zniszczenie dokumentów/danych, działanie wirusów i innego szkodliwego oprogramowania)
4. W przypadku stwierdzenia wystąpienia zagrożenia, Administrator Bezpieczeństwa Informacji prowadzi postępowanie wyjaśniające w toku, którego:
    a. ustala zakres i przyczyny zagrożenia oraz jego ewentualne skutki
    b. inicjuje ewentualne działania dyscyplinarne
    c. rekomenduje działania prewencyjne (zapobiegawcze) zmierzające do eliminacji podobnych zagrożeń w przyszłości
    d. dokumentuje prowadzone postępowania

5. W przypadku stwierdzenia incydentu (naruszenia), Administrator Bezpieczeństwa Informacji prowadzi postępowanie wyjaśniające w toku, którego:
    a. ustala czas wystąpienia naruszenia, jego zakres, przyczyny, skutki oraz wielkość szkód, które zaistniały
    b. zabezpiecza ewentualne dowody
    c. ustala osoby odpowiedzialne za naruszenie
    d. podejmuje działania naprawcze (usuwa skutki incydentu i ogranicza szkody)
    e. inicjuje działania dyscyplinarne
    f. wyciąga wnioski i rekomenduje działania korygujące zmierzające do eliminacji podobnych incydentów w przyszłości
    g. dokumentuje prowadzone postępowania

8. Procedura działań korygujących i zapobiegawczych.

1. Celem procedury jest uporządkowanie i przedstawienie czynności związanych z inicjowaniem oraz realizacją działań korygujących i zapobiegawczych wynikających z zaistnienia incydentów bezpieczeństwa lub zagrożeń systemu ochrony danych osobowych.
2. Procedura działań korygujących i zapobiegawczych obejmuje wszystkie te procesy, w których incydenty bezpieczeństwa lub zagrożenia mogą wpłynąć na zgodność z wymaganiami stawy o Ochronie Danych Osobowych, jak również na poprawne funkcjonowanie systemu ochrony danych osobowych.
3. Osobą odpowiedzialną za nadzór nad procedurą jest Administrator Bezpieczeństwa Informacji.

Definicje

1. Incydent - naruszenie bezpieczeństwa informacji ze względu na poufność, dostępność i integralność.
2. Zagrożenie – potencjalna możliwość wystąpienia incydentu
3. Korekcja – działanie w celu wyeliminowania skutków incydentu.
4. Działanie korygujące – jest to działanie przeprowadzane w celu wyeliminowania przyczyny incydentu lub innej niepożądanej sytuacji.
5. Działanie zapobiegawcze – jest to działanie, które należy przedsięwziąć, aby wyeliminować przyczyny zagrożenia lub innej potencjalnej sytuacji niepożądanej.
6. Kontrola – systematyczna, niezależna i udokumentowana ocena skuteczności systemu ochrony danych osobowych, na podstawie wymagań ustawowych, polityki i instrukcji.

Opis czynności

1. ABI jest odpowiedzialny za analizę incydentów bezpieczeństwa lub zagrożeń ochrony danych osobowych. Typowymi źródłami informacji o incydentach, zagrożeniach lub słabościach są:
   - zgłoszenia od pracowników
   - wiedza ABI
   - wyniki kontroli
2. W przypadku, gdy ABI stwierdzi konieczność podjęcia działań korygujących lub zapobiegawczych, określa: źródło powstania incydentu lub zagrożenia, zakres działań korygujących lub zapobiegawczych, termin realizacji, osobę odpowiedzialną
3. ABI jest odpowiedzialny za nadzór nad poprawnością i terminowością wdrażanych działań korygujących lub zapobiegawczych.
4. Po przeprowadzeniu działań korygujących lub zapobiegawczych, ABI jest zobowiązany do oceny efektywności ich zastosowania.

9. Kontrola systemu ochrony danych osobowych.

1. Celem procedury jest uporządkowanie i przedstawienie czynności związanych zkontrolą stanu bezpieczeństwa danych osobowych
2. Procedura obejmuje wszystkie procesy, gdzie przestrzeganie zasad ochrony danych osobowych jest wymagane.
3. Do kontroli stanu ochrony danych osobowych upoważniony jest ABI, wyznaczeni kontrolerzy wewnętrzni, najwyższe kierownictwo
4. Kontroli podlegają: systemy informatyczne przetwarzające dane osobowe, zabezpieczenia fizyczne, zabezpieczenia organizacyjne, bezpieczeństwo osobowe oraz zgodność stanu faktycznego z wymaganiami U.O.D.O.
5. Administrator Bezpieczeństwa Informacji przygotowuje plan kontroli uwzględniając zakres oraz potrzebne zasoby fizyczne, czasowe i osobowe. Kontrola powinna odbyć się co najmniej raz w roku.
6. Kontrola przeprowadzana jest na podstawie listy kontrolnej
7. Po dokonanej kontroli osoba ją przeprowadzająca przygotowuje i przekazuje raport pokontrolny kierownikowi kontrolowanej jednostki lub komórki organizacyjnej oraz Administratorowi Danych Osobowych.
   Na jego podstawie ABI inicjuje działania korygujące lub zapobiegawcze.

10. Sprawozdanie roczne stanu systemu ochrony danych osobowych.

1. Raz w roku Administrator Bezpieczeństwa Informacji przygotowuje sprawozdanie roczne stanu funkcjonowania systemu ochrony danych osobowych
2. W spotkaniu sprawozdawczym uczestniczą: ABI, Kierownicy działów, w których przetwarzane są dane osobowe, Informatyk.
3. Raport przygotowany jest według Sprawozdania ODO,a następnie przedstawiany jest najwyższemu kierownictwu.

11. Szkolenia użytkowników.

1. Każdy użytkownik przed dopuszczeniem do pracy z systemem informatycznym przetwarzającym dane osobowe winien być poddany przeszkoleniu w zakresie ochrony danych osobowych w zbiorach elektronicznych i papierowych.
2. Za przeprowadzenie szkolenia odpowiada ABI a za jego zorganizowanie odpowiada przełożony użytkowników.
3. Zakres szkolenia powinien obejmować zaznajomienie użytkownika z przepisami ustawy o ochronie danych osobowych oraz wydanymi na jej podstawie aktami wykonawczymi oraz instrukcjami obowiązującymi u Administratora Danych, a także o zobowiązaniu się do ich przestrzegania.
4. Szkolenie zostaje zakończone podpisaniem przez słuchacza Oświadczenia o wzięciu udziału w szkoleniu i jego zrozumieniu oraz zobowiązaniu się do przestrzegania przedstawionych w trakcie szkolenia zasad ochrony danych osobowych
5. Dokument ten (patrz **Załącznik 2 – Oświadczenie użytkownika**) jest przechowywany jest w aktach osobowych użytkowników i stanowi podstawę do podejmowania działań w celu nadania im uprawnień do korzystania z systemu informatycznego przetwarzającego dane osobowe.

12. Postanowienia końcowe.

1. „Polityka Bezpieczeństwa" jest dokumentem wewnętrznym i nie może być udostępniania osobom postronnym w żadnej formie.
2. Kierownicy komórek organizacyjnych są obowiązani zapoznać z treścią „Polityki bezpieczeństwa" każdego użytkownika.
3. Wszystkie regulacje dotyczące systemów informatycznych określone w Polityce Bezpieczeństwa dotyczą również przetwarzania danych osobowych w bazach prowadzonych w jakiejkolwiek innej formie.
4. Użytkownicy zobowiązani są do stosowania przy przetwarzaniu danych osobowych postanowień zawartych w niniejszej „Polityce".
5. Przypadki, nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu potraktowane będą jako ciężkie naruszenie obowiązków pracowniczych.

6. Wobec osoby, która w przypadku naruszenia zabezpieczeń systemu informatycznego lub uzasadnionego domniemania takiego naruszenia nie podjęła działania określonego w niniejszym dokumencie, a w szczególności nie powiadomiła odpowiedniej osoby zgodnie z określonymi zasadami, a także, gdy nie zrealizowała stosownego działania dokumentującego ten przypadek, można wszcząć postępowanie dyscyplinarne.
7. Kara dyscyplinarna, orzeczona wobec osoby uchylającej się od powiadomienia nie wyklucza odpowiedzialności karnej tej osoby zgodnie z ustawą z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (tekst jednolity Dz. U. z 2014 r., poz 1182) oraz możliwości wniesienia wobec niej sprawy z powództwa cywilnego przez pracodawcę o zrekompensowanie poniesionych strat.
8. W sprawach nieuregulowanych w niniejszej „Polityce bezpieczeństwa" mają zastosowanie przepisy ustawy z dnia 29 sierpnia 1997 r., o ochronie danych osobowych (tekst jednolity Dz. U. z 2014 r., poz 1182) oraz wydanych na jej podstawie aktów wykonawczych.