Załącznik nr 1
do Zarządzenia Nr 12/2014
Dyrektora Powiatowej Biblioteki Publicznej w Otwocku z dnia 17 czerwca 2014 r.

Polityka Bezpieczeństwa Danych Osobowych wraz z Instrukcją zarządzania systemem informatycznym przetwarzającym dane osobowe

w Powiatowej Bibliotece Publicznej w Otwocku

Wersja 1		**Pieczęć firmowa:**	
Opracował: ***Ewa Koc***	**Data:** ***17.06.2014 r.***	**Zatwierdził:** ***Ewa Koc***	**Data:** ***17.06.2014 r.*** **…..**

			.

1. Polityka Bezpieczeństwa

1.1 Wstęp

Polityka Bezpieczeństwa, zwana dalej Polityką, oraz Instrukcja zarządzania systemami informatycznymi przetwarzającymi dane osobowe, zwana dalej Instrukcją, została opracowana zgodnie z wymogami ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. Nr 133, poz. 883 z późn. zm.) oraz wymaganiami 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).

1.2 Obowiązki Administratora Danych Osobowych i Administratora Bezpieczeństwa Informacji

Administratorem Danych Osobowych w myśl Ustawy o ochronie Danych Osobowych jest Powiatowa Biblioteka Publiczna w Otwocku.

Do najważniejszych obowiązków ADO, należy:

1. opracowanie i wdrożenie Polityki i Instrukcji (w tym zabezpieczenie zbiorów danych powierzonych do przetwarzania)
2. wydawanie i anulowanie upoważnień dla osób upoważnionych do przetwarzania danych osobowych
3. prowadzenie Ewidencji osób upoważnionych do przetwarzania danych osobowych
4. powołanie Administratora Bezpieczeństwa Informacji
5. szczegółowe obowiązki ABI określone są w **Załączniku 1**

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

Jest to tak zwany Obszar przetwarzania danych osobowych. Wykaz ujęto w **Załączniku 2**

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

Wykaz zbiorów danych osobowych (w tym zbiorów powierzonych do przetwarzania) i programów użytych do przetwarzania tych danych ujęto w **Załączniku 3**

1.5 Sposób przepływu danych pomiędzy poszczególnymi systemami

Sposób przepływu danych osobowych pomiędzy systemami, w których przetwarzane są dane osobowe przedstawiono w **Załączniku 4**

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

1.6.1 Zabezpieczenia organizacyjne

1. **obligatoryjnie:** wyznaczono Administratora Bezpieczeństwa Informacji (ABI)
2. **obligatoryjnie:** została opracowana i wdrożona polityka i instrukcja
3. **obligatoryjnie**: do przetwarzania danych zostały dopuszczone wyłącznie osoby posiadające upoważnienia nadane przez administratora danych
4. **obligatoryjnie:** prowadzona jest ewidencja osób upoważnionych do przetwarzania danych

5. **obligatoryjnie:** osoby zatrudnione przy przetwarzaniu danych zostały zaznajomione z przepisami dotyczącymi ochrony danych osobowych oraz w zakresie zabezpieczeń systemu informatycznego
6. **obligatoryjnie:** osoby zatrudnione przy przetwarzaniu danych osobowych obowiązane zostały do zachowania ich w tajemnicy
7. o**bligatoryjnie**: przetwarzanie danych osobowych dokonywane jest w warunkach zabezpieczających dane przed dostępem osób nieupoważnionych
8. **obligatoryjnie:** 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

1.6.2 Zabezpieczenia fizyczne pomieszczeń, gdzie są przetwarzane dane osobowe w wersji papierowej i elektronicznej

1. **obligatoryjnie:** drzwi zamykane na klucz
2. **obligatoryjnie:** zamknięte niemetalowe / metalowe szafy (klucze)
3. **obligatoryjnie:** niszczarki dokumentów
4. **obligatoryjnie:** stosuje się politykę kluczy
    a. Obowiązuje sześciodniowy tydzień pracy, tzn. od poniedziałku do piątku w godzinach 07,30 – 19:00, w soboty 8,00-14,00.
    b. Dostęp do budynków i pomieszczeń biurowych możliwy jest wyłącznie przez osoby upoważnione, które posiadają do nich klucze
    c. Klucze poza godzinami pracy osoby upoważnione sprawują nad nimi całodobowy nadzór osobisty
    d. Klucze zapasowe przechowywane są w wyznaczonych i zabezpieczonych miejscach (depozyt)
    e. Wydawanie kluczy zapasowych upoważnionym pracownikom może odbywać się tylko w uzasadnionych sytuacjach oraz przypadkach awaryjnych za zgodą bezpośredniego przełożonego.
    f. Klucze zapasowe po ich wykorzystaniu należy niezwłocznie zwrócić do depozytu za poświadczeniem zwrotu w Ewidencji dostępu do pomieszczeń
    g. Klucze służące do zabezpieczenia biurek i szaf muszą być jednoznacznie opisane
    h. W godzinach pracy klucze pozostają pod nadzorem pracowników, którzy ponoszą pełną odpowiedzialność za ich należyte zabezpieczenie
    i. Zabrania się pozostawiania kluczy w biurkach i szafach podczas chwilowej nieobecności osób upoważnionych w pomieszczeniu
    j. Po zakończeniu pracy, klucze służące do zabezpieczenia biurek i szaf muszą być przechowywane w zabezpieczonym miejscu
    k. Naruszenie zasad polityki kluczy może spowodować wyciągnięcie następujących konsekwencji: Poniesienie odpowiedzialności wynikających z art. 52 kodeksu pracy lub poniesienie odpowiedzialności wynikających z art. 363 § 1. kodeksu cywilnego.
5. opcjonalnie: system alarmowy przeciwwłamaniowy
6. opcjonalnie: system przeciwpożarowy /gaśnice

1.6.3 Zabezpieczenia sprzętowe infrastruktury informatycznej i telekomunikacyjnej

1. **obligatoryjnie:** zastosowano UPS do serwera lub kluczowych komputerów, na których są przetwarzane dane osobowe

2. **obligatoryjnie:** dostęp do komputera/laptopa z danymi osobowymi odbywa się poprzez podanie loginu i hasła
3. **obligatoryjnie:** zastosowano system antywirusowy
4. **obligatoryjnie:** użyto system Firewall do ochrony dostępu do sieci komputerowej

1.6.4 Zabezpieczenia programów przetwarzających dane osobowe

1. **obligatoryjnie:** dla osób upoważnionych określono zakres obowiązków i prawa dostępu do danych osobowych
2. **obligatoryjnie:** dostęp do danych osobowych w systemach/programach informatycznych wymaga podania nazwy użytkownika oraz hasła
3. opcjonalnie: użytkownicy systemów/programów informatycznych posiadają w nich konta z określonymi prawami dostępu
4. opcjonalnie: zastosowano zahasłowane wygaszacze ekranu uruchamiane po dłuższej nieaktywności użytkownika
5. opcjonalnie: zmianę haseł wymusza system
6. opcjonalnie: dane osobowe są zaszyfrowane na twardych dyskach lub w bazach danych

2. Instrukcja

2.1 Procedura nadawania uprawnień do przetwarzania danych osobowych.

1. przed nadaniem upoważnienia, osoba jest zapoznana z zasadami ochrony danych osobowych zawartymi w Polityce i Instrukcji
2. osoba zapoznana z zasadami ochrony zobowiązana jest do podpisania Oświadczenia o poufności w **Załączniku 5 Oświadczenie-Upoważnienie**
3. ADO lub ABI w imieniu ADO nadaje upoważnienie osobie upoważnianej wypełniając **Załącznik 5 Oświadczenie-Upoważnienie**
4. ABI prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych, zgodnie z **Załącznikiem 6**

2.2 Metody i środki uwierzytelnienia (polityka haseł)

1. hasła nie mogą być powszechnie używanymi słowami
2. użytkownik zobowiązuje się do zachowania hasła w poufności, nawet po utracie przez nie ważności i jest zobowiązany jest do niezwłocznej zmiany tego hasła, gdy zostało ono ujawnione
3. zabronione jest zapisywanie haseł w sposób jawny oraz przekazywanie ich innym osobom
4. hasło zmieniane jest w sposób automatyczny co 30 dni lub użytkownik zobowiązany jest do zmiany hasła samodzielnie co 30 dni
5. hasło składa się z co najmniej z 8 znaków, w tym dużych i małych liter oraz z cyfr lub znaków specjalnych

2.3 Procedura rozpoczęcia, zawieszenia i zakończenia pracy

1. użytkownik loguje się do systemu/programu informatycznego przetwarzającego dane osobowe z użyciem identyfikatora i hasła
2. użytkownik jest zobowiązany do powiadomienia ABI o próbach logowania się do systemu osoby nieupoważnionej - jeśli system to sygnalizuje
4. użytkownik jest zobowiązany do uniemożliwienia osobom niepowołanym (np. stażystom, pracownikom innych działów, pracownikom ościennych firm) wgląd do danych wyświetlanych na monitorach komputerowych – tzw. Polityka czystego ekranu

5. przed czasowym opuszczeniem stanowiska pracy, użytkownik zobowiązany jest wywołać blokowany hasłem wygaszacz ekranu lub wylogować się z systemu.
6. po zakończeniu pracy, użytkownik zobowiązany jest wylogować się z systemu informatycznego, ewentualnie wyłączyć sprzęt komputerowy oraz stosować politykę czystego biurka dla dokumentów i nośników

2.4. Procedura tworzenia kopii zapasowych

1. procedura obejmuje tworzenie kopii bezpieczeństwa wszystkich programów wraz ze środowiskiem, wymienionych w **Załączniku 2**
2. kopie całościowe wykonywane są z częstotliwością 1-miesięczną
3. kopie przyrostowe wykonywane sporządzane są na streamerze, serwerze (mirror), pendrive lub dysku wymiennym
4. każda kopia jest czytelnie opisana co do zawartości i daty sporządzenia
5. kopie przechowywane są przez okres 5 lat.
6. dostęp do kopii mają: Dyrekcja, Informatyk
7. kopie przechowywane są w innym pomieszczeniu niż serwerownia, zabezpieczone w sejfie lub w szafie zamykanej na klucz
8. Informatyk zobowiązany jest do sporządzenia kopii oraz weryfikacji ich poprawności i możliwości ponownego odtworzenia
9. niszczenie kopii odbywa się poprzez trwałe/fizyczne zniszczenie nośnika lub nieodwracalne usunięcie danych z nośnika z użyciem specjalnego oprogramowana

2.5 Sposób, miejsce i okres przechowywania elektronicznych nośników informacji i wydruków

1. do typowych nośników należą: pen-drive, przenośne twarde dyski, laptopy, dokumentacja papierowa
2. użytkownicy są zobowiązani do niezwłocznego i trwałego usuwania/kasowania danych osobowych z nośników po ustaniu celu ich przetwarzania
3. nośniki są przechowywane w sposób uniemożliwiający dostęp do nich osób nieupoważnionych, jak również zabezpieczający je przed zagrożeniami środowiskowymi (zalanie, pożar, wpływ pól elektromagnetycznych
4. zabrania się wynoszenia poza obszar organizacji niezabezpieczonych nośników z danymi osobowymi – nośniki muszą być zaszyfrowane
5. w przypadku wysyłania danych mailem, pliki muszą być zahasłowane a hasło przesłane inną drogą (mailem)
6. zabrania się przekazywania nośników z nieusuniętymi danymi osobowymi pomiotom lub osobom zewnętrznym (darowizny, naprawy)
7. dane osobowe w postaci papierowej zabezpiecza się w wersji minimum: w szafach i biurkach zamykanych na klucz
8. zabrania się pozostawiania dokumentów i nośników, jako dostępnych dla osób postronnych
9. niszczenie dokumentów i tymczasowych wydruków musi odbywać się w niszczarkach

2.6 Procedura zabezpieczenia systemu informatycznego, w tym przed wirusami komputerowymi

2.6.1 Ochrona antywirusowa

1. każdy z komputerów musi być wyposażony w licencjonowany program antywirusowy

2. program antywirusowy musi być aktywny i zabrania się jego wyłączania
3. program antywirusowy musi zawierać aktualną bazę wirusów, czyli musi być na bieżąco aktualizowany

2.6.2. Ochrona przed nieautoryzowanym dostępem do sieci lokalnej

1. każdy z komputerów (lub router dla sieci) powinien być wyposażony w firewall sprzętowy lub programowy
2. dodatkowo można stosować: systemy IDS/IPS, technikę NAT, proxy serwer

2.7 Zasady i sposób odnotowywania w systemie informacji o udostępnieniu danych osobowych

1. w przypadku udostępnienia danych osobowych innym pomiotom, niż na podstawie wymagań prawa, należy ten fakt odnotować
2. jeżeli system/program informatyczny na to pozwala, dane o udostępnieniu należy wprowadzić do systemu/programu. W przeciwnym wypadku należy dane te wpisać do zaprowadzonej specjalnie w tym celu Ewidencji ręcznej. Ewidencja musi zawierać następujące dane: Data udostępnienia danych, Nazwa i adres podmiotu, któremu dane udostępniono, podstawa prawna udostępnienia danych (Art. 23 / 27 UODO), Zakres udostępnionych danych
3. na żądanie osoby, której dane zostały udostępnione - informacje o udostępnieniu danych są zamieszczane w raporcie z systemu informatycznego lub z Ewidencji ręcznej

2.8. Procedura wykonywania przeglądów i konserwacji

1. zapewniono serwis naprawczy dla sprzętu komputerowego
2. prowadzane są przeglądy i konserwacje systemu informatycznego zgodnie z planem lub wytycznymi producentów
3. naprawa/konserwacja/serwis sprzętu komputerowego i programów, wykonywane przez podmiot zewnętrzny, powinny odbywać się pod ścisłym nadzorem osób upoważnionych
4. przed przekazaniem uszkodzonego sprzętu komputerowego z danymi osobowymi do naprawy poza teren organizacji, należy trwale usunąć dane osobowe z nośników
5. aktualizację oprogramowania należy przeprowadzać zgodnie z zaleceniami producentów oraz opinią rynkową co do bezpieczeństwa i stabilności nowych wersji (np. aktualizacje, service pack-i, łatki)

Załącznik 1.
Powołanie ABI

Otwock , data 17.06.2014 r.

Powołanie Administratora Bezpieczeństwa Informacji

Z dniem 17 czerwca 2014 funkcję Administratora Bezpieczeństwa Informacji obejmuje **Pan Robert Przybysz.**

W zakresie realizacji zadań nałożonych na Administratora Danych Osobowych, Administrator Bezpieczeństwa Informacji podlega bezpośrednio Dyrektorowi.

Do zakresu obowiązków ABI należą:
1. organizacja bezpieczeństwa i ochrony danych osobowych zgodnie z wymogami ustawy o ochronie danych osobowych,
2. zapewnienie przetwarzania danych zgodnie z uregulowaniami polityki bezpieczeństwa informacji
3. wydawanie i anulowanie Upoważnień do przetwarzania danych osobowych,
4. prowadzenie Ewidencji osób upoważnionych do przetwarzania 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. wyznaczania, rekomendowania i egzekwowania wykonania zadań związanych z ochroną danych osobowych w całej organizacji
2. 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,
3. żądać złożenia pisemnych lub ustnych wyjaśnień w zakresie niezbędnym do ustalenia stanu faktycznego,
4. żądać okazania dokumentów i wszelkich danych mających bezpośredni związek z problematyką kontroli,
5. żądać udostępnienia do kontroli urządzeń, nośników oraz systemów informatycznych służących do przetwarzania danych,

Z poważaniem,

Zarządzający

.....

Załącznik 2.
Obszar przetwarzania danych osobowych.

Wykaz budynków i pomieszczeń,
w których przetwarzane są dane osobowe

1. **Adres budynku**: 05-400 Otwock, ul. Kazimierza Pułaskiego 3 A

2. **Wykaz pomieszczeń:**

1) Wypożyczalnia

2) Czytelnia

3) Pokój dyrektora

Wykaz zbiorów danych osobowych

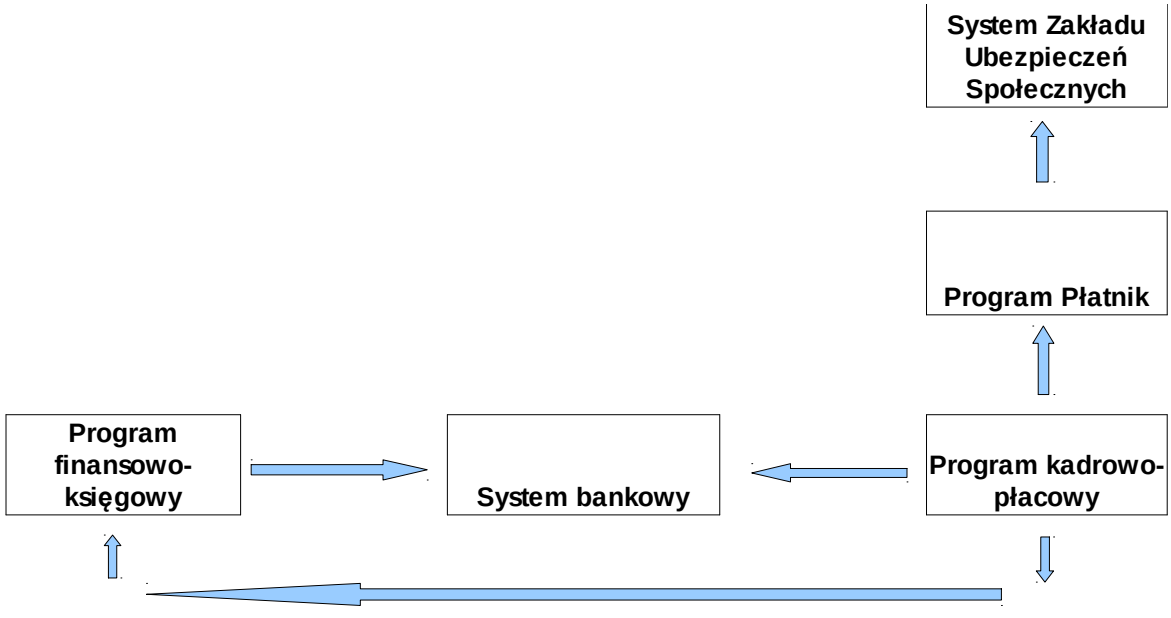
Legenda (1): (D) drzwi zamykane na klucz, (S): zamknięte niemetalowe / metalowe szafy (klucze), (N) niszczarki dokumentów, (O) zabezpieczenie okien (kraty/folia antywłamaniowa/rolety), (A) system alarmowy przeciwwłamaniowy, (M) monitoring kamer, (SO) służba ochrony, (SF)sejf lub kasa pancerna, (P) system przeciwpożarowy /gaśnice

Lp.	Nazwa zbioru danych	Program służący do przetwarzania baz danych	Lokalizacja	Zabezpieczenia fizyczne (1)
1	Zbiór danych osobowych pracowników	Program Symfonia Finanse i Księgowość	Księgowość	S, D, A, S, O
		Program Symfonia Kadry-Płace		
		Program Płatnik		
2	Rejestr czytelników	Program Mateusz	Wypożyczalnia / Czytelnia	A, P
3	Korespondencja	Pliki stworzone za pomocą procesorów tekstów znajdujących się na lokalnym komputerze sieciowym oraz udziałach sieciowych	Dyrektor	A, D, S

Załącznik 4.
Przepływ danych pomiędzy poszczególnymi systemami

Sposób przepływu danych
pomiędzy poszczególnymi systemami

Program A lub Moduł programu	Program B lub Moduł programu	Kierunek przepływu danych osobowych (pomiędzy programami lub modułami)	Sposób przesyłania danych osobowych
Program Symfonia	Kadry i Płace	Dwukierunkowo	Automatycznie
Program Symfonia	Finanse i Księgowość	Dwukierunkowo	Automatycznie
Program Płatnik		Jednokierunkowo z programu kadrowo-płacowego do rogramu Płatnik	Półautomatycznie – eksport pliku z programu kadrowo-płacowego na serwer, który następnie pobierany jest przez program Płatnik
Mateusz		Dane wprowadzane z klawiatury	Dane do wglądu uprawnionego operatora



Jednokierunkowo – tylko do odczytu
dwukierunkowo – odczyt i zapis

Załącznik 5.
Oświadczenie o poufności i upoważnienie do przetwarzania danych osobowych

Miejscowość ……..

Upoważnienie do przetwarzania danych osobowych Nr .....

Z dniem dd-mm-rrrr upoważniam Panią/Pana … do przetwarzania danych osobowych.

Upoważnienie nadane jest celem realizacji obowiązków wynikających z realizacji powierzonych zadań.

Zakres przetwarzania obejmuje *): wgląd, drukowanie, wprowadzanie, modyfikację, usuwanie, archiwizację, przesyłanie, naprawę danych osobowych * - niepotrzebne skreślić

Zobowiązuję Panią*/Pana* do przestrzegania przepisów dotyczących ochrony danych osobowych, w szczególności ustawy z dnia 29 sierpnia 1997r. o ochronie danych osobowych (tj. Dz.U. z 2002r. Nr 101, poz. 926 ze zm.), wydanych na jej podstawie aktów wykonawczych oraz wprowadzonych i wdrożonych do stosowania przez Administratora Danych „Polityki Bezpieczeństwa Informacji" oraz „Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych".

Podpis Upoważniającego

……..

Oświadczenie o poufności

Oświadczam, iż zapoznano mnie z przepisami dotyczących ochrony danych osobowych, w szczególności ustawy z dnia 29 sierpnia 1997r. o ochronie danych osobowych (tj. Dz.U. z 2002r. Nr 101, poz. 926 ze zm.), wydanych na jej podstawie aktów wykonawczych oraz wprowadzonych i wdrożonych do stosowania przez Administratora Danych „Polityki Bezpieczeństwa Informacji" oraz „Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych".

W szczególności zobowiązuję się do:

- przetwarzania danych osobowych wyłącznie w zakresie i celu przewidzianym Upoważnieniem
- zachowania w tajemnicy danych osobowych do których mam lub będę miał/a dostęp w związku z wykonywaniem obowiązków pracowniczych lub zadań zleconych przez Zleceniodawcę
- niewykorzystywania danych osobowych w celach pozasłużbowych bądź niezgodnych ze zleceniem o ile nie są one jawne
- zachowania w tajemnicy sposobów zabezpieczenia danych osobowych o ile nie są one jawne
- ochrony danych osobowych przed udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem Ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.

Przyjmuję do wiadomości, iż postępowanie sprzeczne z powyższymi zobowiązaniami, może być uznane * przez Pracodawcę za ciężkie naruszenie obowiązków pracowniczych w rozumieniu art. 52 § 1 pkt 1 Kodeksu Pracy lub za naruszenie przepisów karnych ustawy z dnia 29 sierpnia 1997r. o ochronie danych osobowych (tj. Dz.U. z 2002r. Nr 101, poz. 926 ze zm.).

Czytelny podpis pracownika, zleceniobiorcy

……..

Ewidencja osób upoważnionych do przetwarzania danych osobowych

Legenda: Uprawnienia: (WG) wgląd, (W) wprowadzanie, (M) modyfikacja, (U) usuwanie, (A) archiwizacja

Nazwa zbioru danych (zakres upoważnienia)	Nazwisko i Imię użytkownika	Identyfikator użytkownika	Rodzaj uprawnień (zakres upoważnienia)	Data nadania upoważnienia	Data usta upoważni
Zbiór danych osobowych pracowników,	Wanda Stańczak	wstańczak	WG, W, M, U, A	01.09.2013 r.	
Rejestr czytelników, Korespondencja	Ewa Koc	ekoc	WG, W, M, U, A	01.09.2013 r.	
Rejestr czytelników	Małgorzata Bonowska	mbonowska	WG, W, M, U	01.09.2013 r.	
Rejestr czytelników	Sylwia Królak	skrolak	WG, W, M, U	01.02.2014 r.	
Rejestr czytelników	Beata Rosłoniec-Kośmicka	brosloniec	WG, W,	18.03.2014 r.	
Rejestr czytelników	Klaudia Pieterwas	kpieterwas	WG, W	18.03.2014 r.	