Załącznik nr 1
do Zarządzenia Nr JZK.0210.42.2012
Dyrektora Jastrzębskiego Zakładu Komunalnego
w Jastrzębiu-Zdroju z dnia 31 grudnia 2012 r.

Jastrzębski Zakład Komunalny w Jastrzębiu-Zdroju

Polityka bezpieczeństwa

1. Podstawa prawna

Niniejszy dokument jest zgodny następującymi przepisami prawa:

- ustawa o ochronie danych osobowych z dnia 29 sierpnia 1997 r. (tekst jednolity Dz. U. z 2002 r., Nr 101, poz. 926 z późn. zm.),
- rozporządzenie Ministra Spraw Wewnętrznych i Administracji w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych z dnia 29 kwietnia 2004 r. (Dz. U. z 2004 r., Nr 100, poz. 1024).

2. Definicje.

Ilekroć w dokumencie jest mowa o:

a) JZK - należy przez to rozumieć miejską jednostkę budżetową Jastrzębski Zakład Komunalny w Jastrzębiu-Zdroju,
b) Administratorze Danych Osobowych (ADO) - należy przez to rozumieć dyrektora Jastrzębskiego Zakładu Komunalnego w Jastrzębiu-Zdroju,
c) Administratorze Bezpieczeństwa Informacji (ABI) - rozumie się przez to osobę odpowiedzialną za nadzór nad przestrzeganiem w JZK zasad ochrony danych osobowych określonych w niniejszym dokumencie oraz wymagań w zakresie ochrony wynikających z powszechnie obowiązujących przepisów prawa,
d) Administratorze Systemu Informatycznego (ASI) - należy przez to rozumieć osobę odpowiedzialną za funkcjonowanie systemu informatycznego w Jastrzębskim Zakładzie Komunalnym w Jastrzębiu-Zdroju,
e) Identyfikatorze - należy przez to rozumieć elektroniczne, indywidualne oznaczenie pracowników w systemie informatycznym, tzw. login,
f) pracowniku lub użytkowniku systemu - rozumie się przez to osobę upoważnioną do przetwarzania danych osobowych w systemie. Jest to osoba zatrudniona w JZK, osoba wykonująca pracę na podstawie umowy zlecenia lub innej umowy cywilno-prawnej, osoba odbywająca staż w JZK,
g) Ustawie - należy przez to rozumieć ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (t.j. Dz. U. z 2002 r. Nr 101, poz. 926 z pózn. zm.).

3. Cel polityki bezpieczeństwa.

Celem polityki bezpieczeństwa jest zapewnienie ochrony danych osobowych przetwarzanych w celach określonych w art. 27 ust. 2 pkt 7 ustawy przetwarzanych przez Jastrzębski Zakład Komunalny w Jastrzębiu-Zdroju przed wszelkiego rodzaju zagrożeniami, tak wewnętrznymi jak i zewnętrznymi, świadomymi lub nieświadomymi.

4. Zakres polityki bezpieczeństwa.

4.1. Polityka bezpieczeństwa reguluje zagadnienia związane z przetwarzaniem w JZK danych osobowych tworzonych w sposób:

a) tradycyjny (w postaci papierowej),
b) elektroniczny (za pomocą systemów informatycznych).

4.2. Polityka bezpieczeństwa obowiązuje wszystkich pracowników JZK oraz dostawców i podmiotów współpracujących z JZK na podstawie umów cywilnoprawnych, mających jakikolwiek

kontakt z danymi osobowymi objętymi ochroną.

5. Odpowiedzialność.

5.1. Administratorem danych osobowych w JZK jest dyrektor. ADO pełni jednocześnie rolę administratora bezpieczeństwa informacji.
5.2. ABI odpowiada za:

a) zapewnienie, aby do danych osobowych miały dostęp wyłącznie osoby upoważnione w zakresie wykonywanych zadań,
b) zarządzanie uprawnieniami do przetwarzania danych osobowych,
c) prowadzenie rejestru wydanych upoważnień do przetwarzania danych osobowych,
d) zlecenie administratorowi systemu informatycznego modyfikacji uprawnień w systemach informatycznych w przypadku odebrania lub zmiany upoważnienia do przetwarzania danych osobowych,
d) fizyczne i techniczne zabezpieczenie pomieszczeń stanowiących obszar przetwarzania danych osobowych oraz kontroli przebywających w nich osób,
e) nadzór nad realizacją zasad ochrony danych określonych w dokumentacji bezpieczeństwa,
f) nadzór na obiegiem oraz przechowywaniem dokumentów zawierających dane osobowe,
g) szkolenie osób dopuszczonych do przetwarzania danych osobowych z zakresu przepisów prawa oraz uregulowań wewnętrznych w zakresie bezpieczeństwa danych osobowych,
h) nadzór nad zgłoszeniami zbiorów danych osobowych do Generalnego Inspektora Ochrony Danych Osobowych,
i) aktualizację dokumentacji bezpieczeństwa,
j) w przypadku zgłoszenia naruszenia bezpieczeństwa danych osobowych: doraźne zabezpieczenie danych, zabezpieczenie dowodów, analizę sytuacji, okoliczności i przyczyn, które doprowadziły do naruszenia bezpieczeństwa danych,
k) okresowe przeprowadzanie przeglądu bezpieczeństwa.

5.3. Administrator Systemu Informatycznego odpowiada za poprawne funkcjonowanie systemu informatycznego JZK oraz stosowanie informatycznych środków ochrony informacji. W szczególności odpowiada za:

a) wykonywanie kopii zapasowych, ich przechowywaniem i weryfikacją,
b) wykonywanie przeglądów, konserwacji oraz uaktualnień systemów informatycznych służących do przetwarzania danych osobowych oraz wszystkich innych czynności na bazach danych osobowych,
c) zapewnienie poprawnego działania systemów zabezpieczeń systemów informatycznych, sieci komputerowej, systemów zapasowego zasilania itp.;
d) nadzór nad prawidłowością funkcjonowania systemów autoryzacji użytkowników w systemie informatycznym przetwarzającym dane osobowe oraz kontroli dostępu do danych osobowych,
e) podjęcie natychmiastowych działań zabezpieczających stan systemu informatycznego w przypadku otrzymania informacji o naruszeniu zabezpieczeń systemu informatycznego lub informacji o zmianach w sposobie działania programu lub urządzeń wskazujących na naruszenie bezpieczeństwa danych osobowych.

5.4. Odpowiedzialność pracowników.

a) użytkownik systemu ma prawo do wykonywania tylko tych czynności, do których został upoważniony,
b) użytkownik systemu ponosi wszelką odpowiedzialność za wszystkie operacje wykonane przy użyciu jego identyfikatora i hasła dostępu z wyjątkiem sytuacji, kiedy ABI użyje

hasła użytkownika podczas jego nieobecności. ABI ma obowiązek sporządzić z tego zdarzenia protokół, z którym zostaje zapoznany kierownik jednostki oraz użytkownik systemu, którego hasło zostało użyte. Po zapoznaniu się z protokołem, użytkownik systemu ma obowiązek dokonać natychmiastowej zmiany hasła dostępu i przekazać je ABI,

c) wszelkie przekroczenia lub jakiekolwiek próby przekroczenia przez pracownika przyznanych uprawnień, traktowane będą jako naruszenie podstawowych obowiązków pracowniczych,
d) na pisemny i uzasadniony wniosek kierownika komórki organizacyjnej JZK ABI może odebrać uprawnienia pracownikowi z podaniem daty oraz przyczyny odebrania uprawnień. W uzasadnionej sytuacji ABI może odebrać uprawnienia w sposób natychmiastowy. Z takiego postępowania ma on sporządzić notatkę służbową do wiadomości kierownika komórki organizacyjnej i użytkownika systemu, którego sprawa dotyczy,
e) hasło oraz uprawnienia użytkownika systemu, który je utracił, należy niezwłocznie wyrejestrować z systemu informatycznego. Wyrejestrowania z systemu dokonuje ASI,
f) użytkownik systemu zatrudniony przy przetwarzaniu danych osobowych zobowiązany jest do zachowania ich w poufności oraz dołożenia wszelkich starań, aby dane osobowe nie zostały przekazane osobom nieuprawnionym,
g) użytkownik zobowiązany jest do niezwłocznego informowania przełożonych lub ABI o stwierdzeniu lub o powzięciu podejrzenia o naruszeniu bezpieczeństwa danych osobowych.

6. Wykaz zbiorów danych przetwarzanych w JZK.

Wykaz zbiorów danych przetwarzanych w JZK przedstawia **załącznik nr 1** do niniejszej polityki bezpieczeństwa.

7. Zakres danych osobowych przetwarzanych w JZK.

Zakres danych osobowych przetwarzanych w w JZK przedstawia **załącznik nr 1** do niniejszej polityki bezpieczeństwa.

8. Wykaz budynków i pomieszczeń, w których przetwarzane są dane osobowe.

Wykaz budynków i pomieszczeń, w których przetwarzane są dane osobowe przedstawia **załącznik nr 1** do niniejszej polityki bezpieczeństwa.

9. Określenie fizycznych, organizacyjnych, sprzętowych i informatycznych środków ochrony danych osobowych polityki bezpieczeństwa.

W JZK stosować należy środki bezpieczeństwa adekwatne dla wysokiego poziomu bezpieczeństwa przetwarzania danych osobowych systemie informatycznym określonego w załączniku nr 1 do Rozporządzenie Ministra Spraw Wewnętrznych i Administracji w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych z dnia 29 kwietnia 2004 r. (Dz. U. 2004 Nr 100, poz. 1024).

9.1. Środki ochrony fizycznej.

a) urządzenia służące do przetwarzania danych osobowych muszą znajdować się w pomieszczeniach zabezpieczonych zamkami patentowymi. Klucze do tych pomieszczeń, po skończeniu pracy, winny być przechowywane w metalowej szafce zamykanej na klucz znajdującej się w zamkniętym pomieszczeniu,
b) budynki JZK, w których znajdują się pomieszczenia stanowiące obszar przetwarzania danych osobowych po zakończeniu pracy winny być chronione przez elektroniczny system alarmowym monitorowany przez firmę ochroniarską.
c) nośnik z kopiami zapasowymi zawierającymi dane osobowe winny być przechowywane w szafie metalowej, ustawionej poza pomieszczeniem serwerowym,
d) dostęp do pomieszczenia, w którym znajdują się urządzenia serwerowe może mieć tylko Administrator Bezpieczeństwa Informacji oraz Administrator Systemu Informatycznego, a w razie ich nieobecności osoby upoważnione,
e) dokumenty papierowe zawierające dane osobowe należy przechowywać w meblach biurowych (szafach, szufladach biurek), a tam gdzie to możliwe, w szafach metalowych, które po zakończeniu pracy są zamykane, a klucze do nich odpowiednio zabezpieczone przed nieupoważnionym dostępem.

9.2. Środki organizacyjne.

a) do przetwarzania danych osobowych przy użyciu systemu informatycznego dopuszczane mogą być osoby na podstawie indywidualnego pozwolenia na dostęp do przetwarzania danych osobowych wydawanego przez Administratora Danych Osobowych.
b) tymczasowe lub zbędne dokumenty papierowe przeznaczone do wyrzucenia, należy niezwłocznie niszczyć w niszczarce dokumentów. W szczególności zabrania się usuwania takich dokumentów przez wyrzucenie ich do kosza na odpadki,
c) stanowiska pracy w powinny być zorganizowane w taki sposób, aby podczas przebywania w pomieszczeniach osób nieuprawnionych uniemożliwiać im nieautoryzowany dostęp do informacji zawartych w dokumentach papierowych, wykonywanych wydrukach komputerowych czy prezentowanych na monitorach komputerowych. Każdego pracownika upoważnionego do przetwarzania danych osobowych obowiązuje zasada tzw. „czystego biurka". Po zakończeniu pracy wszystkie dokumenty zawierające dane osobowe i wrażliwe informacje należy umieścić w przeznaczonych do tego zamykanych na klucz szafach lub szufladach. Klucze należy zabezpieczyć przed dostępem osób niepowołanych. Zabrania się przebywania osób postronnych w pomieszczeniach, w których przetwarzane są dane osobowe bez obecności osób upoważnionych,
d) pracownicy zatrudnieni przy przetwarzaniu danych osobowych zobowiązani są do zachowania ich w tajemnicy,
e) pracownicy przetwarzający dane osobowe przed dopuszczeniem ich do tych danych winni zapoznać się z obowiązującymi przepisami o ochronie danych osobowych, procedurami przetwarzania danych osobowych w JZK oraz informacjami o podstawowych zagrożeniach związanych z przetwarzaniem danych osobowych w systemie informatycznym,
f) należy stosować się do zapisów Instrukcji zarządzania systemem informatycznym,
g) rejestracji podlegają wszystkie przypadki awarii i naprawy systemu,
h) w przypadku, gdy zachodzi konieczność naprawy sprzętu poza siedzibą JZK, należy wymontować z niego nośniki informacji zawierające dane osobowe,
i) w przypadku, gdy uszkodzenie sprzętu zawierającego nośnik danych, na którym zapisane są dane osobowe wymusza konieczność przekazania go poza siedzibę JZK, nośnik ten należy wymontować.

9.3. Sprzętowe środki ochrony.

a) do niszczenia dokumentów stosować należy niszczarki dokumentów,
b) urządzenia wchodzące w skład infrastruktury sieciowej, serwera oraz komputery, na których przetwarzane są dane osobowe winny być podłączone do lokalnych awaryjnych zasilaczy UPS, zabezpieczających przed skokami napięcia i zanikiem zasilania,
c) sieć lokalna winna być skonfigurowana w topologii gwiazdy,
d) sieć lokalna może być podłączona do internetu wyłącznie poprzez router spełniający jednocześnie funkcję sprzętowego, zewnętrznego firewalla filtrującego dane przechodzące pomiędzy siecią lokalną i siecią publiczną,
e) kopie zapasowe danych należy wykonywać codziennie na osobnych zewnętrznych dyskach HD.

9.4. Informatyczne środki ochrony.

a) dostęp do serwera zawierającego dane osobowe winien być zabezpieczony hasłem,
b) dostęp do baz danych osobowych winien być zastrzeżony wyłącznie dla uprawnionych pracowników,
c) należy bezwzględnie stosować działający w tle program antywirusowy w serwerach i na komputerach użytkowników,
d) komputer, z którego możliwy jest dostęp do danych osobowych winien być zabezpieczony hasłem,
e) zastosować należy identyfikatory i hasła dostępu do danych na poziomie aplikacji,
f) dla każdego użytkownika systemu wyznaczać należy odrębny identyfikator,
g) użytkownicy mają dostęp do aplikacji umożliwiający dostęp tylko do tych danych osobowych, do których mają uprawnienia,
h) stosować należy wygaszenie ekranu w przypadku dłuższej nieaktywności użytkownika oraz zabezpieczenie dodatkowym hasem podczas nieaktywności użytkownika trwającej dłuższej niż 15 minut.

10. Nadawanie upoważnienia do przetwarzania danych osobowych.

Szczegółowe wytyczne dotyczące procedury nadawania i odbierania upoważnień do przetwarzania danych osobowych zostały opisane w Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.

11. Spis załączników

Załącznik nr 1 - Wykaz zbiorów danych osobowych
Załącznik nr 2 - Opis przepływu danych pomiędzy systemami

Załącznik Nr 1
do Polityki bezpieczeństwa
w Jastrzębskim Zakładzie Komunalnym
w Jastrzębiu - Zdroju.

WYKAZ

zbiorów danych przetwarzanych w Jastrzębskim Zakładzie Komunalnym w Jastrzębiu-Zdroju

Lp.	Nazwa zbioru danych [1]	Struktura zbiorów danych / Rodzaj danych osobowych	Forma danych [2] (typ bazy danych)	Zabezpieczenie informatyczne [3]	Nazwa programu służącego do przetwarzania danych osobowych	Lokalizacja [4]/ Nr pokoju	Zabezpieczenie fizyczne [5]
1	**Ewidencja interesantów**	**Dane adresowe klienta:** nazwisko, imiona, PESEL, kod pocztowy, miejscowość, ulica, nr domu, nr lokalu, kraj, nr terytorialny, telefon, faks, e-mail, WWW, nazwa banku, numer rachunku bankowego, źródło danych. **Rejestr korespondencji przychodzącej od klienta:** status pisma, stan pisma, kod rejestru, data wpływu, numer kancelaryjny, temat, data pisma, osoba odpowiedzialna, kod nadawcy, nazwa nadawcy, adres nadawcy) **Rejestr korespondencji wychodzącej do klienta:** status pisma, stan pisma, kod rejestru, data wpisu, numer kancelaryjny, temat, data pisma, osoba odpowiedzialna, kod adresata, nazwa adresata, adres adresata, wartość przesyłki, waga przesyłki, opłata, kwota pobrania. **Rejestr spraw klienta:**	EBD (MySQL)	I, SZ	Elektroniczne Zarządzanie Dokumentacją SIDAS	D1/1/8 D2/1/2/3/10/11 /12 O N	A, ZP

		status sprawy, stan sprawy, komórka organizacyjna, symbol JRWA, hasło JRWA, data rozpoczęcia sprawy, osoba odpowiedzialna, znak sprawy, data pisma, termin załatwienia, sposób załatwienia, temat, treść/przebieg załatwienia sprawy, nazwa strony, adres strony.					
2	Kadry	**Dane adresowe pracownika:** nazwisko, imię, drugie imię, płeć, typ pracownika, prawność, imię ojca, imię matki, nazwisko panieńskie matki, nazwisko rodowe, data urodzenia, miejsce urodzenia, narodowość, obywatelstwo, numer dokumentu tożsamości, organ wydający dokument tożsamości, data wydania dokumentu tożsamości, PESEL, NIP). **Przebieg pracy pracownika:** data przyjścia, godzina przyjścia, data wyjścia, godzina wyjścia, powód nieobecności. **Płace pracownika:** rodzaj zatrudnienia, wymiar etatu, staż pracy, rodzaj stawki, stawka zasadnicza, składniki płacy	EBD/DP (FireBird)	I, SZ	VERITUM - Kadry	D2/1	A, ZP, SZK, R
3	Płace	**Dane adresowe pracownika:** numer ewidencyjny, imię, nazwisko, drugie imię, nazwisko rodowe, imię ojca, imię matki, data urodzenia, miejsce urodzenia, PESEL, NIP,	EBD/DP (FireBird)	I,SZ	VERITUM - Płace	D2/1/10	A, ZP, SZK, R

		dokument tożsamości, nr dokumentu tożsamości, obywatelstwo, kod gminy wg GUS, kraj, województwo, powiat, gmina, ulica, numer domu, numer lokalu, miejscowość, kod pocztowy, poczta, telefon, faks, data zameldowania, skrytka pocztowa) **Płace pracownika:** rodzaj zatrudnienia, wymiar etatu, staż pracy, rodzaj stawki, stawka zasadnicza, składniki płacy					
4	**Płatnik - ZUS**	**Dane adresowe pracownika:** nazwisko, imię, nazwisko rodowe, data urodzenia, PESEL, NIP, dokument tożsamości, kod pocztowy, miejscowość, ulica, numer domu, numer lokalu. **Składki pracownika:** kwota składki, podstawa wymiaru składki.	EBD (ACCESS)	I, SZ	PŁATNIK	D2/10	A, ZP
5	**Faktury JZK**	**Dane adresowe klienta:** Imię, nazwisko, adres zamieszkania, PESEL, NIP **Dane dot. faktury:** numer faktury, kwota netto, podatek VAT, kwota brutto, data wystawienia, data sprzedaży, forma płatności, termin płatności.	EBD/DP (DBF)	I, SZ	TRES	D1/8 D2/2/3/11/12 O	A, ZP A, ZP, SZK, R

6	**Faktury Targowisko**	**Dane adresowe klienta:** Imię, nazwisko, adres zamieszkania, PESEL, NIP **Dane dot. faktury:** numer faktury, kwota netto, **podatek VAT, kwota brutto, data wystawienia, data sprzedaży, forma płatności, termin płatności.**	EBD/DP (DBF)	I, SZ	TRES	D1/8 D2/2/3/11/12 O	A, ZP A, ZP, SZK, R
7	**Faktury Cmentarz**	**Dane adresowe klienta:** Imię, nazwisko, adres zamieszkania, PESEL, NIP **Dane dot. faktury:** numer faktury, kwota netto, **podatek VAT, kwota brutto, data wystawienia, data sprzedaży, forma płatności, termin płatności.**	EBD/DP (DBF)	I, SZ	TRES	D1/8 D2/2/3/11/12 O	A, ZP A, ZP, SZK, R
6	**Cmentarze**	**Dane adresowe dysponenta grobu:** imię, nazwisko, adres zamieszkania, PESEL, NIP. **Dane dot. grobu:** Nr kwatery grzebalnej, rząd, nr grobu, Data wniesienia opłaty.	EBD (DBF)	I, SZ	AKWILA	O	A, ZP
7	**System Informacji Terenowej (dane zewnętrzne)**	**Dane adresowe właściciela: nazwisko,** imię, imię ojca, imię matki, PESEL, województwo, powiat, gmina, ulica, nr budynku/lokalu **Grunty i budynki właściciela:** numer działki, identyfikator działki, identyfikator budynku, położenie budynku, miejscowość, ulica, numer	EBD (ORACLE)	I, SZ	SIT - ISPiK	D2/3	A, ZP

		budynku.					
8	**Rejestr umów dzierżawy**	**Dane adresowe klienta:** imię, nazwisko, adres zamieszkania, PESEL, NIP	DP	-	-	D1/2 D2/2	A, ZP, SZK, R
9	**Rejestr umów najmu lokali**	**Dane adresowe klienta:** imię, nazwisko, adres zamieszkania, PESEL	DP	-	-	D2/2	A, ZP, SZK, R
10	**Windykacja**	**Dane adresowe klienta:** Imię, nazwisko, adres zamieszkania. **Dane dotyczące zobowiązań** rodzaj zobowiązania, typ zobowiązania, nazwa wierzyciela, nazwisko i imię zobowiązanego, wartość zobowiązania	DP	-	-	D2/2/12	A, ZP, SZK, R
11	**Adopcje zwierząt**	**Dane adresowe klienta:** imię, nazwisko, adres zamieszkania, PESEL, numer dokumentu tożsamości, organ wydający dokument tożsamości, nr telefonu	DP	-	-	N	A, ZP, SZK
12	**Opieka nad zwierzętami**	**Dane adresowe społecznego opiekuna:** imię, nazwisko, adres zamieszkania, nr telefonu	DP	-	-	O N	A, ZP, SZK
13	**Abonamenty - parking strzeżony**	**Dane adresowe klienta:** imię, nazwisko, adres zamieszkania, nr telefonu, nr rejestracyjny pojazdu	DP	-	-	D1/2	A, ZP, SZK, R
14	**Zezwolenia na wjazd na parking**	**Dane adresowe klienta:** imię, nazwisko, adres zamieszkania.	DP	-	-	D1/2	A, ZP, SZK, R
15	**Sprzedaż drewna**	**Dane adresowe klienta:** imię, nazwisko, adres zamieszkania.	DP	-	-	D1/2	A, ZP, SZK, R
16	**ZFŚS**	**Dane adresowe pracownika i osób uprawnionych do korzystania z ZFŚS:** imię, nazwisko, adres zamieszkania.	DP	-	-	D2/2	A, ZP, SZK, R

		Dane o sytuacji materialnej pracownika: średni dochód na osobę.					
17	**Rejestr skarg i wniosków**	**Dane adresowe klienta:** imię, nazwisko, adres zamieszkania, nr telefonu	DP	-	-	D2/3	A, ZP, SZK, R
18	**Umarzanie należności**	**Dane adresowe dłużnika:** imię, nazwisko, adres zamieszkania, miejsce pracy **Dane o sytuacji materialnej dłużnika:** miejsce pracy, dochody, obciążenia	DP	-	-	D2/2/11/12	A, ZP, SZK, R

Opis:

1) nazwa zwyczajowa lub własna,
2) elektroniczna baza danych (EBD), dokumentacja papierowa (DP),
3) indywidualne hasło dostępu (I), szyfrowanie transmisji danych (SZ), wydzielona sieć fizyczna (SF),
4) ul. Dworcowa 17d - budynek nr 1 (D1-dział techniczny), ul. Dworcowa 17d - budynek nr 2 (D2-dyrekcja), ul. Dworcowa 17d - budynek nr 3 (biuro strefy płatnego parkowania), ul. Okrzei 5 (O), ul. Norwida 50 (N)
5) Alarm (A), kontrola dostępu (KD), zamek patentowy (ZP), szafa metalowa (SZM), szafa zamykana na klucz (SZK), rolety zewnętrzne (R)

Załącznik Nr 2
do Polityki bezpieczeństwa
w Jastrzębskim Zakładzie Komunalnym
w Jastrzębiu - Zdroju.

Opis przepływu danych pomiędzy systemami

Lp.	Zbiór źródłowy	Zbiór docelowy	Zakres przekazywanych danych	Sposób przekazu
1	Kadry	Płace	Przebieg pracy pracownika Składniki płacy	Tradycyjny
2	Cmentarze	Faktury Cmentarz	Dane adresowe dysponenta grobu	Tradycyjny
3	Windykacja	Faktury	Dane adresowe klienta Dane dotyczące zobowiązań	Tradycyjny
4	Abonamenty - parking strzeżony	Faktury	Dane adresowe klienta	Tradycyjny
5	Sprzedaż drewna	Faktury	Dane adresowe klienta	Tradycyjny
6	ZFŚS	Płace	Dane pracownika Wysokość dofinansowania	Tradycyjny
7	Umarzanie należności	Faktury	Dane adresowe dłużnika Dane dotyczące zobowiązań	Tradycyjny