POLITYKA BEZPIECZEŃSTWA SYSTEMÓW INFORMATYCZNYCH SŁUŻĄCYCH DO PRZETWARZANIA DANYCH OSOBOWYCH W GMINNEJ BIBLIOTECE PUBLICZNEJ W BUKOWCU

ROZDZIAŁ 1

PODSTAWA PRAWNA

§ 1

Potrzeba opracowania dokumentu wynika z § 4 rozporządzenia Prezesa Rady Ministrów z dnia 25 sierpnia 2005 roku w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego (Dz. U. Nr 171 poz. 1433) oraz § 3 i § 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).

POSTANOWIENIA OGÓLNE

§ 2

Dokument opisuje reguły dotyczące bezpieczeństwa danych osobowych zawartych w systemach informatycznych w Gminnej Bibliotece Publicznej w Bukowcu. Opisane zasady określają granice dopuszczalnego zachowania wszystkich użytkowników systemów informatycznych stosowanych w Gminnej Bibliotece Publicznej w Bukowcu. Dokument zwraca uwagę na konsekwencje, jakie mogą ponieść osoby przekraczające określone granice oraz procedury postępowania w celu zapobiegania i minimalizowania skutków zagrożeń. Odpowiednie zabezpieczenia i ochrona przetwarzanych danych oraz niezawodność funkcjonowania systemów są podstawowymi wymogami stawianymi współczesnym systemom informatycznym.

§ 3

Dokument „Polityka bezpieczeństwa systemów informatycznych służących do przetwarzania danych osobowych w Gminnej Bibliotece Publicznej w Bukowcu”, zwany dalej „Polityką bezpieczeństwa”, wskazuje sposób postępowania w sytuacji naruszenia bezpieczeństwa danych osobowych w systemach informatycznych, przeznaczony jest dla osób zatrudnionych przy przetwarzaniu tych danych.

1. Polityka bezpieczeństwa określa tryb postępowania w przypadku, gdy:
1) stwierdzono naruszenie zabezpieczenia systemu informatycznego,
2) stan urządzeń, zawartość zbiorów danych osobowych, ujawnione metody pracy, sposób działania programu lub jakość komunikacji w sieci Gminnej Bibliotece Publicznej w Bukowcu mogą wskazywać na naruszenie zabezpieczeń tych danych.

2. Polityka bezpieczeństwa obowiązuje wszystkich pracowników Biblioteki.

3. Wykonywanie postanowień tego dokumentu ma zapewnić właściwą reakcję, ocenę i udokumentowanie przypadków naruszenia bezpieczeństwa systemów oraz zapewnić właściwy tryb działania w celu przywrócenia bezpieczeństwa danych przetwarzanych w systemach informatycznych.

4. Administratorem Bezpieczeństwa Informacji jest Kierownik Gminnej Bibliotece Publicznej w Bukowcu, zwany dalej ABI. Jego obowiązki określa Załącznik Nr 1.

5. ABI realizuje zadania w zakresie ochrony danych, a w szczególności:

1) ochrony i bezpieczeństwa danych osobowych zawartych w zbiorach systemów informatycznych Biblioteki,
2) podejmowania stosownych działań zgodnie z niniejszą „Polityką bezpieczeństwa" w przypadku wykrycia nieuprawnionego dostępu do baz danych lub naruszenia zabezpieczenia danych znajdujących się w systemie informatycznym,
3) nadzoru i kontroli systemów informatycznych służących do przetwarzania danych osobowych i osób przy nim zatrudnionych.

6. Niniejszy dokument jest zgodny z następującymi aktami prawnymi:

1) ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity Dz. U. Nr 101, poz. 926 z późn. zm.),
2) rozporządzeniem 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. z 2004 r. Nr 100, poz.1024),
3) ustawą z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2005r. Nr 64, poz. 565) 4) ustawą o ochronie informacji niejawnych z dnia 22 stycznia 1999 r. (Dz. U. NR 11, poz. 95 z późn. zm.),
5) rozporządzeniem Prezesa Rady Ministrów z dnia 25 sierpnia 2005r. w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego (Dz. U. Nr 177 poz. 1433).

ROZDZIAŁ 2

OPIS ZDARZEŃ NARUSZAJĄCYCH OCHRONĘ DANYCH OSOBOWYCH

§ 4

1. Podział zagrożeń:
1) zagrożenia losowe zewnętrzne (np. klęski żywiołowe, zalania, ogień, przerwy w zasilaniu w energię elektryczną, zwarcia i przepięcia w sieci elektroenergetycznej). Ich występowanie może prowadzić do utraty integralności danych, ich uszkodzenia, zniszczenia, uszkodzenia systemów komputerowych oraz elementów technicznych komputera lub sieci. Ciągłość systemu zostaje zakłócona, jednak nie dochodzi do naruszenia poufności danych,
2) zagrożenia losowe wewnętrzne (np. niezamierzone pomyłki użytkowników, administratora, awarie sprzętowe, błędy oprogramowania, działanie wirusów). Może dojść do zniszczenia danych, zakłócenia ciągłości pracy systemu lub naruszenia poufności danych,
3) zagrożenia zamierzone, świadome i celowe - najpoważniejsze zagrożenia, naruszenia poufności danych (zazwyczaj nie następuje uszkodzenie infrastruktury technicznej i zakłócenie ciągłości pracy). Zagrożenia te możemy podzielić na: nieuprawniony dostęp do systemu z zewnątrz (włamanie do systemu), nieuprawniony dostęp do systemu z jego wnętrza, nieuprawniony przekaz danych, pogorszenie jakości sprzętu i oprogramowania, bezpośrednie zagrożenie składników technicznych systemu.
2. Przypadki zakwalifikowane jako naruszenie lub uzasadnione podejrzenie naruszenia zabezpieczenia systemów informatycznych, w których przetwarzane są dane osobowe to:
1) sytuacje losowe lub nieprzewidziane oddziaływanie czynników zewnętrznych na zasoby systemu jak np.: pożar, zalanie pomieszczeń, katastrofa budowlana, napad, działania terrorystyczne, niepożądana ingerencja ekipy remontowej itp.,
2) niewłaściwe parametry środowiska, jak np. nadmierna wilgotność lub wysoka temperatura, oddziaływanie pola elektromagnetycznego,
3) awaria sprzętu lub oprogramowania, które wyraźnie wskazują na umyślne działanie w kierunku naruszenia ochrony danych lub wręcz sabotaż, a także niewłaściwe działanie serwisu, a w tym sam fakt pozostawienia serwisantów bez nadzoru,
4) pojawienie się odpowiedniego komunikatu alarmowego od tej części systemu, która zapewnia ochronę zasobów lub inny komunikat o podobnym znaczeniu,
5) jakość danych w systemie lub inne odstępstwo od stanu oczekiwanego wskazujące na zakłócenia systemu lub inną nadzwyczajną i niepożądaną modyfikację w systemie,
6) naruszenie lub próba naruszenia integralności systemu lub bazy danych w tym systemie,
7) stwierdzenie próby modyfikacji danych lub zmianę w strukturze danych bez odpowiedniego upoważnienia (autoryzacji),
8) niedopuszczalna manipulacja danymi osobowymi w systemie,
9) ujawnienie osobom nieupoważnionym danych osobowych, objętych tajemnicą procedur ochrony przetwarzania lub innych strzeżonych elementów zabezpieczeń systemu,
10) praca w systemie lub jego sieci komputerowej wykazuje nieprzypadkowe odstępstwa od założonego rytmu pracy, co świadczy o przełamaniu lub zaniechaniu ochrony danych osobowych, np. praca przy komputerze lub w sieci osoby, która nie jest formalnie dopuszczona do jego obsługi, sygnał o uporczywym nieautoryzowanym logowaniu do sieci lub komputera, itp.,
11) ujawnienie istnienia nieautoryzowanych kont dostępu do danych lub tzw. "luk w systemie", itp.,
12) podmienienie lub zniszczenie nośników z danymi osobowymi bez odpowiedniego upoważnienia oraz skasowanie lub skopiowanie w sposób niedozwolony danych osobowych,

13) rażące naruszenie dyscypliny pracy w zakresie przestrzegania procedur bezpieczeństwa informacji (nie wylogowanie z programu, systemu przed opuszczeniem stanowiska pracy, pozostawienie danych osobowych w drukarce, na ksero, nie zamknięcie pomieszczenia z komputerem, prace na danych osobowych w celach prywatnych, itp.).
3. Za naruszenie ochrony danych uważa się również stwierdzone nieprawidłowości w zakresie zabezpieczenia miejsc przechowywania danych osobowych (otwarte szafy, biurka, regały, urządzenia archiwalne i inne) na nośnikach tradycyjnych tj. papier (wydruki), dyskietki w formie niezabezpieczonej itp.
4. Postępowanie w przypadku naruszenia ochrony danych osobowych opisano w Rozdziale 5.

ROZDZIAŁ 3

ZABEZPIECZENIE DANYCH OSOBOWYCH

§ 5

1. Zastosowane środki techniczne ochrony danych osobowych:
1) przetwarzanie danych osobowych w wydzielonych pomieszczeniach położonych w strefie administracyjnej,
2) pomieszczenia w których stoi serwer i komputery zawierające dane osobowe i kartoteki osobowe są zabezpieczone poprzez system alarmowy.

2. Zastosowane zabezpieczenia danych osobowych w systemach informatycznych:
1) na wszystkich stacjach roboczych, na których przetwarzane są dane osobowe wprowadza się wysoki poziom zabezpieczeń,
2) ochronę przez awariami zasilania oraz zakłóceniami w sieci energetycznej serwera, na którym znajdują się bazy danych zapewnia zasilacz UPS,
3) zalogowanie się do systemu wymaga podania nazwy użytkownika i hasła. Każdy użytkownik ma przypisane uprawnienia do wykonywania operacji.
4) Oprogramowanie wykorzystywane do przetwarzania danych posiada własny system kont (zabezpieczonych hasłami) i uprawnień,
10) kopie bezpieczeństwa na nośnikach zewnętrznych wykonuje okresowo użytkownik danego systemu. Kopie przechowywane są w zamkniętej szafie metalowej. Dostęp do nośników zawierających kopie danych maja tylko upoważnione osoby,
11) kartoteki papierowe znajdują się w pomieszczeniach, w których przetwarzane są dane osobowe,
12) wydruki i dokumenty zawierające dane osobowe powinny znajdować się w miejscu, które uniemożliwia dostęp osobom postronnym.

3. Zastosowane środki organizacyjne ochrony danych osobowych:
1) zapoznanie każdej osoby z przepisami dotyczącymi ochrony danych osobowych, przed dopuszczeniem jej do pracy przy przetwarzaniu danych osobowych,
2) przeszkolenie osób, o których mowa w pkt. 1 w zakresie bezpiecznej obsługi urządzeń i programów związanych z przetwarzaniem i ochroną danych osobowych,
3) kontrolowanie otwierania i zamykania pomieszczeń w których są przetwarzane dane osobowe, polegające na otwarciu pomieszczenia przez pierwszą osobę, która rozpoczyna pracę oraz zamknięciu pomieszczenia przez ostatnią wychodzącą osobę,

4) dostęp do danych mają wyłącznie pracownicy wyznaczeni przez ABI. który prowadzi ewidencję tych pracowników obejmujący listę nazwisk użytkowników posiadających dostęp do danych, łącznie z ich identyfikatorami w systemie.

4. Zastosowane zabezpieczenia przed utratą danych:
1) ochrona serwera przed zanikiem zasilania poprzez stosowanie zasilacza UPS,
2) ochrona przed utratą zgromadzonych danych poprzez robienie kopii zapasowych na nośnikach zewnętrznych, z których w przypadku awarii odtwarzane są dane.

5. Opis struktur zbiorów danych osobowych przetwarzanych w Bibliotece określa Załącznik Nr 2.

6. Wykaz zbiorów danych osobowych, systemów informatycznych zastosowanych do ich przetwarzania oraz pomieszczeń w których przetwarzane są dane osobowe w Bibliotece przedstawia Załącznik Nr 3.

ROZDZIAŁ 4

KONTROLA PRZESTRZEGANIA ZASAD ZABEZPIECZENIA DANYCH OSOBOWYCH

§ 6

1. ABI sprawuje nadzór nad przestrzeganiem zasad ochrony danych osobowych wynikających z ustawy o ochronie danych osobowych oraz zasad ustanowionych w Polityce bezpieczeństwa.

ROZDZIAŁ 5

POSTĘPOWANIE W PRZYPADKU NARUSZENIA OCHRONY DANYCH OSOBOWYCH

§ 7

Każda osoba zatrudniona przy przetwarzaniu danych osobowych jest obowiązana niezwłocznie powiadomić ABI, gdy stwierdzi między innymi niewłaściwe lub wadliwe:
1) zabezpieczenia systemu informatycznego,
2) technicznego stanu urządzeń,
3) zawartości zbioru danych osobowych,
4) ujawnienia metody pracy lub sposobu działania programu,
5) jakości transmisji danych w sieciach komputerowych mogącej wskazywać na naruszenie zabezpieczeń tych danych,
6) innych zdarzeń mogących mieć wpływ na naruszenie danych osobowych (np. zalanie pomieszczeń, pożar, itp.).

§ 8

Czynności podejmowane do czasu przybycia ABI na miejsce naruszenia ochrony danych osobowych:
1) niezwłocznie podjąć czynności niezbędne dla powstrzymania niepożądanych skutków zaistniałego naruszenia, o ile istnieje taka możliwość, a następnie uwzględnić w działaniu również ustalenie przyczyn lub sprawców,

2) rozważyć wstrzymanie bieżącej pracy na komputerze lub pracy biurowej w celu zabezpieczenia miejsca zdarzenia,
3) zaniechać - o ile to możliwe - dalszych planowanych przedsięwzięć, które wiążą się z zaistniałym naruszeniem i mogą utrudnić udokumentowanie i analizę,
4) podjąć inne działania przewidziane i określone w instrukcjach technicznych i technologicznych stosownie do objawów i komunikatów towarzyszących naruszeniu,
5) podjąć stosowne działania, jeśli zaistniały przypadek jest określony w dokumentacji systemu operacyjnego, dokumentacji bazy danych lub aplikacji,
6) zastosować się do innych instrukcji i regulaminów, jeżeli odnoszą się one do zaistniałego przypadku,
7) udokumentować wstępnie zaistniałe naruszenie,
8) nie opuszczać bez uzasadnionej potrzeby miejsca zdarzenia do czasu przybycia ABI.

§ 9

Czynności podejmowane przez ABI po przybyciu na miejsce naruszenia ochrony danych osobowych:
1) zapoznanie się z zaistniałą sytuacją i dokonanie wyboru metody dalszego postępowania mając na uwadze ewentualne zagrożenia dla prawidłowości pracy Biblioteki,
2) żądanie dokładnej relacji z zaistniałego naruszenia od osoby powiadamiającej, jak również od każdej innej osoby, która może posiadać informacje związane z zaistniałym zdarzeniem naruszenia ochrony danych.

§ 10

1. ABI dokumentuje zaistniały przypadek naruszenia oraz sporządza raport wg wzoru stanowiącego Załącznik Nr 4, który powinien zawierać w szczególności:
1) wskazanie osoby powiadamiającej o naruszeniu oraz innych osób zaangażowanych lub odpytanych w związku z naruszeniem,
2) określenie czasu, miejsca naruszenia i powiadomienia,
3) określenie okoliczności towarzyszących i rodzaju naruszenia,
4) wyszczególnienie wziętych faktycznie pod uwagę przesłanek do wyboru metody postępowania i opis podjętego działania,
5) wstępną ocenę przyczyn wystąpienia naruszenia,
6) ocenę przeprowadzonego postępowania wyjaśniającego i naprawczego.

2. Po wyczerpaniu niezbędnych środków doraźnych po zaistniałym naruszeniu ABI podejmuje postępowanie naprawcze.

ROZDZIAŁ 6

POSTANOWIENIA KOŃCOWE

§ 11

1. 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, bądź też nie zrealizowała stosownego działania dokumentującego ten przypadek, wszczyna się postępowanie dyscyplinarne.

2. ABI zobowiązany jest prowadzić ewidencję osób upoważnionych do przetwarzania danych osobowych, zgodnie z Załącznikiem Nr 5.

3. Osoby uprawnione do przetwarzania danych osobowych obowiązuje zakres obowiązków, które stanowi Załącznik Nr 6.

4. Osoby uprawnione do przetwarzania danych osobowych składają oświadczenia zgodnie z Załącznikiem Nr 7.

5. Osoby uprawnione do przetwarzania danych osobowych otrzymują Upoważnienie do przetwarzania danych osobowych zgromadzonych w zbiorze danych osobowych wydane przez ABI, zgodnie z Załącznikiem Nr 8.

6. W sprawach nie uregulowanych niniejszym dokumentem mają zastosowanie przepisy ustawy z dnia 29 sierpnia 1997 roku o ochronie danych osobowych (tekst jednolity Dz. U. z 2002 r. Nr 101, poz. 926), 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) oraz rozporządzenie Ministra Sprawiedliwości z dnia 28 kwietnia 2004 r. w sprawie sposobu technicznego przygotowania systemów i sieci do przekazywania informacji – do gromadzenia wykazów połączeń telefonicznych i innych przekazów informacji oraz sposobów zabezpieczenia danych informatycznych (Dz. U. Nr 100, poz. 1023).

Załącznik Nr 1
do Polityki bezpieczeństwa systemów informatycznych
służących do przetwarzania danych w GBP w Bukowcu

Obowiązki Administratora Bezpieczeństwa Informacyjnego.

1. Administrator Bezpieczeństwa Informacyjnego zobowiązany jest do zapewnienia, aby dane osobowe były:
a) przetwarzane zgodnie z prawem,
b) zbierane dla oznaczonych, zgodnych z prawem celów,
c) merytorycznie poprawne i adekwatne w stosunku do celów.
3. Wdraża Politykę Bezpieczeństwa i Instrukcję Zarządzania Systemem Informatycznym.
4. Prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych w poszczególnych systemach.
5. Organizuje szkolenia mające na celu zaznajomienie każdej osoby przetwarzającej dane osobowe z przepisami dotyczącymi ich ochrony.
6. Odpowiada za to, by zakres czynności osoby zatrudnionej przy przetwarzaniu danych osobowych określał odpowiedzialność tej osoby za:
a) ochronę danych przed niepowołanym dostępem,
b) nieuzasadnioną modyfikację lub zniszczenie danych,
c) nielegalne ujawnienie danych w stopniu odpowiednim do zadań realizowanych w procesie przetwarzania danych osobowych.
7. Zgłasza zbiory danych osobowych do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych.
8. Ponadto do zakresu zadań ABI należy:

- realizacja ustawy o ochronie danych, w tym danych osobowych w zakresie dotyczącym Administratora Bezpieczeństwa Informacji,
- zapewnienie, że do informacji chronionych mają dostęp wyłącznie osoby upoważnione oraz że mogą one wykonywać wyłącznie uprawnione operacje,
- zabezpieczenie obszarów przetwarzania danych, w tym danych osobowych w sposób uniemożliwiający dostęp do nich osób trzecich,
- ewidencjonowanie udostępniania danych zgodnie z ustawą o ochronie danych osobowych,
- weryfikację dopuszczenia użytkowników do przetwarzania danych.

Załącznik Nr 2
do Polityki bezpieczeństwa systemów informatycznych
służących do przetwarzania danych w GBP w Bukowcu

Opis struktur zbiorów danych przetwarzanych w Miejskiej Bibliotece Publicznej w Sławkowie

Struktury wewnętrzne baz danych przetwarzanych w Gminnej Bibliotece Publicznej w Bukowcu są zastrzeżone prawami autorskimi należącymi do producentów w/w oprogramowania.

Załącznik Nr 3
do Polityki bezpieczeństwa systemów informatycznych
służących do przetwarzania danych w GBP w Bukowcu

1. Wykaz zbiorów danych osobowych oraz systemów informatycznych zastosowanych do ich przetwarzania.

Lp.	**Nazwa zbioru**	**Program/system przetwarzający ; forma przetwarzania**	**Lokalizacja (nr pomieszczenia)**
1.	System Płatnik	System Płatnik – elektroniczna forma przetwarzania	Księgowość
2.	Zbiór zobowiązań użytkowników Biblioteki	Manualna forma przetwarzania	Wypożyczalnia/ Czytelnia
3.	Zbiór akt osobowych pracowników zatrudnionych w GBP	Manualna forma przetwarzania	Księgowość
4.	Zbiór podań osób ubiegających się o pracę	Manualna forma przetwarzania	Księgowość
5.	Zbiór umów o dzieło i umów zleceń	Manualna forma przetwarzania	Księgowość
6.	Rejestr korespondencji przychodzącej i wychodzącej	Manualna forma przetwarzania	Kierownik
7.	Rejestr delegacji	Manualna forma przetwarzania	Księgowość

2. Wykaz budynków i pomieszczeń w których przetwarzane są dane osobowe.

Lp.	**Adres budynku**
1.	Bukowiec, ul Dworcowa 7, 86-122 Bukowiec
2.	Przysiersk, 86-122 Bukowiec – Filia GBP

Załącznik Nr 4
do Polityki bezpieczeństwa systemów informatycznych
służących do przetwarzania danych w GBP w Bukowcu

R a p o r t
z naruszenia bezpieczeństwa systemu informatycznego
w Gminnej Bibliotece Publicznej w Bukowcu

1. Data: ..... Godzina: .....
(dd.mm.rrrr) (00:00)

2. Osoba powiadamiająca o zaistniałym zdarzeniu:

.....
(Imię, nazwisko, stanowisko służbowe, nazwa użytkownika (jeśli występuje)

3. Lokalizacja zdarzenia:

.....
(np. nr pokoju, nazwa pomieszczenia)

4. Rodzaj naruszenia bezpieczeństwa oraz okoliczności towarzyszące:

.....

.....

5. Podjęte działania:

.....

.....

6. Przyczyny wystąpienia zdarzenia:

.....

.....

7. Postępowanie wyjaśniające:

.....

.....

…….....
(Data, podpis Administratora Bezpieczeństwa Informacji)

Załącznik Nr 5
do Polityki bezpieczeństwa systemów informatycznych
służących do przetwarzania danych w GBP w Bukowcu

Ewidencja osób upoważnionych do przetwarzania danych osobowych

Lp.	Imię i nazwisko	Data przyznania uprawnienia	Data odebrania uprawnienia	Zakres upoważnienia lub system informatyczny

Załącznik Nr 6
do Polityki bezpieczeństwa systemów informatycznych
służących do przetwarzania danych w GBP w Bukowcu

Dodatkowy zakres obowiązków
dla pracowników Gminnej Bibliotece Publicznej w Bukowcu

1. Pracownik zobowiązany jest dbać o bezpieczeństwo powierzonych mu do przetwarzania, archiwizowania lub przechowywania danych zgodnie z obowiązującą w Bibliotece Polityką Bezpieczeństwa oraz Instrukcją zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych, a w szczególności:
a) chronić dane przed dostępem osób nieupoważnionych,
b) chronić dane przed przypadkowym lub nieumyślnym zniszczeniem, utratą lub modyfikacją,
c) chronić nośniki magnetyczne i optyczne oraz wydruki komputerowe przed dostępem osób nieupoważnionych oraz przed przypadkowym zniszczeniem,
d) utrzymywać w tajemnicy powierzone identyfikatory, hasła, częstotliwość ich zmiany oraz szczegóły technologiczne systemów także po ustaniu zatrudnienia w Bibliotece.
2. Zabrania się pod rygorem odpowiedzialności służbowej i karnej:
a) ujawniać dane - w tym dane osobowe zawarte w obsługiwanych systemach,
b) kopiować bazy danych lub ich części poza przewidzianymi instrukcją technologiczną kopiami bezpieczeństwa,
c) przetwarzania danych w sposób inny niż opisany instrukcją technologiczną.

Załącznik Nr 7
do Polityki bezpieczeństwa systemów informatycznych
służących do przetwarzania danych w GBP w Bukowcu

……..….. Bukowiec, dn. ……
(imię i nazwisko pracownika)

…….…..
(adres)

……..…..

OŚWIADCZENIE

Niniejszym oświadczam, że zapoznałem się z przepisami ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 ze zmianami) oraz że zobowiązuję do ich przestrzegania.

W szczególności zobowiązuję się do właściwego przechowywania i zabezpieczenia informacji zawierających dane osobowe oraz do skutecznego niszczenia dokumentów i brudnopisów, które podlegają zniszczeniu a zawierają dane osobowe tak, aby osoby nieupoważnione nie uzyskały dostępu do przedmiotowych danych.

……..

(podpis)

…… ……
(podpis pracownika) (podpis przełożonego)

Załącznik Nr 8
do Polityki bezpieczeństwa systemów informatycznych
służących do przetwarzania danych w GBP w Bukowcu

UPOWAŻNIENIE

Niniejszym upoważniam ....., pracownika Gminnej Biblioteki Publicznej w Bukowcu do przetwarzania danych osobowych zgodnie z zakresem obowiązków dla zajmowanego przez Panią stanowiska pracy.

Podstawa prawna: art. 37 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926 ze zmianami ogłoszonymi w Dz. U. z 2002 r. Nr 153, poz. 1271; z 2004 r. Nr 25, poz. 219, Nr 33, poz. 285).

Bukowiec, dn.

.....

(podpis)

Przyjęłam do wiadomości i stosowania

……